creative commons
COMMONS DEED

저작자표시-비영리-변경금지 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.

다음과 같은 조건을 따라야 합니다:

저작자표시. 귀하는 원저작자를 표시하여야 합니다.

비영리. 귀하는 이 저작물을 영리 목적으로 이용할 수 없습니다.

변경금지. 귀하는 이 저작물을 개작, 변형 또는 가공할 수 없습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 이용허락규약(Legal Code)을 이해하기 쉽게 요약한 것입니다.

Disclaimer

dCollection

이학석사 학위논문

디지털 증거의 본질에 어울리는 증거조사 방안

Methods for Examination of Evidence that conforms to the nature of Digital Evidence

2021년 2월

서울대학교 융합과학기술대학원

수리정보과학과 디지털포렌식학 전공

박 찬 석

디지털 증거의 본질에 어울리는 증거조사 방안

지도교수 이 병 영

이 논문을 이학석사 학위논문으로 제출함

2020년 12월

서울대학교 융합과학기술대학원

수리정보과학과 디지털포렌식학 전공

박 찬 석

박 찬 석의 석사 학위논문을 인준함

2021년 1월

위 원 장	안 정 호	(인)
부 위 원 장	이 병 영	(인)
위 원	김 판 기	(인)

요약 (국문초록)

형사소송의 목표는 구체적 법률관계 즉, 범죄의 성립 여부를 확정하고, 범죄가 성립하는 경우 적정한 형벌의 종류와 양을 정함에 있다. 이러한 법률관계는 일정한 사실관계를 전제로 하고, 그 사실관계를 확정하는데 사용되는 자료가 증거이다. 증거는 아래 3가지 의미를 포괄한다. 즉 ① 사실 인정의 자료가 되는 물건이나 사람 자체(예: 증인, 증거서류, 증거물)를 가리키는 **증거방법**, ② 증거방법을 조사함으로써 알게 된 내용(예: 증인의 증언내용, 증거물의 성질)을 가리키는 **증거자료**, 그리고 ③ 증거자료와 그 밖에 증거조사를 통해 얻는 비언어적인 자료(예: 증인신문시의 표정이나 태도 등)를 포괄하여 뜻하는 **증거결과**가 그것이다.

디지털 증거는 '2진수 형태로 저장 혹은 전송되는 것으로서 법정에서 신뢰할 수 있는 정보'라 정의할 수 있다. 이는 증거의 위 3가지 의미 중 '증거자료'에 주안점을 둔 개념이다.

우리나라에서 디지털 증거에 관한 수사 및 재판실무상 그 증거능력 인정 요건으로서 동일성, 무결성, 신뢰성 등을 충족하여야 하고, 전자정보가 담긴 저장매체 또는 하드카피나 이미징 등 형태를 수사기관 사무실 등으로 옮겨 복제·탐색·출력하는 경우 판례는 그와 같은 일련의 과정에서 원칙적으로 피압수자나 변호인에게 참여의 기회를 보장하여야 한다고 보고 있다. 실무상 디지털 증거를 수집할 때에 해시값을 산출하여 이를 기재한 확인서를 참여자에게 교부하는 방식으로 동일성 등의 문제에 대처하고 있다.

그런데 예컨대 세월호 선체의 CCTV 동영상 저장장치를 둘러싼 논란에서 보듯이 디지털 증거를 최초 수집할 때 피압수자 등이 참여할 수 없거나, 조사 주체에 대한 신뢰가 없는 상황에서는 디지털 증거를 최초로 수집한 시각 및 그 이후의 분석 과정에 대하여도 불신이 생길 수 있다.

이에 이 논문은 우선 디지털 증거에 관한 계층적 구조를 살펴보고,

디지털 증거의 본질과 특성에 가장 어울리는 증거조사 방법으로 아래 3가지 개선 방안을 제안한다.

첫째는 현재와 같이 '압수물인 디지털 저장매체로부터 출력한 문건 등'(= '증거방법'에 해당, 증거능력 요건으로서 동일성, 무결성, 신뢰성 등 입증이 필요)을 증거로 제출하는 것이 아니라, '0과 1이라는 디지털 형태의 정보 자체'(='증거자료'에 해당)를 증거로 수집하여 법정에 제출하는 방안이다. 이 경우 디지털 형태의 정보인 파일 자체(1차 증거)와 이를 문서뷰어 등 프로그램으로 재현한 화면이나 문서(2차 증거)를 함께 제출하는데, 이는 예컨대 외국어나 기술부호로 기재된 문서(1차 증거)와 이를 번역 또는 감정한 결과(2차 증거)를 함께 제출하는 것에 비견될 수 있다.

둘째는 위와 같이 1차 증거로 제출하는 디지털 증거의 진정성을 확보하는 기술적 봉인기법의 개선 방안이다. 현재는 증거자료인 파일 자체에 대한 해시값을 산출하여 참여자에게 확인서를 교부하는데, 해시값 산출 대상에 증거자료인 파일 외에 '객관적으로 검증 가능한 해당 파일의 수집시각'을 포함하는 것이다. 해당 파일의 수집시각을 공인된 방법으로 획득하여 해시 대상에 포함시키면 수집 현장에 참여자가 없더라도 해당 파일의 수집시각을 객관적으로 보장할 수 있다. 그 기술적 수단으로는 NTP 또는 TSA 방식을 고려할 수 있다.

셋째는 위와 같은 일련의 증거수집 및 분석 과정에 대한 신뢰를 확보하기 위하여, 파일 수집, 분석 및 시각 확인 등의 모든 절차를 수행하는 시스템을 가상머신으로 구현하고, 그 가상머신에서 이루어지는 모든 행위를 기록한 후, 가상머신 자체에 대한 해시값과 행위 기록에 대한 해시값을 산출하여 보존하는 것이다. 이로써 포렌식 조사 주체 및 조사 과정에 대한 신뢰를 확보할 수 있다.

이상과 같이 디지털 증거의 수집, 조사에 관한 현행 실무상 미비점에 대한 개선방안을 이론적 차원에서 검토하였다. 향후 형사전자소송시스템이 완비되면 법정에서 제안된 방식의 증거조사가 원활히

이루어질 수 있을 것이다.

.....

주요어 : 디지털 증거, 증거능력, 해시, 수집시각, NTP, TSA, 가상머신

학 번 : 2019-29821

<본문 차례>

<그림 차례>

<첨부자료>

1. 서론

현대 사회에서 디지털 데이터의 중요성은 점차 커지고 있다. 우리는 현실의 물리적 세계와 가상의 디지털 세계를 오가며 또는 양자역학에서 말하는 것처럼 중첩하여 존재하며 생활을 이어가고 있다. 이는 범죄의 세계에서도 마찬가지이다. 그리하여 범죄수사 및 형사재판의 실무에서도 디지털 데이터 형태의 증거, 즉 디지털 증거가 지속적으로 증가하고 있다.[1)]

그러나 디지털 증거의 개념이나 본질이 무엇인지 아직 모호하고, 그에 따라 디지털 증거의 수집, 탐색, 분석 및 법정에의 제출 과정에서 수많은 쟁점이 해결되지 않은 상황이다.

대표적으로 범죄와 관련된 디지털 증거를 최초로 수집하고, 이를 복제 및 재복제한 후 탐색, 분석 과정을 거쳐 법정에 증거로 제출하는 일련의 과정에서 피압수자(대표적으로 피의자)의 참여권을 어디까지 보장해야 하고, 보장해 줄 수 있는지? 왜 디지털 증거에 대하여는 다른 일반적인 증거와는 달리 '동일성, 무결성' 등의 증거능력 요건이 필요한 것인지? 만약 최초 수집 현장에 피압수자가 없었거나 피압수자(예컨대 ISP)와 정보주체(예컨대 인터넷 서비스 이용자)가 다른 경우에, 법정에 제출된 디지털 증거를 최초로 수집한 시각이나 그 조사과정에 대한 의혹이 제기될 경우 이를 객관적으로 확인할 수단은 없는 것인지 등이다.

---

1) 미국 버클리대학(University of California, Berkeley)의 한 연구에 의하면 세계에서 생성되는 정보의 약 90% 이상이 디지털 형태로 만들어지고 있다고 한다. Peter Lyman & Hal R. Varian, U.C. Berkely, "How Much Storage is Enough?", ACM Queue vol.1, no.4 June 2003.; 이상미, "관련성 없는 디지털 증거 삭제시 이중해시를 이용한 무결성 입증 방안", 석사학위논문, 서울대학교(2016), 3에서 재인용

이러한 쟁점은 단지 이론적인 가정이 아니다. 디지털 증거에 관한 일련의 압수·수색영장 집행과정에 피압수자의 참여권이 온전히 보장되지 않았다는 이유로 해당 디지털 증거의 증거능력을 부정한 사례가 있고,[2] 최근에는 세월호참사특별조사위원회(이하 '특조위' 또는 '사참위'라 한다)가 2014년 법원에 제출된 세월호 참사 당시 선체 내부를 찍은 폐쇄회로(CC)TV 영상이 조작됐다는 조사 결과를 발표했다. 특조위는 2020. 9. 22. "2014년 광주지법 목포지원에 제출됐던 CCTV 분석 결과 1만 8353곳에서 원본과 다른 데이터가 발견됐다."며 "원본에 다른 데이터가 덮어씌워지며 남은 흔적으로 보인다."고 했다. 원본과 다른 데이터가 씌워진 구간은 재생이 되질 않는데, 이는 인위적으로 조작하지 않으면 벌어질 수 없는 현상이란 지적이다. 이에 대해 "조작에 실패한 흔적일 수도 있고 재생되지 않게 하는 것 자체가 목적일 수도 있다"고 설명했다. 특조위는 또 "당시 사고를 수습하던 현장지휘본부 문서를 살펴보니 2014년 5월 9일 DVR를 인양했다는 흔적이 있다. 이는 해군이 밝혀왔던 발견 시점보다 한 달 이상 앞선다."고 전했다.[3]

본 연구는 이러한 문제점들을 해결할 수 있는 세 가지 개선방안을 제안하고자 한다. 간략히 앞서 말하자면 (1) 디지털 증거의 본질에 대한 인식 전환, (2) 디지털 증거의 최초 수집시각을 객관적으로 보증하는 방안, (3) 포렌식 조사 시스템과 조사과정에 대한 객관적 검증 방안이다.

이하 제2장에서 우선 디지털 증거의 개념에 관한 논의상황, 디지털 증거의 특징, 그리고 디지털 증거에 특별히 요구되는 증거능력 요건을 살펴보고, 제3장에서 현재 수사 및 재판실무의 문제점을 상세히

2) 대법원 2015. 7. 16.자 2011모1839 전원합의체 결정 사안
3) 동아일보 2020. 09. 23. 기사

살펴본 후, 제4장 내지 제6장에서 위 개선방안을 차례로 상술한 후 제7장에서 결론을 맺고자 한다.

2. 디지털 증거의 증거능력

가. 증거란?

형사소송의 궁극적 목표는 구체적 법률관계의 형성·확정이다. 여기에 속하는 것으로 1) 범죄의 성립 여부, 2) 범죄가 성립하는 경우 형벌의 종류와 양형이 있다. 이러한 구체적 법률관계는 독자적으로 구성되는 것이 아니고 언제나 일정한 사실관계를 전제로 발전한다. 그러므로 형사소송에서는 이러한 사실관계의 확정이 무엇보다 중요한데, 이러한 "사실관계 확정에 사용되는 자료"를 **증거**라고 한다. 증거에 의해 사실관계를 확인하는 과정이 증명이다.

증거는 증거방법(증거수단), 증거자료(증명자료) 및 증거결과의 세 가지 의미를 포함한다. ① **증거방법**은 사실 인정의 자료가 되는 물건이나 사람 자체(예: 증인, 증거서류, 증거물)이다. ② **증거자료**는 증거방법을 조사함으로써 알게 된 내용(예: 증인의 증언내용, 증거물의 성질)이다. 또한 ③ **증거결과**는 증거자료와 그 밖의 증거조사

[그림 1] 증거방법(증인)과 증거자료("2번이 훔치는 걸 봤다"는 진술내용)의 구별

를 통해 얻는 비언어적인 자료(예: 증인신문시의 표정이나 태도 등)를 포괄한다.[4)]

수사는 숨겨진 범죄의 진상을 발견하기 위하여 수사기관이 은밀하게 진실 인식에 접근하는 과정이다. 이에 대하여 재판은 수사기관과 피고인 그리고 수집된 증거를 전제로 진실을 인식하고 확정하기 위한 공식적인 절차이다. 공식성은 국민으로부터 재판의 정당성을 인정받기 위해 필요하다. 이러한 점에서 올바른 증거라는 에토스(ethos)야말로 국민적 신뢰의 출발점이다. 적어도 재판에서 증거는 자격 있는 증거이어야 하고, 이처럼 '사실인식(유죄 인정)의 증거가 될 수 있는 자격'을 **증거능력**이라고 할 수 있다.[5)]

나. 디지털 증거의 개념

디지털 증거가 활용되는 영역이 계속 확대되고 있고 그에 따른 문제가 발생함에도 디지털 증거가 무엇인가에 대한 개념적 정의는 아직 확립되었다고 보기 어렵다. 이는 국내뿐 아니라 외국에서도 마찬가지이다.

일부 국가의 법률에서는 '전자적 기록(Electronic Document)'이라는 용어를 사용하는 경우도 있다. 미국 법무부의 경우를 보면 2001년 발간한 수사지침 및 2002년 발간한 압수수색매뉴얼에서는 '전자

---

4) 배종대·이상돈, 형사소송법 제2판, 홍문사(1997), 480

5) 송희식, "증거법이론에 있어서 인식과 진술-증거법 일반이론의 모색-", 형사법의 신동향 통권 39호(2013), 55-56 ; 송희식은 이 글에서 영미법상 배심재판에서 증거능력은 배심원들에 대한 증거인식의 허용성(admissibility)와 같은 의미이고, 대륙법의 전문법관제에서 증거능력은 유죄판결문에서 유죄의 증거로 적시될 수 있는 자격이라고 하면서, 양 법체제에서 증거능력의 본질이 상이함을 지적한 후, 그럼에도 우리나라와 일본의 증거능력 개념이 증거법의 일반이론을 정초할 수 있는 단서라는 흥미로운 주장을 전개한다.

적 증거(Electronic Evidence)'라는 용어를 사용하고 있으나, 2004년 4월 NIJ(National Institute of Justice)에서 발간한 지침서에서는 '디지털 증거(Digital Evidence)'라는 용어를 사용하고 있다. 한편 미국의 NCFS(National Center for Forensic Science)에서는 포렌식(forensic)의 대상인 증거의 종류를 크게 물리적 증거(Physical Evidence), 생물학적 증거(Biological Evidence), 디지털 증거(Digital Evidence) 등으로 나누고 있다.[6)]

우리나라에서는 법률 용어로 '전자적'이라는 용어 대신 '디지털'이라는 용어를 사용하는 것이 아직 보편적이지는 않다. 형법에서는 '전자기록'이라는 용어를 사용하고 있고(예컨대 제227조의2 공전자기록위작·변작죄), 형사소송법에서는 '정보저장매체'라는 용어를 사용하며(예컨대 제106조 압수 조항), 전자서명법, 전자거래기본법 등에서 '전자'라는 용어를 사용하고 있다. 한편 콘텐츠산업 진흥법에서는 '디지털'이라는 용어를 사용하기도 한다(예컨대 제16조 표준화의 추진).[7)]

전자(電磁)는 전기적, 자기적 기억장치를 의미하지만 오늘날 컴퓨터 정보처리 및 기억장치의 대부분은 전자(電子) 장치이므로, 컴퓨터나 스마트폰 등 전자매체의 특성을 고려하여 법률용어로서도 전자증거라는 우리말을 사용하는 것이 좋다는 견해[8)]가 있다. 또 전자증거란 전기와 자기신호를 이용하여 매체에 저장된 증거를 총체적으로 의미하는 것으로, 저장형태는 디지털 방식이 될 수도 있고 아날로그 방식(녹음테이프나 비디오테이프 등)이 될 수도 있으나, 아날로그 방식을 사용하는 녹음테이프나 비디오테이프가 점차 사라지

---

6) 정교일, "디지털 증거의 압수와 공판정에서의 제출방안", 형사법의 신동향 통권 제25호(2010), 109

7) 정교일, "디지털 증거의 압수와 공판정에서의 제출방안", 형사법의 신동향 통권 제25호(2010), 110 참조

8) 오기두, "관련성 없는 전자증거의 수집과 영장주의", 사법논집 제65집(2017), 265

고 있어 전자증거를 디지털 증거와 같은 의미로 사용하더라도 개념상의 혼동은 발생할 여지가 적고, 우리나라의 법률 중 대다수는 아직도 '디지털 형태'라는 용어 대신 '전자적 형태'라는 표현을 사용하고 있으므로 전자증거나 전자적 증거라는 표현을 굳이 배척할 이유는 없다는 견해[9]도 있다.

그럼에도 이 논문은 디지털 증거의 본질에 천착하여 그에 부합하는 증거조사 방안을 제안함을 목적으로 한 학술논문이므로, 보다 엄밀하고 적확한 용어인 '디지털 증거'를 사용하기로 한다.

디지털 증거에 관하여, 국제 조직인 IOCE(International Organization on Computer Evidence)[10]에서는 '2진수 형태로 저장 혹은 전송되는 것으로서 법정에서 신뢰할 수 있는 정보'라 정의하고,[11] 미국 과학실무그룹(SWGDE, Scientific Working Group on Digital Evidence)은 '디지털 형태로 저장되거나 전송되는 증거가치 있는 정보'[12]로 정의하였다. Eoghan Casey는 종래 이를 '범죄를 입증하거나 범죄와 피해자 또는 범죄자 사이의 연결 고리를 제공할 수 있는 모든 디지털 데이터'[13]로 정의하였다가, Chisum을 인용하

9) 이숙연, "디지털 증거 및 그 증거능력과 증거조사방안-형사절차를 중심으로 한 연구-", 사법논집 제53집(2011), 251

10) 미국, 호주, 홍콩, 영국 등 각국의 실무자들을 중심으로 만들어진 디지털 증거에 관한 국제기구

11) 김방글, "삭제 후 복구된 디지털 파일의 증거능력 인정 요건에 관한 연구", 석사학위 논문, 서울대학교(2020), 4

12) 1998년 미국 법무부 마약수사청, 연방수사국, 관세청 및 국세청 등의 증거분석 연구소들 중심으로 구성된 '디지털 증거에 관한 과학실무그룹(Scientific Working Group on Digital Evidence)'에서 정의한 것이다. 탁희성·이상진, 디지털 증거분석 도구에 의한 증거수집절차 및 증거능력 확보방안, 한국형사정책연구원(2006), 31 ; 이숙연, "디지털 증거의 증거능력과 증거조사방안", 재판자료 제133집 형사법 실무연구Ⅱ(2016), 48에서 재인용

13) Eoghan Casey, Digital Evidence and Computer Crime, 2nd edition, 12 ; 이숙연, "디지털 증거의 증거능력과 증거조사방안", 재판자료 제133집 형사법 실무연구Ⅱ(2016), 48에서 재인용

며 '컴퓨터를 이용하여 저장되거나 전송되는 데이터로, 범죄가 어떻게 발생하였는지에 대한 가설을 뒷받침 또는 반박하거나, 고의나 알리바이와 같이 범죄의 중요한 요소를 드러내는 정보'[14]로 정의하고 있다.

디지털 증거는 저장방식이 0과 1로 이루어진 2진수 방식의 정보이며 이를 기본적으로 디지털이라고 한다는 점, 기본적으로 저장매체와 별개인 정보라는 점, 그리고 증거로서의 가치를 가지고 있는 정보이어야 한다는 점 등을 고려하면 디지털 증거를 '디지털 형태로 저장되거나 전송되는 증거 가치가 있는 정보'라고 규정한 디지털 증거에 관한 SWGDE의 정의는 이러한 특징을 합리적으로 나타낸다고 볼 수 있다.

따라서 **디지털 증거**란 범죄와 피해자 또는 범죄와 가해자 사이의 연결고리를 제공할 수 있는 모든 디지털 데이터를 말하는 것으로 이해할 수 있다. 여기에서 디지털 데이터란 전통적 의미의 컴퓨터상에 있는 데이터뿐만 아니라 이진 형태로 저장되거나 전송될 수 있는 모든 텍스트, 이미지, 오디오 및 비디오 데이터 등을 포함한다고 할 것이다.[15]

결국 디지털 증거란 위와 같은 요건을 갖춘 '디지털 형태의 정보 그 자체' 다시 말하면 '0과 1의 수로 표현할 수 있는 수의 배열 정보 그 자체"라고 할 수 있다.

한편 국내문헌으로 오기두, 전자증거법, 박영사, 2015, 5면은 "디지털 증거란 전자적으로 기록되거나 그 내용이 현출되고 있는 증거를

---

14) "any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi"(Eoghan Casey, Digital Evidence and Computer Crime, 2nd edition, 12) ; [이숙연의 위 2016년 논문에서 재인용]

15) 정교일, "디지털 증거의 압수와 공판정에서의 제출방안", 형사법의 신동향 통권 제25호(2010), 111

통틀어 말한다. 일반적으로 컴퓨터의 입력장치, 연산·제어·기억장치, 출력장치 등 컴퓨터의 기본구조에 관련된 증거방법, 컴퓨터 통신에 관련된 증거방법, 디지털 방식에 의한 전자적 기억매체에 수록된 전자정보나 그 전자기억매체 내지 그 전자정보의 출력물 등을 총칭하고, 그 전자정보 전부나 일부를 복제한 자기디스크, 그 데이터를 새로이 가공처리한 데이터 내지 그와 같이 가공처리된 데이터를 저장한 자기디스크, 컴퓨터 모니터에 떠 있는 문자나 화상, 동화상, 컴퓨터 스피커에 출력되는 소리 또는 음악, 전선이나 광섬유를 통해 전자적 방식으로 이동되거나 무선방식으로 이동하는 컴퓨터 통신 데이터나 음성, 데이터베이스, 전자우편, 전자게시판에 있는 데이터 등을 일컫는 용어이다."라고 한다.[16]

다. 디지털 증거의 특성[17]

1) 매체독립성과 원본과 사본 구분의 곤란성

앞서 본 대로 디지털 증거는 '유체물'이 아니라 각종의 디지털 매체에 저장된 혹은 전송 중인 '정보' 그 자체로 보아야 한다. 2진수의 형태로 변환하여 작성·저장된 정보 값은 어느 매체에 저장되든 동일한 가치를 가진다. 아날로그 형태의 신호를 복사하는 경우에는 복사본의 신호가 원본의 신호보다 S/N(신호/잡음)비가 감소하므로 이론적으로 원본과 복사본의 구별이 가능하다. 그러나 디지털 신호의 경우 신호의 유·무만을 검출하면 소기의 목적을 달성할 수 있으므로, 원본의 신호형태를 복사하는 것이 아니라 신호의 유·무만을 검출한

16) 김방글, "삭제 후 복구된 디지털 파일의 증거능력 인정 요건에 관한 연구", 석사학위 논문, 서울대학교(2020), 5에서 재인용

17) 이하는 주로 손지영·김주석, 디지털 증거의 증거능력 판단에 관한 연구, 사법정책연구원(2015), 25-30을 발췌, 인용함

후 디지털 형태의 신호를 다시 만들어서 기록하게 된다.[18] 따라서 이 정보는 값이 같다면 어느 매체에 저장되어 있든지 매체와 독립하여 동일한 가치를 지니게 되는 것이다.

2) 변경의 용이성 내지 취약성[19]

디지털 정보는 일부 또는 전체에 대한 수정 및 삭제 등 편집이 용이하다. 이 특징은 실용적 측면에서 디지털 정보를 쉽게 가공할 수 있다는 장점으로 활용될 수 있지만 증거가치 측면에서는 전부·일부의 삭제, 변경 등이 용이하다는 단점으로 작용한다. 이러한 취약성 때문에 지체 없이 신속하게 정보를 수집하여야 할 수사상 필요가 생기고, 디지털 포렌식 절차를 통하여 수집된 증거가 변경되지 않은 것임을 법정에서 입증할 필요가 생긴다.

3) 비가시성·비가독성 및 잠재성[20]

디지털 기록매체에 저장된 데이터는 2진수의 신호체계로 작성·보존되어 그 존재 및 상태를 보통 사람의 지각으로는 바로 인식할 수

---

18) 이성진, "디지털 포렌식스 기술 발전 방안", 디지털 포렌식 연구(2007. 11.), 3 ; 이숙연, "디지털 증거 및 그 증거능력과 증거조사방안-형사절차를 중심으로 한 연구-", 사법논집 제53집(2011), 256에서 재인용

19) 노명선, "전자적 증거의 수집과 증거능력에 관한 몇 가지 검토", 형사법의 신동향 제16호 (2008), 78

20) 비가시성·비가독성이란 용어와 함께 잠재성을 특징으로 꼽는 견해에 따르면 디지털 증거는 모니터나 프린터를 통해서 출력되어야만 가시성과 가독성을 갖는다는 점에서 정보 자체가 비가시성·비가독성의 성격을 갖지만 출력과정에서도 여러 정보가 누락되고 일정한 가시적 정보만 제공된다는 점을 지적한다. 이 때에도 데이터 안에는 좀 더 많은 잠재적 정보가 포함되어 있다는 점을 들어 더 포괄적인 용어로 잠재성(Latent)이란 용어를 사용하고 있다. 탁희성·이상진, 디지털 증거분석 도구에 의한 증거수집절차 및 증거능력 확보방안, 한국형사정책연구원(2006), 35-36

없다. 또한 수집된 디지털 증거에는 표면상 알 수 없고 숨어 있는 잠재 정보가 존재하며 이를 확인하기 위해서는 그에 맞는 적절한 소프트웨어가 필요하다. 디지털 정보를 증거로 사용하기 위해서는 일정한 판독절차를 거쳐야 하고, 디코딩(Decoding), 복호화(Decrypt), 압축 해제(Decompress)의 과정이 필요하며,[21] 이 과정에는 소프트웨어와 전문가들이 개입한다. 이와 같이 디지털 정보의 확보 과정은 물리적이 아닌 기술적·논리적인 방법이 동원되며, 이러한 측면은 디지털 증거의 증거능력 검토 과정에서 포렌식 도구의 신뢰성이나 분석관의 전문성 검증과 연결된다.

4) 대량성

과거에는 정보의 생성 및 저장이 종이와 잉크를 매체로 한정적으로 이루어졌으나, 최근에는 이 과정이 디지털 형태로 급격히 전환되면서 그 정보의 양이 기하급수적으로 늘어나고 있다. 디지털 증거는 개인이 사용하는 컴퓨터에서 기업의 전산회계자료에 이르기까지 갖가지 종류의 응용프로그램에 의해 생성된 수많은 형태의 자료가 저장되어 있는 경우가 대부분이다. 아주 적은 저장매체에도 방대한 분량의 정보를 저장할 수 있어 저장매체의 압수에 있어 범죄와의 관련성이 있는 정보뿐 아니라 그와 관련이 없는 수많은 사생활 비밀, 영업비밀 자료가 포함되어 있을 수 있다.

---

21) 미리 약속된 일정한 규칙에 따라 데이터를 특정 포맷으로 코드화하는 것을 **인코딩**, 그 반대를 디코딩이라고 한다. **복호화**는 암호화된 코드를 원래의 평문으로 복구하는 과정을 말한다. 데이터 **압축**은 파일이나 통신 메시지와 같은 데이터 집합의 기억 영역을 절감하거나 전송 시간을 단축하기 위해 데이터에 포함되어 있는 중복된 bit열 또는 패턴을 삭제하고 그것들을 좀더 적은 수의 bit 또는 요약 형식으로 부호화하는 등 여러 가지 방법으로 행해진다. 중복된 bit열 또는 패턴을 복원하면 원래의 데이터가 복원된다. 탁희성·이상진, 디지털 증거분석 도구에 의한 증거수집절차 및 증거능력 확보방안, 한국형사정책연구원(2006), 35

5) 전문성

디지털 증거를 처리하는 과정에는 많은 전자적 기술과 프로그램이 사용된다. 따라서 저장된 자료가 어떤 소프트웨어를 사용하여 저장되었는지 정확하게 규명하지 않으면 자료에 접근하기조차 어려운 문제가 발생하기도 한다.[22] 이러한 경우가 아니라고 해도 수집된 자료를 가독성·가시성 있는 자료로 변환하여 제시하고 그 내용을 해석하는 데 전문적 지식이 없이는 불가능한 경우가 있고, 법정에 제시된 최종 산출물이 원본 증거에 대한 정확한 해석인지 검증하는 것도 필요하다.[23] 따라서 디지털 증거의 수집과 적정한 분석을 위해서는 디지털 정보, 분석 프로그램이나 도구 등에 대한 전문가의 도움을 필요로 한다.[24]

6) 네트워크 관련성

현재의 디지털 환경은 각각의 장치들이나 기기들이 독립적으로 움직이기도 하지만 서로 네트워크로 연결되어 있는 경우가 더 일반적이다. 네트워크는 일상생활의 수단이자 범죄의 수단이 되기도 한다. 따라서 디지털 증거를 수집하기 위해서는 네트워크를 통해야 하는 경우도 발생한다. 웹하드, 파일공유 네트워크, 클라우드 서비스 등으로 네트워크상에 대량의 정보가 저장, 공유되기도 한다.

---

22) 최성필, "디지털 증거의 증거능력에 관한 비교법적 연구", 국외훈련검사 연구논문집 제26집 (2011), 57

23) 양근원, "디지털 증거의 특징과 증거법상의 문제 고찰", 경희법학 제41권 제1호(2006. 6.), 183

24) 박혁수, "개정 형사소송법상 디지털 증거의 증거능력-관련성, 신뢰성, 진정성, 원본성을 중심으로", 해외연수검사 연구논문집 제25집(2010), 44

7) 익명성

일반 문서와는 달리 컴퓨터나 네트워크상에 있는 정보들은 작성자의 서명 등에 의한 확인이 불가능한 것이 대부분이다. 따라서 누구에 의하여 만들어진 정보인지 확인할 수 없어 증거능력을 인정받는 데에 어려움이 따르는 경우가 많다. 예컨대 전자우편의 경우 표면상 작성자(ID 소지자)가 실제로 해당 전자우편을 작성하여 보내지 않았을 가능성이 있고, 특히 사용된 컴퓨터가 소유자 개인뿐만 아니라 타인에 의하여 사용이 용이한 상태에 있는 경우에 타인이 해당 기기를 사용하여 작성한 정보이거나 타인의 아이디를 이용하여 인터넷 게시판에 명예훼손이나 음란물을 게재한 경우 등이 그러하다. 위와 같은 디지털 정보의 익명성은 증거법상 진정성의 문제로 연결된다.[25]

라. 디지털 증거의 증거능력 요건

1) 관련 논의의 개관

일반 증거와 관련된 증거법의 원칙들은 주로 유체물인 증거, 사람에 의한 진술증거 등을 상정하고 있다. 그런데 디지털 증거는 전술한 바와 같은 고유한 특성 때문에 다른 증거들과 달리 형사소송상 의미 있는 증거로 사용하기 위해 해결되어야 할 문제들이 발생하고, 이러한 문제가 해결되지 않으면 디지털 증거는 증거능력을 인정받을 수 없게 된다.[26]

---

25) 박혁수, "개정 형사소송법상 디지털 증거의 증거능력-관련성, 신뢰성, 진정성, 원본성을 중심으로", 해외연수검사 연구논문집 제25집(2010), 47-48

26) 장상귀, "디지털 증거의 증거능력에 관한 연구", 법학실무연구회(2009. 5.),

즉 디지털 증거의 취약성 및 매체 독립성, 수집과 분석의 어려움 등으로 말미암아 그 증거능력 판단에는 다른 증거와 구별되는 특성, 즉 무결성, 동일성, 신뢰성, 전문성 등이 거론된다. 각 특성 간의 관계를 살펴보면, 무결성과 동일성은 동전의 양면과 같아서, 어느 한 특성만을 언급하더라도 다른 특성까지 포함하는 것으로 볼 여지가 있다.[27]

디지털 증거의 증거능력 요건 또는 요소에 대한 견해는 다양한 스펙트럼을 보인다.[28] ① 동일성, 무결성은 사본 제출단계에서 증거능력의 요건일 뿐이고, 이후에는 진정성립, 신용성 등의 증거능력 요건을 인정하기 위한 사실요소로 기능하는 데 불과하며 그 자체로서 독자적 증거능력 요건이 되지 않는다는 견해,[29] ② 관련성(relevancy), 신뢰성(reliability), 진정성(authenticity), 원본성(original), 동일성, 무결성 등을 디지털 증거의 증거능력 인정을 위한 순차적인 관문으로 보는 견해,[30] ③ 무결성(authenticity), 신뢰성(reliability), 원본성(best evidence)의 문제가 해결되어야 한다는 견해,[31] ④ 증거능력의 요건으로 진정성(authenticity), 무결성(integrity), 신뢰성(reliability)을 드는 견해[32] 등을 들 수 있다.

---

233 ; 손지영·김주석, 디지털 증거의 증거능력 판단에 관한 연구, 사법정책연구원(2015), 30에서 재인용

27) 이숙연, "디지털 증거의 증거능력과 증거조사방안", 재판자료 제133집 형사법 실무연구Ⅱ(2016), 65

28) 이하 4가지 견해는 이숙연, "디지털 증거의 증거능력과 증거조사방안", 재판자료 제133집 형사법 실무연구Ⅱ(2016), 64에서 재인용

29) 오기두, "디지털 증거의 증거능력과 증거조사방안"에 대한 지정토론문, 코트넷 게시판

30) 박혁수, "개정 형사소송법상 디지털 증거의 증거능력", 해외연수검사연구논문집 2010(2), 25집

31) 김영기, "디지털 증거의 진정성립부인과 증거능력 부여 방안", 형사판례연구 19호(2011. 6.)

32) 오길영, "디지털검증의 현재와 그 부당성", 민주법학, 통권 48호(2012. 3.)

2) 디지털 증거에 특유한 증거능력 요건의 내용[33]

가) 동일성 내지 무결성(진정성)[34]

디지털 증거는 다른 증거와는 달리 앞서 본 변개의 용이성 내지 취약성으로 말미암아 최초 증거가 저장된 매체에서 법정에 제출되기까지 변경이나 훼손이 없었다는 점이 입증되어야 한다. 디지털 증거에 대한 수집·분석·보관·처리·법정제출 과정에서 많은 사람들의 행위가 개입되는데 이 경우 각 행위 시마다 원본 데이터의 무결성이 그대로 유지되고 있다는 절차적 보증이 필요하다.[35] 디지털 포렌식 과정에서도 자료의 무결성을 입증하기 위해 기술적인 방법들이 사용되어야 한다.

나) 진정성

진정성은 특정한 사람의 행위 결과가 정확히 표현되었고 그로 인해 생성된 자료인 것임이 인정되어야 한다는 것이고, 동일성 내지

---

33) 이하는 주로 손지영·김주석, 디지털 증거의 증거능력 판단에 관한 연구, 사법정책연구원(2015), 31-34를 발췌, 인용함

34) 이 용어는 미국 연방증거규칙(Federal Rules of Evidence) 제901조의 증거능력 인정 요건인 'Authenticating or Identifying'에서 비롯된 용어로 생각된다. 또는 디지털 포렌식 문헌에서 사용하는 'Integrity(of Evidence)'를 위와 같이 번역하기도 하는 듯하다. 그런데 위 Authentication 또는 Authenticity를 '진정성'으로 번역하거나, '진정 성립'으로 번역하는 등으로 용어 사용에 혼란이 있어 주의가 필요하다. 이른바 일심회 사건(대법원 2007. 12. 13. 선고 2007도7257 판결)과 왕재산 사건(대법원 2013. 7. 26. 선고 2013도2511 판결)에서는 동일성, 무결성을 사실상 같은 개념으로 사용하는 듯 보인다.

35) 권양섭, "디지털 증거수집에 관한 연구", 박사학위 논문, 군산대학교(2009), 114

무결성은 최초 증거가 생성되어 법정에 제출되기까지 변경이나 훼손이 없었다는 것을 의미한다고 하면서, 진정성은 압수한 디지털 증거의 수집과 보존까지를 다루는 문제이고, 무결성 내지 동일성은 디지털 증거의 수집과 보존을 포함하여 분석, 법정제출 등 전 과정에 걸친 문제로 파악되어야 한다고 보는 견해가 있다.[36]

이에 대해 디지털 증거의 경우 익명성과 대량성으로 인하여 작성자의 진정성에 문제가 제기되고 이에 대한 입증이 요구되는데, 이러한 진정성의 문제는 동일성의 문제 또는 원본성의 문제와도 관련이 있다고 보면서 "전자우편과 설계도면 파일을 주고받은 적은 있지만 압수된 전자우편과 설계도면 파일은 자신들이 보낸 것이 아니라는 주장은 진정성을 부인하는 취지이나 자신들이 실제로 보냈던 전자우편과 설계도면 파일이 불상의 방법으로 변경되었다는 주장으로서 동일성을 부인하는 취지이기도 하다. 그러나 이러한 측면의 '동일성 요건'을 진정성 요건에 포함시켜 검토하여도 무방하다고 본다. 진정성의 일부 부인 주장으로 볼 수도 있을 뿐만 아니라 무엇보다도 원본 데이터, 사본 데이터, 출력물의 내용이 완전히 일치해야 한다는 원래 의미의 동일성 요건과 혼동될 가능성이 있기 때문이다."[37]라고 하여 진정성 요건을 동일성 요건과 결부된 문제로 보는 견해도 있다.

나아가 이러한 주장은 외국의 법령, 판례 및 문헌의 번역에서 오는 혼란에서 초래되었다고 하면서, 진정성 문제는 사람의 행위가 개입된 증거에 관한 동일성·무결성의 문제로서 그에 포함되어 논의될 성질의 것이며, 우리 형사소송법에서 전문증거 예외를 인정하기 위한 요건인 성립의 진정 인정 문제(형사소송법 제312, 313조)와 사실상

---

36) 양근원, "디지털 증거의 특징과 증거법상의 문제 고찰", 경희법학 제41권 제1호(2006. 6.), 217

37) 박혁수, "개정 형사소송법상 디지털 증거의 증거능력-관련성, 신뢰성, 진정성, 원본성을 중심으로", 해외연수검사 연구논문집 제25집(2010), 77

같거나 유사하여 혼동을 초래할 수 있으므로, 동일성·무결성의 문제와 분리된 진정성의 개념을 별도로 인정하여 검토할 실익은 적다고 하는 견해[38]도 있다.

다) 신뢰성

디지털 증거는 위와 같이 변조가 용이하고 의도적, 비의도적 조작에 취약하므로 그 신뢰성이 보장되어야 할 필요가 있다. 신뢰성을 인정하기 위해서는 절차적으로 '보관의 연속성'을 보장하는 방법이 사용되어야 하고, 이와 관련하여 디지털 포렌식 전문가의 신뢰성과 디지털 포렌식 도구와 방법의 신뢰성이 요구된다.

대법원 2007. 12. 13. 선고 2007도7257 판결(소위 일심회 사건), 대법원 2013. 7. 26. 선고 2013도2511 판결(소위 왕재산 사건)에서 대법원은 디지털 증거의 동일성·무결성을 인정하기 위해서는 정보저장매체 원본과 '하드카피', '이미징'[39]한 매체 사이에 자료의 동일성과 아울러 이를 확인하는 과정에서 이용한 컴퓨터의 기계적 정확성, 프로그램의 신뢰성, 입력·처리·출력의 각 단계에서 조작자의 전문적인 기술능력과 정확성이 담보되어야 한다고 설시하고 있다.

현재 우리나라의 수사기관은 통합 포렌식 프로그램으로 미국에서 신뢰성이 입증된 'EnCase'를 주로 사용하고 있는 것으로 보인다. EnCase의 주요기능은 증거자료의 무결성 보장, 유연한 이미지 추출 방법 제공, 정확한 시간대 추적, 삭제된 파일, 폴더 및 비할당 클러

---

38) 손지영·김주석, 디지털 증거의 증거능력 판단에 관한 연구, 사법정책연구원 (2015), 32

39) '**하드카피**'란 특수장비(디스크 이미징 장비)를 이용하여 하드디스크를 물리적으로 그대로 복사하는 방법이고, '**이미징**'이란 소프트웨어를 이용하여 대상 하드디스크 전체를 하나의 파일 형태로 복사하는 방법을 말한다.

스터 영역 검색 및 복구, 컴퓨터 포렌식 결과 보고서 작성 등이다.[40] 디지털 증거를 분석하는 인력도 일정한 수준의 전문적인 지식을 갖추어야 하는데, 현재 검찰에서는 대검찰청 및 각 고등검찰청 또는 지방검찰청에 별도의 기구로 교육훈련 등 일정한 자격을 갖춘 디지털 포렌식 수사관으로 구성된 전담 팀을 설치하여 수사 일선에서 지원 요청을 받아 압수·수색, 분석, 현출, 기술적 자문, 법정 증언에 이르기까지 디지털 증거의 수집 및 분석과 관련된 수사 및 공소유지 업무의 전 과정에 참여하도록 하고 있다.[41]

라) 원본성

디지털 증거의 경우 원본과 사본을 구별하기 힘들고, 미국에서 이른바 '최량증거의 원칙(Best Evidence Rule)'으로 원칙적으로 원본에 의한 입증을 요구한 데에 따라 그 원본성 문제가 논의되고 있다. 그런데 미국 연방증거규칙[42] 제1001조 제3호는 "If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an original.(데이터가 컴퓨터 또는 동종의 기억장치에 축적되어 있는 경우에 가시성을 가지도록 출력된 인쇄물 또는 산출물로서 데이터의 내용을 정확히 반영하고 있다고 인정되는 것은 원본으로 본다.)"이라고 규정하고 있어 디지털 증거를 출력한 문건의 원본성을 입법적으로 인정하고 있다.

디지털 증거는 일반적 증거와 달리 유체물이 아닌 정보 그 자체를

---

40) 최성필, "디지털 증거의 증거능력에 관한 비교법적 연구", 국외훈련검사 연구논문집 제26집 (2011), 91

41) 디지털 증거 수집 및 분석 규정<대검예규 991호 2019. 5. 20. 시행> 제10조, 제11조

42) Federal Rules of Evidence, 미국 연방법원에 적용되는 성문법으로 연방증거법 혹은 연방증거규칙으로 번역된다.

의미하는 것으로 매체독립적이고 원본과 사본의 구분이 곤란한 특성을 지닌다. 디지털 증거는 원본의 완벽한 복제가 가능하기 때문에 특별한 사정이 없는 한 원본 데이터와 사본 데이터가 정확히 일치하고, 그 출력물도 완벽히 데이터와 등가를 이룬다.[43]

우리의 경우에도 2007년 개정된 형사소송법 제292조의3[44]과 그 위임을 받은 형사소송규칙이 제134조의7[45]로 컴퓨터용 디스크 등에 기억된 문자정보 등에 대한 증거조사 방법에 관한 규정을 신설함으로써 기존에 문제되었던 저장매체에서 출력된 문건의 원본성 문제를 입법적으로 해결하였다고 보이나, 원 저장매체에 있는 데이터를 다른 저장매체에 복사 또는 이전하는 방법으로 디지털 증거를 수집하는 경우 그 다른 저장매체를 원본으로 인정할 수 있는지의 문제에 대하여 우리 형사소송법이나 형사소송규칙은 아무런 언급을 하고 있지 않다. 이로 인하여 증거법의 일반원칙상 복사된 디지털 증거의 원본 문제는 여전히 논란이 될 수 있다고 보는 견해도 있다.[46]

3) 대법원 판례의 입장[47]

---

43) 박혁수, "개정 형사소송법상 디지털 증거의 증거능력-관련성, 신뢰성, 진정성, 원본성을 중심으로", 해외연수검사 연구논문집 제25집(2010), 77

44) 제292조의3(그 밖의 증거에 대한 조사방식) 도면·사진·녹음테이프·비디오테이프·컴퓨터용디스크, 그 밖에 정보를 담기 위하여 만들어진 물건으로서 문서가 아닌 증거의 조사에 관하여 필요한 사항은 대법원규칙으로 정한다.

45) 제134조의7(컴퓨터용디스크 등에 기억된 문자정보 등에 대한 증거조사) ① 컴퓨터용디스크 그 밖에 이와 비슷한 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.

46) 최성필, "디지털 증거의 증거능력에 관한 비교법적 연구", 국외훈련검사 연구논문집 제26집 (2011), 93

47) 이하는 손지영·김주석, 디지털 증거의 증거능력 판단에 관한 연구, 사법정책연구원(2015), 35-36을 주로 인용함

디지털 증거에 특유한 증거능력에 대하여 언급하고 있는 대표적 판례들은 '일심회 사건'(대법원 2007. 12. 13. 선고 2007도7257 판결), '왕재산 사건'(대법원 2013. 7. 26. 선고 2013도2511 판결)이다. 그 판시 내용에 나타난 디지털 증거의 증거능력을 부여하기 위한 요건을 정리해 보면 다음과 같다.

가) 동일성 내지 무결성의 요구

대법원은 2007. 12. 13. 선고 2007도7257 판결(일명 '일심회 사건')의 이유에서 "압수물인 디지털 저장매체로부터 출력한 문건을 증거로 사용하기 위해서는 디지털 저장매체 원본에 저장된 내용과 출력한 문건의 동일성이 인정되어야 할 것인데, 그 동일성을 인정하기 위해서는 디지털 저장매체 원본이 압수된 이후 문건 출력에 이르기까지 변경되지 않았음이 담보되어야 하고, 특히 디지털 저장매체 원본에 변화가 일어나는 것을 방지하기 위해 디지털 저장매체 원본을 대신하여 디지털 저장매체에 저장된 자료를 '하드카피'·'이미징'한 매체로부터 문건이 출력된 경우에는 디지털 저장매체 원본과 '하드카피'·'이미징'한 매체 사이에 자료의 동일성도 인정되어야 한다."라고 판시하였다. 디지털 증거의 동일성을 디지털 증거의 증거능력을 부여하기 위한 요건으로 꼽은 것이다. 대법원은 2013. 7. 26. 선고 2013도2511 판결(일명 '왕재산 사건')에서도 "압수물인 컴퓨터용 디스크 그 밖에 이와 비슷한 정보저장매체에 입력하여 기억된 문자정보 또는 그 출력물을 증거로 사용하기 위해서는 정보저장매체 원본에 저장된 내용과 출력 물건의 동일성이 인정되어야 하고, 이를 위해서는 정보저장매체 원본이 압수 시부터 문건 출력 시까지 변경되지 않았다는 사정, 즉 무결성이 담보되어야 한다."라고 하여 동일한 입장을 취하고 있고, '동일성'을 담보하기 위한 요건으로 '무

결성'이라는 용어를 사용하였다. 양자는 사실상 표리(表裏)의 관계에 있다고 보인다.

나) 신뢰성의 요구

위 대법원 판결들은 법원에 제출된 디지털 증거의 증거능력을 인정받기 위한 요건으로서 동일성 내지 무결성을 요구하고 이를 담보하기 위한 조건으로 다시 디지털 포렌식 전문가의 신뢰성과 디지털 포렌식 도구와 방법의 신뢰성을 요구하고 있다. 즉 "…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 동일성'도 인정되어야 할 뿐만 아니라, 이를 확인하는 과정에서 이용한 컴퓨터의 기계적 정확성, 프로그램의 신뢰성, 입력·처리·출력의 각 단계에서 조작자의 전문적인 기술능력과 정확성이 담보되어야 한다."(위 일심회 사건 판결)는 것이다. 이와 같은 판시는 왕재산 사건의 판결에서도 그대로 이어지고 있다.

그러나 디지털 포렌식 도구의 신뢰성과 관련하여 재판과정에서 프로그램 등의 신뢰성 자체가 본격적으로 문제가 된 사례는 아직까지 없는 것으로 보이고, 관여자들이 신뢰성을 인정받기 위해 갖추어야 할 전문성, 기술적 능력의 정도에 관해 본격적으로 판단한 사례도 보이지 않는다.[48)]

---

48) 장상귀, "디지털 증거의 증거능력에 관한 연구", 법학실무연구회(2009. 5.), 235-236; 최성필, "디지털 증거의 증거능력에 관한 비교법적 연구", 국외훈련검사 연구논문집 제26집 (2011), 91; 위 일심회 사건에서 대법원은 우리나라 수사기관에서 이미징 작업에 이용하는 'EnCase' 프로그램을 '세계적으로 인정받는 프로그램'이라고만 하고 있다. 위 사건의 제1심[서울중앙지방법원 2007. 4. 16. 선고 2006고합1365, 1363, 1364, 1366, 1367(각 병합) 판결]에서도 EnCase 프로그램이 '전 세계적으로 많이 사용되고 있다'는 점만을 언

다) 원본성의 요구

종래 우리나라에서 디지털 증거의 출력물을 원본으로 인정할 수 있는지에 대하여 여러 학설이 나뉘어 있었으나, 우리 형사소송법은 미국과 같이 최량증거원칙을 채택하고 있지 않으므로 디지털 증거의 원본성에 대하여 다툴 실익은 그다지 많지 않다고 본다.[49] 더구나 형사소송규칙은 제134조의7로 디지털 증거 중 문자정보에 관하여 이를 증거자료로 하는 경우에는 읽을 수 있도록 출력하여 인증한 등본을 낼 수 있다는 내용을 신설하였는바, 그 논의의 실익은 더욱 감소하였다고 할 것이다.

일심회 사건 및 왕재산 사건 판시 내용에서도 알 수 있듯이 대법원도 디지털 증거의 원본성 문제를 무결성·동일성의 문제와 분리하여 별도로 고찰하고 있지는 않고 있다. 여기에서 주목할 것은 위 판례의 내용을 자세히 보면 대법원이 '디지털 증거 자체의 증거능력'이 아니라 '그로부터 출력한 문건 등'에 관한 증거능력 인정요건을 판시하고 있다는 점이다.

> **압수물인 디지털 저장매체로부터 출력한 문건**을 증거로 사용하기 위해서는 **디지털 저장매체 원본에 저장된 내용**과 **출력한 문건**의 동일성이 인정되어야 하고, 이를 위해서는 디지털 저장매체 원본이 압수시부터 문건 출력시까지 변경되지 않았음이 담보되어야 한다. 특히 디지털 저장매체 원본을 대신하여 저장매체에 저장된 자료를 '하드카피' 또는 '이미징'한 매체로부터 출력한 문건의 경우에는

급하고 있다. 위 제1심판결에서는 위 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 설시하였다.

49) 장상귀, "디지털 증거의 증거능력에 관한 연구", 법학실무연구회(2009. 5.), 237

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 정확성**이 담보되어야 한다.(대법원 2007. 12. 13. 선고 2007도7257 판결)

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 출력 시까지 변경되지 않았음이 담보되어야 한다. 그리고 압수된 디지털 저장매체로부터 출력한 문건을 진술증거로 사용하는 경우, 그 기재 내용의 진실성에 관하여는 전문법칙이 적용되므로 형사소송법 제313조 제1항에 따라 공판준비나 공판기일에서의 그 작성자 또는 진술자의 진술에 의하여 그 성립의 진정함이 증명된 때에 한하여 이를 증거로 사용할 수 있다.(대법원 2013. 6. 13. 선고 2012도16001 판결)

3. 현재 수사 및 재판실무의 문제점

가. 문제상황 및 그 원인

앞서 본 대로 디지털 증거의 개념이 명확히 확립되지는 않았으나, 디지털 증거의 특성 - 특히 매체독립성, 원본과 사본의 구분 곤란, 변경의 용이성 내지 취약성 - 에 가장 부합하는 것은 형사소송법상 '증거방법' 측면이 아니라 '증거자료' 측면에서의 포착이라고 할 것이다. 즉 디지털 증거란 '0, 1로 이루어진 수의 배열정보 그 자체'라고 파악하는 것이 그 본질에 가장 부합한다.

그럼에도 앞서 본 대로 디지털 증거의 증거능력과 관련하여 일반적인 증거에서는 전혀 문제되지 않는 특유한 증거능력 인정요건이 요구되고, 대법원 판례에서 보듯 소송에서 '디지털 증거 그 자체'가 아닌 '디지털 저장매체로부터 출력한 문건'의 증거능력이 다투어지는 이유는, 수사 및 형사소송 실무상 디지털 증거 그 자체가 증거로 수집, 제출되지 않기 때문이다.

이러한 실무현황은 피압수자의 참여권 보장 문제에도 연결된다. 즉 대법원은 2015. 7. 16. 자 2011모1839 전원합의체 결정에서, "저장매체 자체 또는 적법하게 획득한 복제본을 탐색하여 혐의사실과 관련된 전자정보를 문서로 출력하거나 파일로 복제하는 일련의 과정 역시 전체적으로 하나의 영장에 기한 압수·수색의 일환에 해당한다."고 판시하였다. 나아가 그렇기 때문에 "검사가 압수·수색영장을 발부받아 갑 주식회사 빌딩 내 을의 사무실을 압수·수색하였는데, 저장매체에 범죄혐의와 관련된 정보(이하 '유관정보'라 한다)와 범죄혐의와 무관한 정보(이하 '무관정보'라 한다)가 혼재된 것으로 판단하여 갑 회사의 동의를 받아 저장매체를 수사기관 사무실로 반출

한 다음 을 측의 참여하에 저장매체에 저장된 전자정보파일 전부를 '이미징'의 방법으로 다른 저장매체로 복제(이하 '제1 처분'이라 한다)하고, 을 측의 참여 없이 이미징한 복제본을 외장 하드디스크에 재복제(이하 '**제2 처분**'이라 한다)하였으며, 을 측의 참여 없이 하드디스크에서 유관정보를 탐색하는 과정에서 갑 회사의 별건 범죄혐의와 관련된 전자정보 등 무관정보도 함께 출력(이하 '**제3 처분**'이라 한다)한 사안에서, 제1 처분은 위법하다고 볼 수 없으나, 제2·3 처분은 제1 처분 후 피압수·수색 당사자에게 계속적인 참여권을 보장하는 등의 조치가 이루어지지 아니한 채 유관정보는 물론 무관정보까지 재복제·출력한 것으로서 영장이 허용한 범위를 벗어나고 적법절차를 위반한 위법한 처분이며, 제2·3 처분에 해당하는 전자정보의 복제·출력 과정은 증거물을 획득하는 행위로서 압수·수색의 목적에 해당하는 중요한 과정인 점 등 위법의 중대성에 비추어 위 **영장에 기한 압수·수색이 전체적으로 취소되어야 한다**"고 판단하였다.

즉 실무상 디지털 증거 자체가 아닌 디지털 저장매체로부터 출력한 문건을 증거 수집의 대상으로 상정하여 압수·수색영장을 발부받고, 그 집행 과정에서 원본 저장매체에 저장된 정보를 이미징 방법으로 복제한 후, 그 복제한 저장매체 또는 재복제한 저장매체를 탐색, 분석하여 그 결과를 출력한 문건을 법원에 증거로 제출하기 때문에, 그 모든 과정에 피압수자의 참여권을 보장해야 하는 문제가 발생한다.

나. 본 연구의 제안내용

본 연구는 다음과 같은 3가지 개선방안을 제안한다.

첫째는 디지털 증거의 본질에 대한 실무관여자의 인식 전환이다.

즉 현재와 같이 '압수물인 디지털 저장매체로부터 출력한 문건 등'(= 증거방법으로서의 증거)을 증거로 수집·제출하는 것이 아니라, '0과 1이라는 디지털 형태의 정보 자체'(= 증거자료로서의 증거)를 증거로 수집하여 법정에 제출한다는 인식이다. 이 경우 디지털 형태의 정보인 파일 자체(1차 증거)와 이를 문서뷰어 등 프로그램으로 재현한 화면이나 문서(2차 증거)를 함께 제출하는데, 이는 예컨대 외국어나 기술부호로 기재된 문서(1차 증거)와 이를 번역 또는 감정한 결과(2차 증거)를 함께 제출하는 것에 비견될 수 있다.

둘째는 위와 같이 1차 증거로 제출하는 디지털 증거의 진정성을 확보하는 기술적 봉인기법의 개선 방안이다. 현재는 증거자료인 파일 자체에 대한 해시값을 산출하여 참여자에게 확인서를 교부하는데, 해시값의 산출 대상에 증거자료인 파일 외에 '객관적으로 검증 가능한 해당 파일의 수집시각'을 포함하는 것이다. 해당 파일의 수집시각을 공인된 방법으로 획득하여 해시 대상에 포함시키면 수집 현장에 참여자가 없더라도 해당 파일의 수집시각을 객관적으로 보장할 수 있다. 그 기술적 수단으로는 NTP 또는 TSA 방식을 고려할 수 있다.

셋째는 위와 같은 일련의 증거수집 및 분석 과정에 대한 신뢰를 확보하기 위하여, 파일 수집, 분석 및 시각 확인 등의 모든 절차를 수행하는 시스템을 가상머신으로 구현하고, 그 가상머신에서 이루어지는 모든 행위를 기록한 후, 가상머신 자체에 대한 해시값과 행위 기록에 대한 해시값을 산출하여 보존하는 것이다. 이로써 포렌식 조사 주체 및 조사 과정에 대한 신뢰를 확보할 수 있다. 아래에서 보다 상세히 살펴본다.

이러한 개선방안에 따를 경우 최초의 원본 저장매체에서 저장된 디지털 데이터를 수집하여 기술적 봉인조치를 마침으로써 증거의

수집 즉, 압수·수색영장의 집행이 완료된 것으로 보아, 더 이상 참여권의 문제는 발생하지 않는다. 나아가 위 봉인조치의 대상에 공인된 수집시각을 포함시키고, 이후 법정에 제출하기 위한 탐색, 분석 등의 과정에 대하여도 그 시스템 자체와 행위기록에 대한 해시값을 산출·보존함으로써 디지털 증거의 수집시각에 대한 논란, 조사 주체 및 과정에 대한 불신을 불식시킬 수 있을 것이다.

4. 증거조사 대상에 대한 인식 전환

가. 디지털 증거의 계층 구조

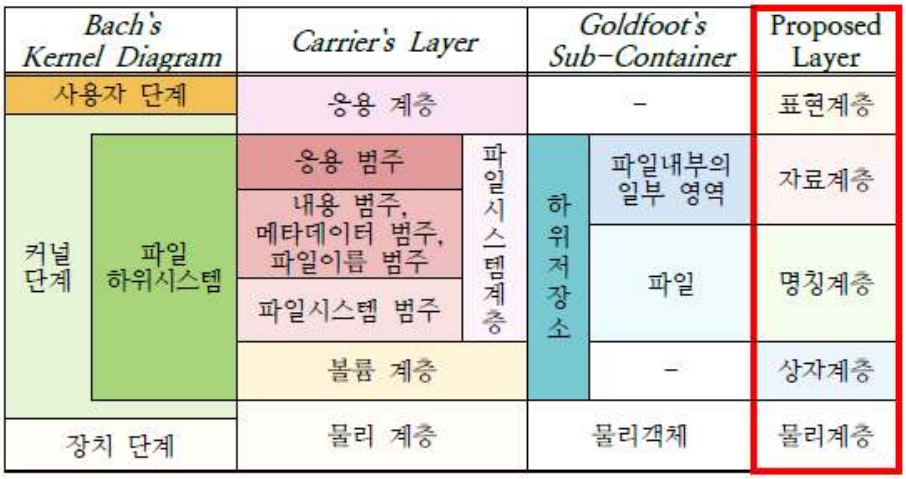
사법기관이 범죄 사실을 확인하기 위해 압수·수색을 할 때는 개인의 기본권보호 기대 수준과 사안의 경중에 따라 '압수·수색 대상'의 범위와 '압수 목적물'의 제한 요건을 비례적으로 판단하여 그 적절성을 검토하여야 한다. 우리 헌법은 모든 국민에게 인간으로서 존엄을 지키기 위한 기본권을 보장하고 있는 한편, 국가의 안녕을 위해 필요한 경우 법으로 정해진 범위에 한정하여 기본권을 제한할 수 있도록 하고 있다. 그러나 국가가 개인의 기본권을 제한하고자 할 때에도 필요한 한도에 그치도록 하여야 하며(침해의 최소성), 보호하고자 하는 공익과 침해되는 사익의 비교형량에서 보호되는 공익이 더 커야 하는(법익의 균형성) 원칙 즉, 과잉금지의 원칙을 유지해야 한다.

이러한 비례성 원칙은 디지털 증거에 대한 압수·수색에서도 예외가 될 수 없음에도 불구하고 디지털 증거에 대한 압수·수색 실무에서 사법기관은 압수·수색의 대상물을 '정보저장매체'로, 그 결과물은 '선별된 파일'로 획일화하여 접근하고 있다.[50]

원용기는 2016년 서울대학교 석사학위논문에서 디지털 증거의 계층구조에 관하여 Bach, Carrier, Goldfoot 등의 선행연구를 분석한 다음 이를 종합하여 아래와 같은 새로운 계층화를 제안한 바 있다.

---

50) 원용기, "디지털 증거에 대한 계층적 접근 방안 연구", 석사학위논문, 서울대학교(2016), 3; 원용기는 위 논문에서 디지털 증거를 객관적인 기준으로 계층화하고, 사안에 따라 비례적으로 판단하여 접근 계층을 제한하자고 제안한다.



[그림 2] 원용기가 제안하는 디지털 증거의 새로운 계층구조 5단계(Proposed Layer)

그의 설명에 의하면, '디지털 증거 계층구조'에서 최하위계층으로 이루어진 '**물리계층**Physical Layer'은 하드디스크나 메모리와 같은 주·보조기억 장치나 네트워크카드 장치 등과 같이 물리매체의 성격을 그대로 갖고 있는 계층을 말한다. 이 계층의 증거는 전통적 증거들과 동일한 성격을 갖는다.

다음으로 물리매체 위에 디지털정보를 기록하기 위한 체계 공간인 '**상자계층**Container Layer'이 있다. C드라이브나 D드라이브와 같은 볼륨과 파일시스템이 여기 속한다. Carrier`s Layer에서의 '볼륨계층'과 '파일시스템 계층'의 '파일시스템 범주' 중 파일시스템 구조에 관한 사항 즉, 파일시스템 메타정보가 여기 해당된다. 또한 기능과 역할에 비추어 볼 때 메모리 안에서는 '페이지Page', 네트워크 장치에서는 '프로토콜Protocol'을 같은 계층으로 볼 수 있다.

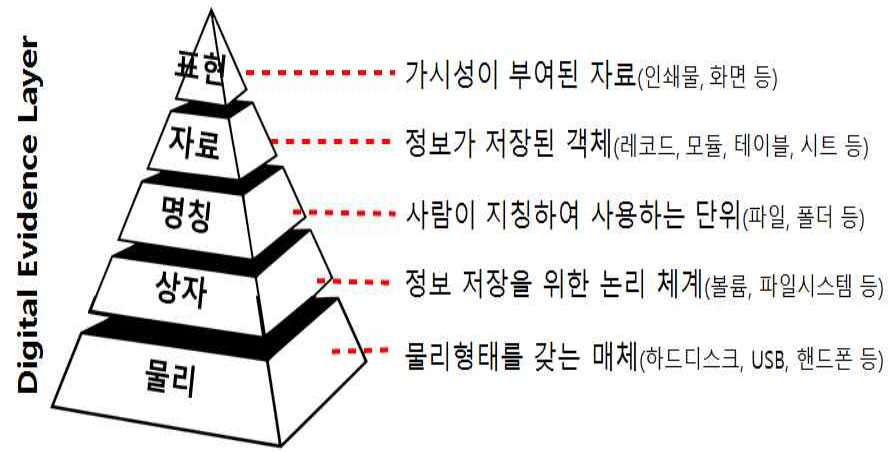
'**명칭계층**Named Layer'은 파일이나 폴더와 같이 논리적으로 연관성 있는 정보를 묶고 고유의 이름을 붙여 접근하는 계층으로 일반적으로 가장 많이 접하는 계층이다. Carrier`s Layer의 '파일시스템

계층'에서 '파일시스템 범주' 중 파일과 연계된 정보인 '파일이름 범주', '메타데이터 범주'가 이에 해당된다. 매체에 저장된 파일이 메모리로 이동하면 프로세스를 통해 접근 가능하고 네트워크로 연결된 파일은 Uniform Resource Identifier(URI)를 통해 접근이 가능하므로 이들 역시 명칭계층으로 볼 수 있다. 또한, 일반적으로 접근이 제한된 파일이나 영역도 사람이 논리적으로 지명할 수 있는 방법이 있다면, 역시 명칭계층으로 다룰 수 있다. 예를 들어 파일시스템을 전문적인 방법으로 열람할 경우 '$MFT, Unallocated Clusters, Alternate Data Streams'와 같은 정보를 찾아 볼 수 있는데 이 영역도 증거로서 가치 있는 경우가 많이 있다.

'**자료계층**Data Layer'은 데이터베이스의 특정 테이블이나 엑셀파일의 특정 행과 같이 명칭계층 내부에 저장된 정보 및 객체들을 내부 구조에 따라 접근하는 단위이다. 하나 혹은 다수의 명칭계층을 특정 기준에 따라 나누어 접근하는 것이 가능할 때 그 영역의 일부를 자료계층으로 본다. Carrier`s Layer에서는 '파일시스템 계층' 중 파일의 실제 내용이 저장된 '내용 범주'와 운영체제에서 사용하기 위한 정보가 저장된 '응용 범주'가 여기 해당된다. 메모리 영역에서는 Virtual Address Descriptor(VAD)가 여기 속한다. 명칭계층에 포함된 정보가 그 특성으로 인해 관련성 없는 정보의 혼재가 명백하고, 이에 관한 접근이 반드시 제한되어야 할 상황이나 단일 파일의 복제로는 그 정보의 가치가 훼손되는 사안에서 유효하게 참조할 수 있다. 또한, 데이터베이스에 저장된 정보와 같이 분산 저장된 정보를 의미에 따라 구성하여 추출할 필요가 있을 경우도 증거 가치 재고를 위하여 이 계층 단위로 접근하는 것이 합리적이다.

마지막 계층은 저장된 정보를 사람에게 의미 있는 형태로 변환하여 표현하는 단계인 '**표현계층**Rendering'이다. Carrier`s Layer에서 '응용 계층'과 응용프로그램 상위 단계에서 표현되는 모든 형태를

말한다. 디지털정보는 비가시적인 특성으로 인하여 같은 값이라도 응용프로그램이나 설정에 따라 표현 결과가 달라지고, 그로 인해 정보가치에 영향을 끼칠 가능성이 많기 때문에 이를 고려한 접근이 필요하다. 특히 물리적 장치이나 응용프로그램과 매체에 저장된 정보가 상호 의존적으로 존재하여 복제 후 정보가치를 보존할 수 없거나 기술적·정책적인 이유로 정보의 복제가 제한되는 경우 표현계층 단위로 접근할 필요가 있다. 표현계층은 그 특성상 디지털정보의 수집 과정이 아닌 제출과정에서 가장 효과적으로 참조할 수 있는 계층이다. 문서파일의 인쇄물, 모니터에 출력된 사내 업무 시스템 전용 전자결재 문서 등이 표현계층 단위의 디지털 증거이다.[51]



[그림 3] 원용기의 디지털 증거 계층구조

원용기는 계층화된 디지털 증거는 사용자가 정보에 이르는 접근성에 따라 물리계층을 최하위 계층, 표현계층을 최상위 계층으로 볼 수 있고, 하위계층은 '상위계층의 내용'과 '상위계층의 정보를 설명하는 메타데이터'를 포함하는 피라미드식 구조를 갖는다면서, 비례

51) 원용기, "디지털 증거에 대한 계층적 접근 방안 연구", 석사학위논문, 서울대학교(2016), 17-19

성 원칙에 따라 정보저장매체에 저장된 정보민감도가 높을수록, 요증사실이 경미할수록 디지털 증거 계층구조의 상위계층에 접근하고, 저장된 정보 민감도가 낮을수록, 요증사실이 엄중할수록 디지털 증거 계층구조의 하위계층에 접근하는 방식으로 압수·수색의 대상을 조정하는 것이 합리적이라고 제안한다.[52]

원용기의 연구는 디지털 증거의 계층구조에 착안하여 압수, 수색의 대상을 조정하고 제한하자는 것으로서 헌법상 기본권 보장과 실체진실 발견의 조화를 지향하는 매우 합리적인 제안이라고 생각된다.

다만 수사 및 재판실무에 비추어 볼 때, 이러한 제안이 실현되기 위해서는 수사기관의 압수·수색영장 청구를 심사하여 그 발부 여부를 결정하는 법관들이 이러한 디지털 증거의 계층구조를 이해해야만 가능한 일인데, 현실적으로 쉽지 않은 일이다. 우리나라 일선 수사관의 업무량이나 기본적으로 범죄진실 탐구가 수사기관의 우선적 임무라는 점을 고려할 때, 수사기관이 스스로 사안에 따라 디지털 증거의 압수·수색 대상을 제한하여 영장을 청구하기를 기대하기 어렵고, 일단 발부된 아무런 제한 없는 압수·수색영장을 집행하면서 자의적 판단에 따라 그 대상을 제한하는 것도 바람직하지 않다.
결국 압수·수색의 발부 또는 제한 여부를 판단하는 법관들이 구체적 사안에 따라 비례의 원칙에 맞는 범위에서 결정하여야 할 텐데, 현실적으로 가까운 장래에 실현하기는 어려울 것이다.

현재의 실무 여건에서는 디지털 증거의 물리계층(하드디스크, usb, 휴대전화 등)이나 상자계층(볼륨 등)을 압수·수색을 통해 확보한 후 이를 탐색, 분석하여 증거가치 있는 정보를 추출한 다음 그 정보를 표현계층(인쇄물, 화면 등)의 형태로 법원에 증거로 제출하는 상황

52) 원용기, "디지털 증거에 대한 계층적 접근 방안 연구", 석사학위논문, 서울대학교(2016), 21, 23

이 장기간 지속될 것으로 보인다.

문제는 이러한 일련의 과정을 거치는 동안 증거가치 있는 해당 정보(‘증거자료’에 해당)가 담긴 저장매체가 바뀔 때마나 피압수자의 참여권 보장 여부가 문제되고, 법정에 최종 제출된 표현계층(‘증거방법’에 해당)의 동일성, 무결성 문제가 대두된다는 것이다.

나. 증거방법이 아닌 증거자료 자체에 대한 조사 방안

이에 본 연구는 증거방법이 아닌 증거자료를 법원에 증거로 제출하는 방안을 제안한다. 원용기의 계층구조를 빌리자면 표현계층이 아니라 상자계층이나 명칭계층에 들어있는 binary code 자체를 말한다.

즉, 압수·수색의 집행과정에서 물리계층 또는 상자계층을 최초로 확보한 후 그로부터 증거가치 있는 디지털 데이터인 binary code를 수집하는 순간에 다음 장에서 살펴보는 것처럼 ‘객관적으로 공인된 수집시각’을 포함하여 해시값을 산출, 보존한 다음 해당 binary code 자체를 usb 등에 담아 법정에 증거로 제출하는 것이다. binary code 자체의 동일성과 무결성을 보장하는 한 이를 담는 매체가 무엇이든 증거능력에는 아무런 영향을 미치지 못한다(디지털 증거의 매체독립성).

다만 앞서 본 대로 디지털 증거는 2진수의 신호체계로 되어 있어 그 자체로는 보통 사람의 육안으로 인식할 수 없다(디지털 증거의 비가시성). 이러한 binary code가 증거로 제출되면 법관의 입장에서는 마치 곧바로 해독할 수 없는 외국어나 기술부호로 된 정보가 제출된 것과 마찬가지의 상황이다.

이러한 경우에 대비하여 우리 형사소송법은 통역과 번역이라는 수단을 마련해 두고 있다. 즉 국어에 통하지 아니하는 자의 진술에는 통역인으로 하여금 통역하게 하여야 하고(형사소송법 제180조), 농자 또는 아자의 진술에는 통역인으로 하여금 통역하게 할 수 있으며(같은 법 제181조), 국어 아닌 문자 또는 부호는 번역하게 하여야 한다(같은 법 제182조).

법관이 직접 지득하기 어려운 외국어나 수어 또는 외국의 문자나 부호는 번역 등을 통하여 인식하므로, 디지털 증거로 제출된 binary code에 대하여도 통·번역에 관한 규정을 준용하여 이를 해독할 수 있는 응용프로그램으로 표시한 문서를 함께 제출하도록 할 수 있다.

실제로 우리 형사소송법과 그로부터 위임을 받은 형사소송규칙은 컴퓨터용디스크 그 밖에 이와 비슷한 정보저장매체에 기억된 문자정보나 도면, 사진 등을 증거자료로 하는 경우에는 읽거나 인식할 수 있도록 출력하여 인증한 등본을 낼 수 있다고 규정하고 있다.

형사소송법

제292조(증거서류에 대한 조사방식) ①검사, 피고인 또는 변호인의 신청에 따라 증거서류를 조사하는 때에는 신청인이 이를 낭독하여야 한다.

제292조의2(증거물에 대한 조사방식) ①검사, 피고인 또는 변호인의 신청에 따라 증거물을 조사하는 때에는 신청인이 이를 제시하여야 한다.

제292조의3(그 밖의 증거에 대한 조사방식)

도면·사진·녹음테이프·비디오테이프·컴퓨터용디스크, 그 밖에 정보를 담기 위하여 만들어진 물건으로서 문서가 아닌 증거의 조사에 관하여 필요한 사항은 대법원규칙으로 정한다. [본조신설 2007. 6. 1.]

형사소송규칙

제134조의7(컴퓨터용디스크 등에 기억된 문자정보 등에 대한 증거조사)

① 컴퓨터용디스크 그 밖에 이와 비슷한 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.

② 컴퓨터디스크 등에 기억된 문자정보를 증거로 하는 경우에 증거조사를 신청한 당사자는 법원이 명하거나 상대방이 요구한 때에는 컴퓨터디스크 등에 입력한 사람과 입력한 일시, 출력한 사람과 출력한 일시를 밝혀야 한다.

③ 컴퓨터디스크 등에 기억된 정보가 도면·사진 등에 관한 것인 때에는 제1항과 제2항의 규정을 준용한다.

[본조신설 2007. 10. 29.]

즉, 위 규정을 자세히 보면, 컴퓨터디스크 등에 기억된 (문자, 도면, 사진 등에 관한) **정보**를 증거자료로 하는 경우라고 하여, 디지털 증거인 binary code 자체를 증거로 제출하는 경우를 상정하고 있다고 해석된다. 나아가 출력한 인증등본을 낼 수 있다는 규정을 반대로 해석하면 출력한 인증등본 없이 binary code 자체만을 증거로 내는 경우도 당연히 예정하고 있는 것이다.

위 규정에 관한 실무지침서의 설명내용은 다음과 같다.[53]

① 컴퓨터용 디스크 등의 조사방법

컴퓨터용 디스크 그 밖에 이와 비슷한 정보저장매체(이하 '컴퓨터디스크 등'이라 한다)에 기억된 문자정보를 증거자료로 하는 경우에는 읽을 수 있도록 출력하여 인증한 등본을 낼 수 있다(규 134조의7 제1항). 이는 컴퓨터디스크 등의 특성을 감안하여 이에 기억된 내용을 증거자료로 하는 경우에 그 내용을 출력한 출력문서를 내도록 함으로써 증거조사에 편의를 도모할 수 있도록 한 것이다.

그러나 문자정보가 기억된 컴퓨터디스크 등에 대한 증거조사방법으로서 그 출력문서를 제출하는 것은 출력문서 자체를 증거서류로 제출하는 것과는 구별된다. 전자의 경우에는 증거방법은 여전히 '컴퓨터디스크 등'임에 반하여, 후자의 경우에는 '출력문서' 자체가 증거방법이 되므로 증거서류에 해당한다. 따라서 전자의 방법으로 증거조사를 한 경우에

53) 법원실무제요 형사[Ⅱ] 196-197

는 증거서류 등 목록이 아닌 증인 등 목록에 컴퓨터디스크 등의 증거조사 사실을 기재한다. 그 경우 신청인이 제출한 출력문서는 공판기록(신청인이 검사인 경우에는 증거기록)에 편철하고, 컴퓨터디스크 등의 증거조사를 실시한 연·월·일·시를 증거조사기일란에 기재한 뒤 비고란에 "인증등본제출"이라고 추가 기재하고 출력문서가 편철된 기록의 쪽수를 괄호 안에 표시한다.

컴퓨터디스크 등에 기억된 문자정보에 대한 증거조사를 신청한 당사자는 법원이 명하거나 상대방이 요구하는 때에는 컴퓨터디스크 등에 입력한 사람과 입력한 일시, 출력한 사람과 출력한 일시를 밝혀야 한다(규 134조의7 제2항). 이는 출력문서의 진정성립과 내용의 정확성을 담보하고 이에 관하여 다툼이 생기는 경우에 증인으로 신문하거나 감정에 필요한 정보를 제공하도록 하기 위한 것이다.

한편 위와 같은 증거조사방법은 컴퓨터디스크 등에 기억된 정보가 도면·사진 등에 관한 것인 때에도 준용된다(같은 조 3항).

이에 따르면 ① 문자정보가 기억된 컴퓨터디스크 등에 대한 증거조사방법으로서 그 출력문서를 제출하는 것과 ② 출력문서 자체를 증거서류로 제출하는 것은 명확히 구분됨을 알 수 있다. 현재 실무상으로는 ②의 방법이 대종을 이루는바, 이는 디지털 증거의 본질이나 특성, 그 계층구조에 대한 법조 종사자들의 인식 부족에 기인하는바, 필자는 그 인식전환을 통해 ①의 방법을 주된 증거조사방법으로 삼을 수 있다고 제안하는 것이다.

"디지털 증거의 본질은 디지털이다.
출력문서가 아니라 binary code 자체를 증거로 제출하라."

5. 기술적 봉인기법의 개선

가. 현재의 실무현황

실무상 국내 수사기관에서는 디지털 증거의 무결성을 증명하기 위한 지침을 마련하고 다음과 같은 절차를 시행하도록 하고 있다.

즉 “① 하드디스크 등의 저장매체를 압수한 다음 피의자의 서명을 받아 봉인한다. ② 서명, 봉인과정을 비디오카메라로 녹화한다. ③ 피의자가 입회한 가운데 봉인을 풀고, 통합 포렌식 프로그램인 인케이스(EnCase)를 이용하여 압수한 저장매체에 대한 이미지 파일을 생성한 후 별도의 저장장치에 이미지 파일을 저장한 다음, 이미지 파일을 이용하여 복구 등의 분석 작업을 실시한다. ④ 쓰기방지장치(Fastblock)를 압수한 저장매체에 연결한 상태에서 이미지 파일 생성 작업을 실시하고, 이미지 파일에 대한 해시(Hash) 값[54]을 계산하여 피의자로 하여금 해시값이 기재된 서면에 서명·날인케 한다. ⑤ 피의자가 공판과정에 무결성을 부정하는 경우에는 압수한 저장장치의 해시값과 이미지 파일의 해시값을 비교할 수 있도록 법원에 검증을 요구한다.”라고 한다.[55]

---

54) 해시값은 해시함수의 결과로 만들어진 코드이다. 무결성 입증 방법은 수학적 해시함수를 이용한 원본과 사본의 결과 값을 비교하는 방법이 가장 일반적이라고 하며, 해시함수의 특성상 입력 데이터가 한 bit라도 변경되면 다른 결과 값이 출력되므로, 쉽게 변조가 되는 디지털 데이터라도 무결성을 입증할 수 있다고 한다. 무결성이 보장되기 위해서는 원본 디스크의 해시값, 원본 디스크 이미지의 해시값, 사본 디스크 이미지의 해시값, 사본 이미지의 해시값이 모두 동일하여야 한다고 한다.

55) 김영기, "디지털 증거의 진정성립 부인과 증거능력 부여방안", 형사판례연구 제19호(2011), 516-517; 최성필, "디지털 증거의 증거능력에 관한 비교법적 연구", 국외훈련검사 연구논문집 제26집 (2011), 90; 하기봉, "디지털 포렌식에 의한 디지털 증거의 증거능력", 석사학위 논문, 성균관대학교 국가전

이와 관련한 대검찰청의 관련 예규는 아래와 같다. 이 예규 제18조 제2항의 별지 제2호 '현장조사확인서' 양식은 별지로 첨부하였다.

디지털 증거 수집 및 분석 규정<대검예규 991호 2019. 5. 20. 시행>

제18조 (디지털 증거의 압수·수색·검증)

① 압수의 목적물이 정보저장매체 등인 경우에는 기억된 정보의 범위를 정하여 출력하거나 복제하여 압수하여야 한다. 다만, 범위를 정하여 출력 또는 복제하는 방법이 불가능하거나 압수의 목적을 달성하기에 현저히 곤란하다고 인정되는 경우 또는 피압수자 등의 동의가 있는 경우에는 정보저장매체 등을 압수하거나 정보저장매체 등에 기억된 전자정보 전부를 복제할 수 있다.

② 사건과 관련성이 있는 정보를 수색하여 디지털 증거를 압수하는 경우에는 해시값(Hash Value)을 생성하고 별지 제2호 서식의 "**현장조사확인서**"를 작성하여 확인·서명을 받거나 다음 각 호의 내용이 포함된 확인서를 작성하여 피압수자 등의 확인·서명을 받아야 한다. 이 경우, 확인서는 디지털포렌식 도구에 의해 자동 생성된 자료로 갈음할 수 있다.

1. 확인서 작성일시 및 장소
2. 정보저장매체 등의 종류 및 사용자
3. 해시값, 해시함수
4. 확인자의 인적사항 및 연락처, 확인자와 피압수자와의 관계
5. 기타 진정성·무결성·신뢰성을 확인하는데 필요한 사항

제19조 (확인서 인계 및 전자정보상세목록 교부)

① 디지털포렌식 수사관은 피압수자 등이 작성한 각종 확인서를 주임검사 등에게 인계하여 압수목록 작성, 참여기회 보장 등 후속 절차 진행에 참고할 수 있도록 한다.

② 디지털포렌식 수사관은 디지털포렌식 압수·수색·검증이 종료되면 압수한 **파일의 상세목록**을 작성하여 피압수자 등에게 교부하여야 한다. 다만, 다음 각 호와 같이 상세목록 작성이 곤란한 경우는 예외로 한다.

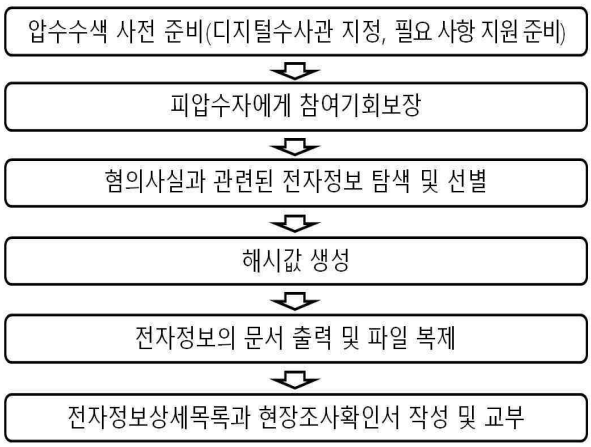
1. 범위를 정하여 출력 또는 복제하는 방법이 불가능하여 정보저장매체 등을 압수한 경우

략 대학원(2012), 89; 손지영·김주석, 디지털 증거의 증거능력 판단에 관한 연구, 사법정책연구원(2015), 31-32에서 재인용

2. 정보저장매체에 저장된 전자정보를 파일 단위로 온전하게 압수할 수 없는 경우
③제2항에 따른 상세목록의 교부는 서면의 형태로 교부하는 방법 이외에 파일의 형태로 복사해주거나 전자메일로 전송하는 등의 방법으로 갈음할 수 있다.

위 예규에 따른 집행절차는 (1) 현장에서의 파일 선별이 가능한 경우와 (2) 불가능한 경우가 달리 정해져 있다.

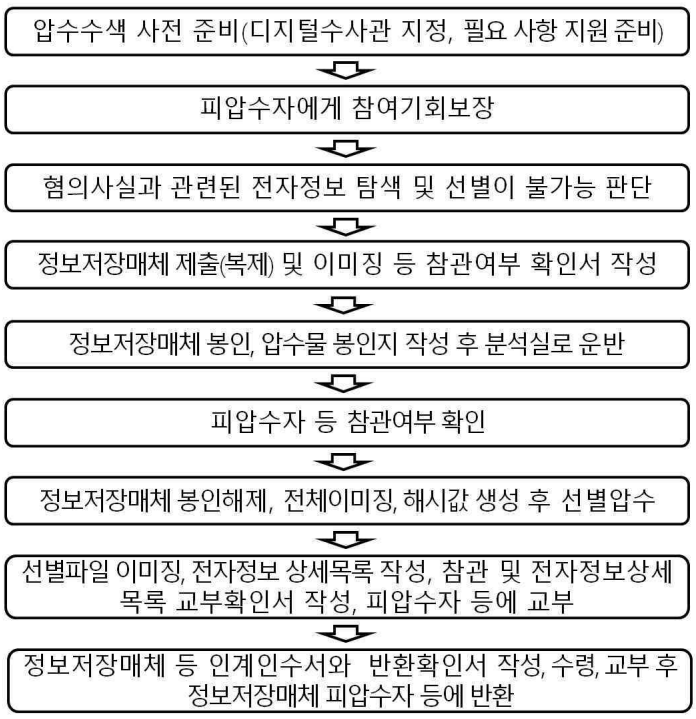
즉 (1) 원칙적으로는 ① 압수·수색 사전 준비(디지털 수사관 지정, 필요한 사항 지원준비) → ② 피압수자에게 참여기회 보장 → ③ 압수현장에서 저장매체 수색 후 혐의사실과 관련된 전자정보 탐색 및 선별 → ④ 압수할 전자정보의 해시값 생성 → ⑤ 전자정보의 문서 출력 및 파일 복제 → ⑥ 전자정보상세목록과 현장조사확인서 작성 및 교부로 압수·수색 집행이 종료된다.[56]



[그림 4] 디지털 증거의 압수수색 과정(현장에서 선별 가능한 경우)

56) 김종빈, "전자정보를 대상으로 한 압수수색검증영장의 효율적인 집행방법에 대한 연구", 석사학위논문, 서울대학교(2020), 19

(2) 예외적으로 압수·수색 현장에서 선별이 불가능한 경우에는, ① 압수·수색 사전 준비(디지털 수사관 지정, 필요한 사항 지원준비) → ② 피압수자에게 참여기회 보장 → ③ 압수현장에서 저장매체 수색 후 혐의사실과 관련된 전자정보 탐색 및 선별이 불가능 판단 → ④ 정보저장매체 제출(복제) 및 이미징 등 참관여부 확인서 작성 → ⑤ 정보저장매체 봉인, 압수물 봉인지 작성 후 분석실로 운반 → ⑥ 피압수자 등 참관여부 확인 → ⑦ 정보저장매체 봉인해제, 전체이미징, 해시값 생성 후 선별압수 → ⑧ 선별파일 이미징, 전자정보 상세목록 작성, 참관 및 전자정보상세목록 교부확인서 작성, 피압수자 등에 교부 → ⑨ 정보저장매체 등 인계인수서와 반환확인서 작성, 수령, 교부 후 정보저장매체 피압수자 등에 반환으로 압수·수색 집행이 종료된다.[57]



[그림 5] 디지털 증거의 압수수색 과정(현장선별 불가능한 경우)

57) 김종빈, "전자정보를 대상으로 한 압수수색검증영장의 효율적인 집행방법

현장조사확인서 및 압수목록 관련 구체적 절차를 보면, '현장조사보고서'에 생성한 이미지 파일에 대한 해시값 등을 기재하고 피압수자 또는 참여인으로부터 확인을 받아 2부를 사본한다. 그중 사본 1부는 피압수자에게 교부하고 다른 사본 1부는 디지털 포렌식 수사관이 보관하며, 원본은 수사팀 수사관에게 인계한다. 수사팀 수사관은 인계 받은 '현장조사보고서'의 내용을 참조하여 압수목록을 작성해 피압수자에게 교부한다고 한다.[58]

즉 현재 실무상 디지털 증거의 무결성을 보장하는 가장 핵심적인 장치는 원본 저장매체로부터 복제한 이미지 파일에 대한 해시값을 산출하여 피압수자 등으로부터 현장에서 확인을 받는 것이다.

나. 해시 함수의 활용과 그 한계

이하 해시(Hash) 함수 또는 해시(Hash) 알고리즘에 관하여 조금 더 살펴본다. 해시(Hash) 알고리즘은 데이터 무결성 및 메시지 인증 등에서 사용할 수 있는 함수로서 임의의 길이 bit열[59]을 고정된 길이의 출력값인 해시 코드로 압축시키는 함수이다.[60] 해시함수의 결과를 해시값, 메시지 다이제스트, 메시지 지문 등으로 칭하는데 위와 같은 이름에서 알 수 있듯이 임의의 길이의 메시지를 대신 대

에 대한 연구", 석사학위논문, 서울대학교(2020), 19, 20

58) 박소연, "디지털 증거물의 수집 및 보관과정에서 접근제한 확보방안", 석사학위논문, 서울대학교(2016), 26

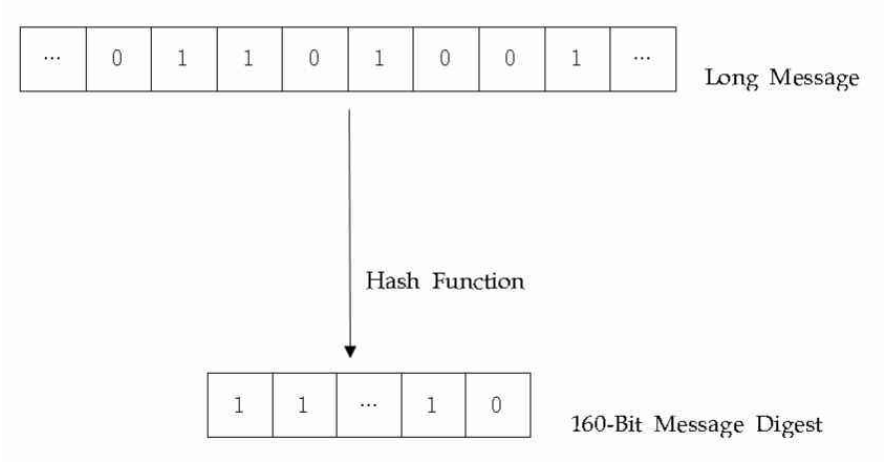
59) bit란 Binary digit의 약자로서 데이터 구성의 최소단위이다. 수학적으로는 0과 1로 표현한다. 박상준, 디지털포렌식 강의자료Ⅱ, 서울대학교(2020), 289

60) 탁희성·이상진, 디지털 증거분석 도구에 의한 증거수집절차 및 증거능력 확보방안, 한국형사정책연구원(2006), 143; 이상미, "관련성 없는 디지털 증거 삭제시 이중해쉬를 이용한 무결성 입증 방안", 석사학위논문, 서울대학교(2016), 12에서 재인용

표할 수 있는 고정된 길이의 값을 계산하여 주는 함수를 말한다.

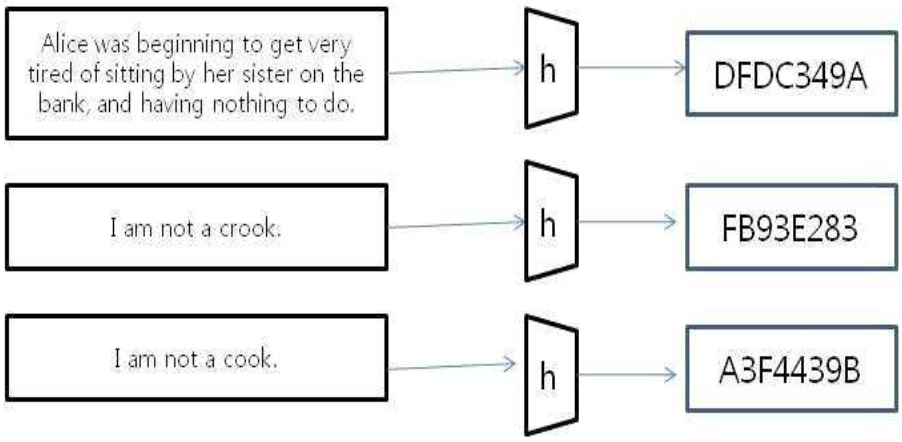
컴퓨터가 인간생활의 여러 국면에 더욱 폭넓고 깊게 관여하게 됨에 따라 프로그램이나 데이터의 송수신 및 저장을 안전하고 완벽하게 통제해야 함에 있어서 요구되는 사항은 데이터에 대한 공격을 찾아내는 일일 것이다. 해시함수의 사용이 시작된 것은 인가받은 자 또는 인가받지 않은 자로부터 또는 여하한 형태의 공격으로부터 야기된 데이터 상의 변화를 찾아야 하는 필요성으로부터 시작되었다고 한다.

따라서 해시함수는 MDC(manipulation detection code), finger print 등으로 일컫는 경우도 있다.[61] 해시 함수의 기본적인 개념과 입·출력 원리를 도해하면 다음 그림과 같다.



[그림 6] 해시 함수의 개념

61) 황석근·조한혁, "디지탈 서명과 해쉬 함수", 정보보호학회지 제2권 제1호 (1992. 3.), 23: 이상미, "관련성 없는 디지털 증거 삭제시 이중해쉬를 이용한 무결성 입증 방안", 석사학위논문, 서울대학교(2016), 12에서 재인용



[그림 7] 해시 함수의 입·출력 원리

※ [그림 6]의 출처[62], [그림 7]의 출처[63]

문제는 현재 실무상 해시값의 산출 대상 즉, 해시 함수의 입력인자는 수사기관이 수집하려는 디지털 데이터 자체만이라는 점이다. 따라서 원본 저장매체의 내용 전체를 하나의 파일로 이미징한 경우는 그 이미지 파일 전체에 대한 해시값을 산출하고, 이후 그 이미지 파일을 탐색, 분석하여 유의미한 데이터 파일을 찾은 후 이를 증거로

62) Wade Trappe & Lawrence C. Washington, Introduction to Cryptography with Coding Theory, Pearson(2013), 219. Figure 8.1.; 이상미, "관련성 없는 디지털 증거 삭제시 이중해쉬를 이용한 무결성 입증 방안", 석사학위논문, 서울대학교(2016), 13에서 재인용

63) 크리스토프 파르 · 얀 펠즐(원동호·이영숙·김지연 공역), 「암호기술의 이해」, 도서출판 그린(2013), 397, 그림 11.3.; 해쉬함수의 입-출력 특성은 임의의 크기의 메시지 x에 해쉬 함수를 적용할 수 있으며, 함수 h는 계산적으로 효율적이고, 그 출력은 고정된 길이로서 입력 길이에 독립적이라는 점이다. 또한, 계산된 값(message digest)은 입력 비트에 민감해서 입력 x를 약간 변경하더라도 출력은 완전히 다르다. 위 그림은 이러한 특성을 잘 보여준다(크리스토프 파르 · 얀 펠즐, 앞의 책,; 이상미, "관련성 없는 디지털 증거 삭제시 이중해쉬를 이용한 무결성 입증 방안", 석사학위논문, 서울대학교(2016), 13에서 재인용

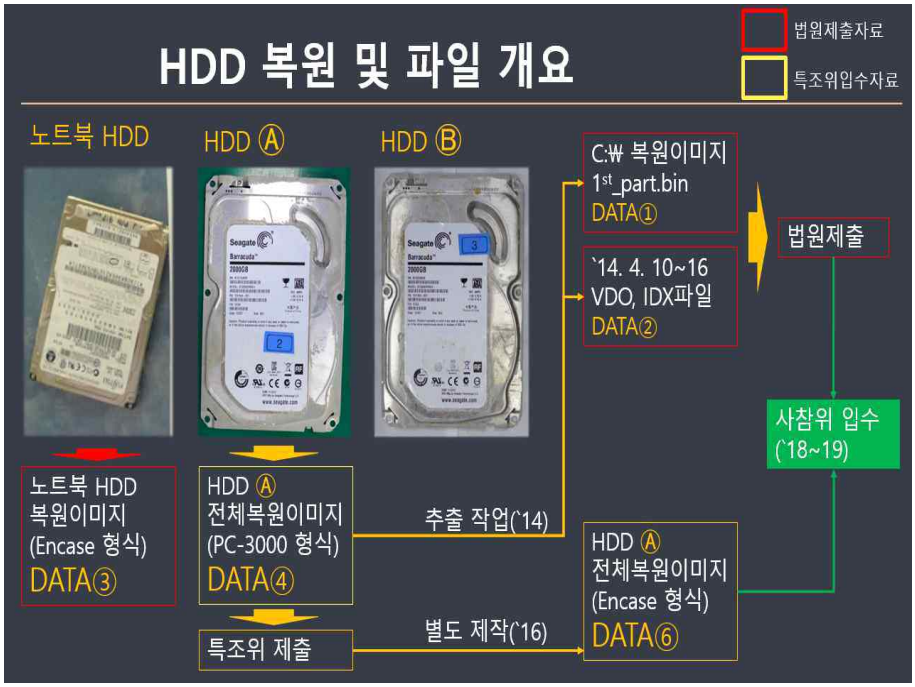
다시 획득하려 할 때 해당 데이터 파일에 대한 해시값을 산출하는 것이다.

앞서 본 디지털 증거 수집 및 분석 규정<대검예규 991호 2019. 5. 20. 시행> 등이 상정하고 있는 정상적인 상황 즉, 디지털 증거의 수집현장에 피압수자 등이 참여하고 있을 때에는 해당 이미지 파일이나 데이터 파일에 대한 해시값을 산출하여 이를 기재한 현장조사 확인서에 피압수자 등의 서명, 날인을 받게 되므로 별다른 문제가 없다.

그러나 그 수집현장에 피압수자가 참여할 수 없는 상황이거나 또는 해당 디지털 데이터를 예컨대 인터넷 서비스 제공자(ISP) 등이 관리하고 있고, 그 데이터의 정보주체는 제3자인 경우 등 정보주체가 정보관리자를 신뢰하지 못하는 경우 등에는 정보주체인 제3자가 사후에 해당 디지털 증거의 수집시각 등에 대하여 이의를 제기한다면 이를 기술적·객관적으로 검증하기 어렵다.

최근 논란이 되는 세월호 선체의 CCTV 복원 동영상이 그 대표적인 예다.

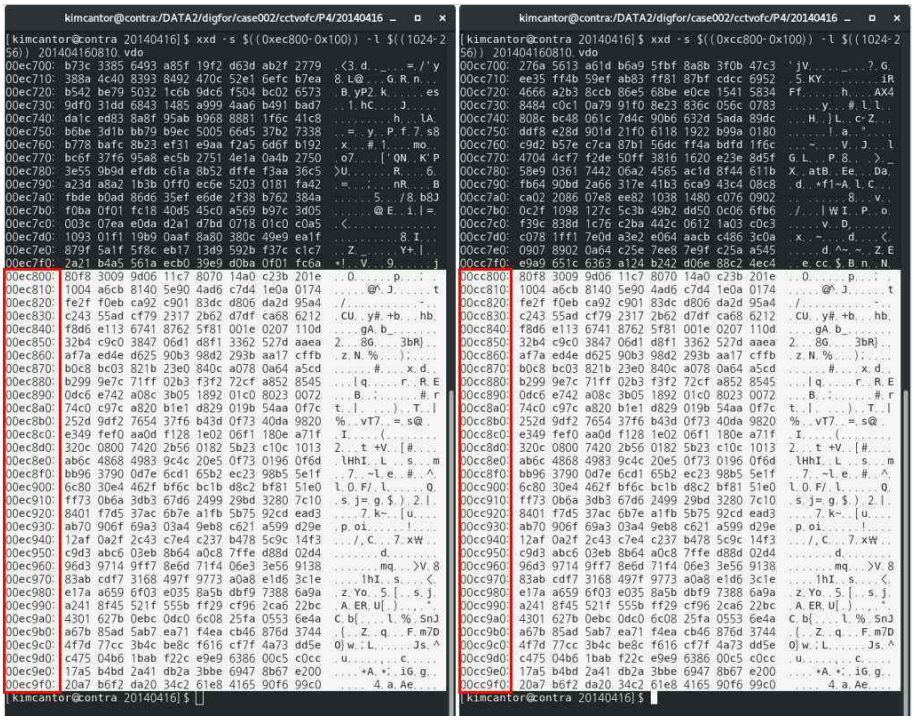
사회적 참사 특별조사위원회(이하 '사참위'라 한다)는 2020. 9. 22. 보도자료를 통하여 "세월호 안에는 64개의 CCTV가 설치되어 있었고 그 영상 저장장치인 DVR(digital video recorder)은 항공기의 블랙박스와 같아 사고 발생 시 바로 수거되었다면 사고 원인은 물론 구조를 기다리던 승객들의 마지막 동선을 쉽게 파악할 수 있었을 것임. 사참위(위원장: 장완익)는 세월호 CCTV 영상 조작의혹을 조사한 결과, 참사 당시 법원에 제출된 CCTV 복원 영상파일이 조작되었다는 사실을 확인하였고, DVR 본체 수거과정 조작에 대한 증거를 추가 확보함에 따라 국회에 특별검사 임명을 요청할 예정"이라고 밝혔다.



[그림 8] 세월호 CCTV 자료의 종류(사참위 2020. 9. 22.자 보도자료 2쪽)

사참위에 따르면, 광주지방법원 목포지원에 제출된 '2014. 4. 10.~16.의 영상파일'(위 그림의 DATA②)을 분석한 결과 18,353곳에서 주변부와 동일한 내용의 섹터가 식별되었고, 이는 엉뚱한 주변 섹터의 데이터가 복사된 후 덮어쓰기(overwriting) 되는 바람에 해당 섹터들의 영상 재생 시 에러가 발생하는 것으로 확인되었다고 한다. 덮어쓰기에 사용된 소스(Source) 데이터와 에러가 발생하는 데이터 사이의 간격에 임의의 규칙성이 발견되며, 덮어쓰기 된 데이터는 동영상파일임에도 MPEG-4 규격에 부적합한 것으로 누구든 식별 가능하다고 한다.

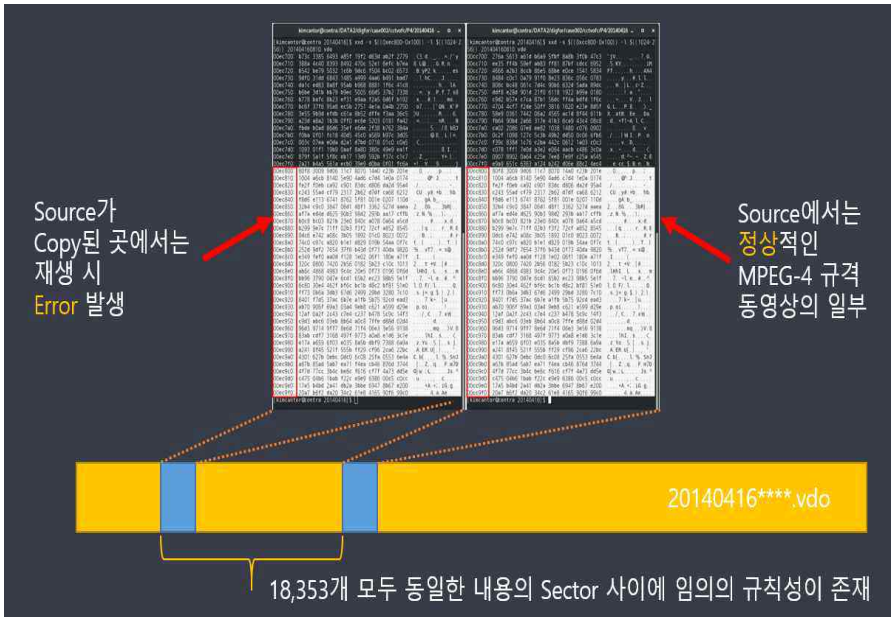
(여백)



[그림 9] 법원에 제출된 영상파일(201404160810.vdo)에서 식별되는 사례(사참위 2020. 9. 22.자 보도자료 3쪽)

- 섹터번호 3099503185(클러스터 번호 EC800)와 동일한 내용으로 채워져 있는 같은 파일 내 섹터번호 3099015920(클러스터번호 CC800).
- 우측 부분은 MPEG-4 규격에 적합하여 에러없이 재생되는 반면, 좌측 부분은 동일 파일임에도 MPEG-4 규격에 부적합하여 재생 시 에러 발생. 따라서, 우측 부분이 좌측 부분에 덮어 씌어진 Source 데이터임. 이러한 동일 사례가 법원에 제출된 영상파일 중에서 18,353군데 식별됨.

(여백)



[그림 10] 복사 후 덮어쓰기(overwrite)가 발생한 곳이 총 18,353섹터로 특히 4.15~16 사이에 74% 집중됨

나아가 사참위는 DVR 본체 수거과정 특히 수거일시가 허위로 조작된 것으로 판단하였다고 밝혔다.

그 근거로 ① '세월호 DVR'의 뒷면이 4개의 커넥터에 의해 강하게 결속된 상태였기 때문에 '세월호 DVR'은 당초 설치되었던 장소에서 커넥터와 분리된 채 이격된 곳에서 발견될 수 없으나, DVR이 설치 장소에서 1m를 훨씬 넘는 이격된 장소에서 영상에 포착된 점, ② 해당 영상을 분석한 결과 수중 40m 깊이에서 노출된 DVR 왼쪽 손잡이 바깥면에 부착되어 있던 고무 패킹이 압착되어 있지 않고 원래 부착되어 있던 상태를 그대로 유지하고 있음이 확인되는 점, ③ 2014. 5. 9. 작성된 것으로 추정되는 해경 "현장지휘본부 문서 정리 현황" 중 63번 항목의 "DVR 인양후 인수인계 내역" 공문서 제목이 확보된 점을 들고 있다. 즉 당초 해군이 밝혀왔던 수거시점보다 한 달 이상 앞선다는 주장이다.

실제 세월호 관련 형사재판에서 '세월호 선내 CCTV 화질개선 동영상 DVD'가 증거로 제출되어 조사되었고, 법원은 이를 근거로 출항 당시 세월호에 화물이 적치된 상황에 대한 사실인정을 하였다.[64]

해당 재판부는 나중에 재판의 경과를 정리한 백서를 발간하였는데, 그중 위 CCTV 관련 부분은 다음와 같다.

"선장 및 선원들에 대한 재판이 진행되는 도중에 세월호의 선실에 설치되어 있던 CCTV 저장매체가 인양되었고, 유가족들이 광주지방법원 목포지원에 신청한 증거보전 절차에 따라 확보된 동영상이 증거로 제시되었다. 유가족들은 세월호 선내 CCTV로 촬영한 동영상에 의하여 세월호가 전복된 직후의 상황에 대하여 규명이 될 것으로 기대하였으나, 세월호가 전복되기 직전까지의 상황만 촬영되어 있었기 때문에 검찰은 세월호가 출항한 후 전복될 때까지 항간에서 제기되는 이상상황이 없었다는 사실을 입증하기 위하여 위 동영상에 대한 증거조사를 신청하였고, 재판부는 동영상의 주요 부분을 재생하는 방식으로 CCTV 동영상에 대한 증거조사를 실시하였다."[65]

즉 2014년 재판 당시 법원에 증거로 제출되어 조사된 CCTV 동영상이 재판부의 사고 원인 판단에 일정한 영향('출항 후 전복시까지 이상상황이 없었다는 소극사실의 증거자료')을 미쳤는바, 2020년도에 사참위라는 공적 기구에 의해 그 CCTV 동영상의 최초 수거시점과 그 내용이 조작된 것이라는 의혹이 제기된 것이다.

이 사건에서도 2014년도에 CCTV 동영상을 복원, 분석하면서 원본

64) 광주지방법원 2014. 11. 11. 선고 2014고합180 등 판결 36쪽, 61쪽
65) 광주지방법원 형사 제11, 13부, 세월호 사고 관련 제1심재판 백서(2014), 코트넷(법원 내부 게시판) 게재, 50쪽

저장매체로부터 최초로 이미지 파일을 복제하면서 해시값을 산출하였을 터인데, 그 해시값은 CCTV 동영상 데이터 자체만을 해시 함수에 입력하여 산출된 값으로 여겨진다.[66] 이러한 논란을 객관적, 기술적으로 방지할 수 있는 수단은 무엇일까?

다. 개선방안

필자는 이 문제에 대한 대안으로 디지털 증거를 수집하는 시각에 대한 객관적인 정보를 기술적으로 보존하는 방안을 제안한다. 즉 디지털 데이터에 대한 해시값 외에 해당 데이터를 수집하는 시각을 획득하여, “디지털 데이터 + 수집시각”을 해시 함수에 입력하여 최종 해시값을 산출, 보존하는 것이다.

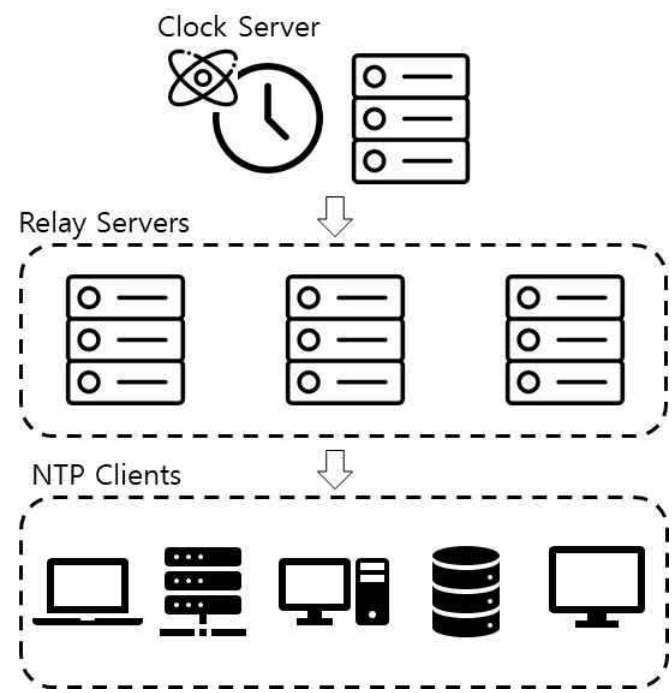
그렇다면 객관적으로 검증 가능한 수집시각을 어떻게 획득할 것인가. 필자는 NTP와 TSA 두 가지 방법을 제시한다.

먼저, 수집시각을 특정하는 방법으로 네트워크상의 시간 동기화를 위한 공용 NTP(Network Time Protocol) 서버들과 수집 환경 간의 시간 차이를 조회하는 방법이 있다. NTP는 아래 그림과 같이 계층적으로 구성되어 상위 계층으로부터 시간을 동기화한다.
NTP의 최상위 계층(Primary Reference Clock)에는 세슘원자시계 수준의 정확도를 보장하며 시간을 하위 계층에 제공한다. 공공 NTP 서버는 높은 보안 수준을 갖추고 있어 특정 개인이나 기관이 악의적으로 위변조하기 매우 힘들고 설령 하나의 공공 NTP 서버가 위, 변조되었다고 하더라도 올바르게 동작하는 다른 공공 NTP 서버들

66) 명확한 자료를 확인할 수 없으나, 해당 CCTV 영상 데이터를 최초 수집한 시각을 객관적으로 보장할 수 있는 데이터는 보존되지 않은 것으로 추측할 수 있다.

에서 조회한 정보와 교차 검증하여 이를 바로 잡을 수 있다.

또한, 암호화 통신하에서 공개키 암호기반 인증서를 교환하여 서버의 신원이 인증되므로 NTP 서버로 위장하여 조작된 시간을 보내는 것은 불가능(infeasible)하다. 따라서 공공 NTP서버에 접속하여 암호화 프로토콜의 Hand-Shake 단계에서 교환하는 인증서를 확인하여 신뢰할 수 있는 기관임을 검증할 수 있다.



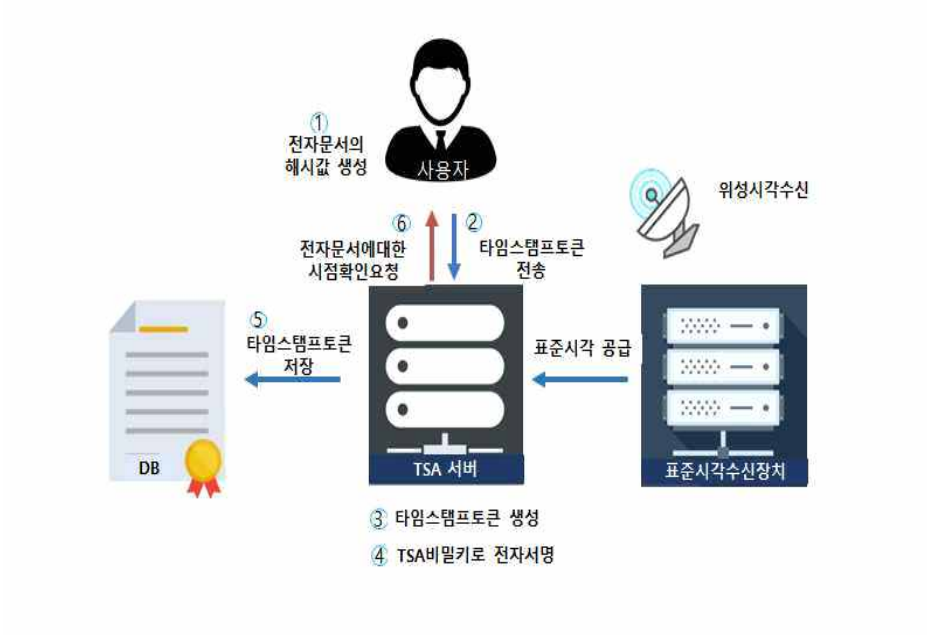
[그림 11] NTP의 시간 동기화 구조

이 방법의 안전성은 전자서명과 인증서에 적용된 암호 알고리즘의 안전성에 의존한다. 이로써 신뢰할 수 있는 시간 조회 수단을 얻게 되며 이 서버와 수집 환경의 시간 차이를 조회함으로써 수집의 시점을 특정할 수 있다.[67]

67) 서강윤, "원격지 디지털 증거 수집을 위한 프레임워크", 고려대학교 정보보호연구원 디지털포렌식연구센터(2019), 6-7; 서강윤은 이 논문에서 '원격지 시스템으로부터 디지털 증거를 수집하는 경우' 수집 대상과 연결된 네트워

다음으로 TSA(Time Stamp Authority)에 관하여 살펴본다.

TSA는 전자문서의 데이터에 대해 인증기관이 표준시각정보를 포함하여 전사서명한 타임스탬프를 제공하는 서비스이다.[68] 전자문서의 위·변조 용이성 및 비가시성 등의 특성을 극복하기 위해 특정 시점에 해당 전자문서의 존재 여부를 시점확인서비스를 통해 확인이 가능하다. 이는 현재 금융결제원에서 제공하는 서비스로 인터넷뱅킹, 전자상거래, 병원의료차트 등에 사용되고 있다.



[그림 12] TSA 흐름도

크의 신뢰성 확보 수단으로 위 NTP 시각 조회방안을 제안하고 있다. 필자는 원격지에 소재하여 필수적으로 네트워크를 통한 수집이 필요한 경우에 한정할 것이 아니라, 원격지가 아닌 일반적인 디지털 증거 수집현장에서도 수집시각 획득이 필요한 경우 이러한 수단을 활용할 수 있음을 주장한다.

68) 금융결제원 전자인증센터 부가서비스 시점확인서비스(Time Stamping Authority) https://www.yessign.or.kr/additionalservice/subIndex/353.do

TSA는 사용자가 전자문서의 해쉬값을 생성하여 전자문서에 대한 시점 확인을 요청하면 TSA서버는 타임스템프토큰을 생성하여 TSA 인증서의 비밀키로 전자서명하여 별도의 DB에 타임스탬프토큰을 저장한다. 생성 저장된 타임스탬프 토큰은 사용자에게 전송되어 무결성이 입증되고, 그 과정에서 표준시각수신장치는 위성으로 시각을 수신 받아 TSA서버에 표준시각을 공급한다.

이로써 디지털 증거의 수집시각을 명확화하기 위한 기술적 활용방안으로서 TSA를 활용할 수 있는 것이다.[69]

이러한 NTP 또는 TSA를 이용하여 디지털 증거를 수집할 때 그 수집시각을 객관적으로 확인하고, 이를 해시 함수의 입력인자에 포함하여 해시값을 산출하여 보존하면 사후에 디지털 증거의 수집시각에 대한 논란이 발생할 소지를 원천적으로 예방할 수 있다.

이때 위와 같이 수집시각을 획득하는 시스템 자체에 대한 신뢰성 보장도 필요하다. 즉 NTP나 TSA를 이용하여 수집시각을 획득하는 과정에서 또는 그 시간 값을 해시하는 과정에서 값이 변조되는 문제가 있을 수 있으므로, 이러한 문제를 기술적으로 완벽하게 해결하려면 해당 해시 연산과정을 수행하는 모든 디바이스(device)가 신뢰 가능한 디바이스여야 한다. 다음 장에서 좀 더 상세히 살펴본다.

“모두에게 공개된 정보는 누구도 변조할 수 없다.”

---

69) 이정인, "디지털 증거의 관리연속성(Chain of Custody)과 적법절차의 원리에 관한 연구", 석사학위논문, 서울대학교(2019), 75-76; 이정인은 위 논문에서 일단 수사기관에 수집된 이후 디지털 증거의 이동 경로 및 접근시간을 명확히 하여 관리연속성을 확보하는 방안으로 TSA를 제안하고 있다. 반면, 필자는 디지털 증거의 최초 수집 당시에, 그 수집시각을 객관적으로 획득, 보존하여 사후에 검증할 수 있는 수단으로 이를 제안한다.

6. 포렌식 조사 주체 및 과정에 대한 신뢰 확보

가. 현재 실무현황과 문제점

위 세월호 CCTV 동영상 사례에서 보듯이, 국가기관에 대한 피해자들의 불신이 심각할 경우 포렌식 조사를 거쳐 제출된 디지털 증거의 내용 자체에 대하여도 의혹이 제기될 수 있다.

이에 대한 대비책으로 디지털 증거에 대한 해시값을 산출하여 확인하는 제도가 있으나, 세월호 사례와 같이 디지털 증거의 최초 수집현장에 피압수자 등 이해관계인이 참여할 수 없거나 혹은 고의로 참여시키지 않은 경우에는 이러한 논란에 객관적으로 대처할 수 없다.

나. 개선방안

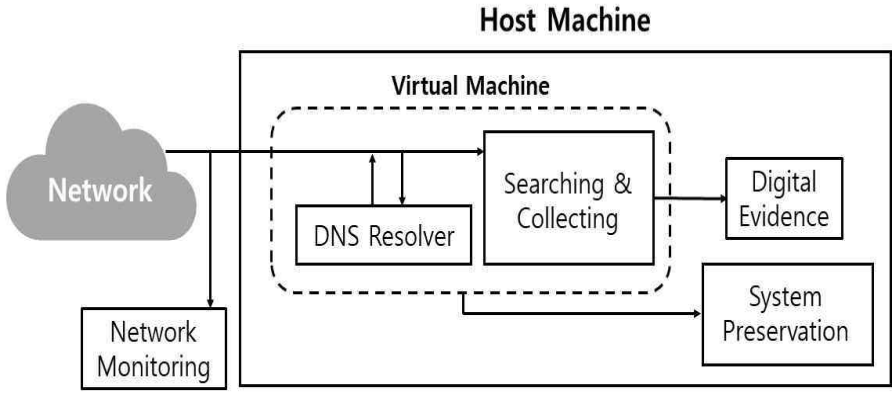
이런 상황에 대비하여 포렌식 조사의 시스템이나 조사 과정을 사후에 검증할 수 있는 프로토콜을 마련할 필요가 있다.

서강윤은, 원격지에 있는 디지털 증거를 네트워크를 통해 수집하는 경우에 수집 시스템의 신뢰성을 보장하는 방안으로서 가상머신으로 구현한 시스템을 제안하였다.
즉 “먼저, 운영체제 구동을 위한 시스템 파일과 편의를 위해 운영체제와 함께 설치되는 응용프로그램만이 존재하는 가상환경을 구축한다. 이때 설치하는 운영체제 또한 사후에 검증할 수 있도록 설치에 사용된 파일과 버전 정보, 설치 파일의 해시값을 기록하여 보관

한다. (중략)

다음으로, 행위기록 시스템을 구축한다. 이로써 앞으로 발생하는 프로세스 실행, 프로그램 설치, 파일의 입출력, 네트워크 접속 등의 일련의 활동을 재현할 수 있게 됨으로써 사후 사용자의 행위를 검증할 수 있다.

마지막으로, 수집된 증거의 신뢰성을 보이고 수집 대상과의 네트워크 접속의 신뢰성을 보이기 위해 네트워크 트래픽 모니터링 및 수집 도구를 설치한다. 패킷 수집 도구는 수집 시스템의 영향을 받지 않은 네트워크를 통해 수신된 그대로를 수집하기 위해 네트워크 인터페이스에서 직접 수집한다."는 것이다.[70]



[그림 13] 서강윤이 제안한 원격지의 디지털 증거 수집 프레임워크

위 제안은, 원본 저장매체를 보존하기 어려운 원격지의 디지털 증거를 네트워크를 통해 수집하는 경우에 수집 시스템의 신뢰성을 보장하려는 방안인데, 필자는 이를 원격지의 디지털 증거를 수집하는 경우로 한정할 필요가 없다는 입장이다.

피해자 또는 피고인 측도 국가기관에 대한 불신이 극심한 때에는

70) 서강윤, "원격지 디지털 증거 수집을 위한 프레임워크", 고려대학교 정보보호연구원 디지털포렌식연구센터(2019), 6

수사기관의 모든 발표에 의혹을 제기할 수 있다. 따라서 증거 수집부터 탐색, 분석, 추출 등 포렌식 조사의 모든 과정의 행위를 기록하고, 나아가 그 조사시스템 자체를 가상머신으로 구현하여 그 행위 기록과 가상머신 자체에 대한 기술적 봉인 즉 해시값을 산출하여 보존해 놓으면, 언제든지 사후 검증이 가능하다. 서강윤의 설명처럼 포렌식 조사 시스템을 가상으로 구현할 경우 사후검증뿐 아니라 포렌식 조사 과정에서의 효율성이나 시스템 유지비용 등에서도 이점이 있을 수 있다.[71]

또한 앞 장에서 본 것처럼 NTP나 TSA를 이용하여 디지털 증거의 수집시각을 획득하는 시스템도 위와 같은 방법으로 포렌식 조사시스템의 일부로서 가상머신으로 구현할 것을 제안하는 것이다.

이로써 피해자나 피고인 또는 어떤 이해관계자라도 법정에 제출된 디지털 증거의 수집시각이나 최초 수집부터 법정 제출까지의 조사, 분석 과정에 대하여 이의를 제기할 경우 법정에서 동일한 과정을 재현해 보임으로써 수집시각뿐 아니라 디지털 증거의 내용 자체도 진정한 것임을 객관적으로 검증할 수 있다.

“포렌식은 과학이다.
디지털 증거의 진정성은 과학적 수단으로 입증하라”

---

71) 서강윤에 따르면, ① 기존의 전문가의 도움을 받아 해결했던 수집 과정의 신뢰성 보장을 기술적으로 해결할 수 있고, ② 원격에 있는 데이터는 조사자의 통제 밖에 있어 긴급한 수집이 요구되는데 이런 수집 환경이 미리 갖추어져 있다면 신속한 대응도 가능하며, ③ 제시한 프레임워크는 수집 환경을 가상화하여 동시에 여러 대상에 대한 수집과 반복 수집이 가능하고, ④ 이 프레임워크는 디지털포렌식 조사 프로세스 모델의 일부로서 이용하도록 고안함으로써 기존의 디지털포렌식 조사솔루션 또는 도구에 하나의 모듈로 포함시킬 수 있다. 서강윤, "원격지 디지털 증거 수집을 위한 프레임워크", 고려대학교 정보보호연구원 디지털포렌식연구센터(2019), 10

7. 결론

이상으로 디지털 증거의 개념과 특성, 그리고 본질을 탐구하고, 그 본질에 가장 어울리는 증거조사 방안으로서 현재의 실무처럼 증거방법(디지털 증거를 출력한 문서 등, 이른바 '표현계층')이 아니라 증거자료 자체(binary code)를 법정에 증거로 제출하여 조사하는 방안을 검토하였다.

나아가 디지털 증거의 수집현장에 피압수자 등이 참여하지 않거나 참여할 수 없는 경우에도 그 증거자료의 동일성과 무결성 등을 보장하기 위해 현재와 같이 해시 함수에 디지털 증거 자체만 입력하는 것이 아니라 '객관적으로 공인된 수집시각'까지 입력하여 해시값을 산출하는 방안을 제안하고, 나아가 조사 주체와 과정에 대한 신뢰성 확보를 위해 포렌식 조사 시스템(수집시각 획득 시스템 포함) 자체와 모든 행위기록에 대한 기술적 봉인(해시값 산출, 보존)을 제안하였다.

우리나라는 현재 수사와 재판, 형 집행 등 전(全) 형사사법절차의 전자화를 적극 추진하고 있다. 보도자료에 따르면, 정부는 2024년 완료를 목표로 사건관계인이 기관에 직접 가지 않고 컴퓨터 등을 이용해 서류와 증거자료를 제출할 수 있고, 전자서명된 조서 등 각종 서류가 전산망을 통해 작성·유통되며, 재판에서는 각종 조서나 스캔된 증거자료를 법정 내 스크린에 띄워 함께 내용을 보면서 변론과 증인신문을 하는 전자법정을 형사소송에서도 실현할 수 있도록 추진 중이다.[72]

---

72) "형사사법절차도 전부 전자화… 2024년 완료 목표", 법률신문 홈페이지, 2020-08-13자

이러한 형사전자소송에서는 필자가 제안한 ‘증거자료인 binary code 자체에 대한 증거조사’ 방안이 지금보다 훨씬 수월하게 실현될 수 있다.

[참고문헌]

□ 국내 단행본

박상준, 디지털포렌식 강의자료Ⅱ, 서울대학교(2020)

배종대·이상돈, 형사소송법 제2판, 홍문사(1997)

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

탁희성·이상진, 디지털 증거분석 도구에 의한 증거수집절차 및 증거능력 확보방안, 한국형사정책연구원(2006)

크리스토프 파르 · 얀 펠즐(원동호·이영숙·김지연 공역), 암호기술의 이해, 도서출판 그린(2013)

법원실무제요 형사[Ⅱ]

광주지방법원 형사 제11·13부, 세월호 사고 관련 제1심재판 백서(2014)

□ 국내 논문

권양섭, “디지털 증거수집에 관한 연구”, 박사학위 논문, 군산대학교(2009)

김방글, “삭제 후 복구된 디지털 파일의 증거능력 인정 요건에 관한 연구”, 석사학위 논문, 서울대학교(2020)

김영기, “디지털 증거의 진정성립부인과 증거능력 부여 방안”, 형사판례연구 19호(2011. 6.)

김종빈, “전자정보를 대상으로 한 압수수색검증영장의 효율적인 집행방법에 대한 연구”, 석사학위논문, 서울대학교(2020)

노명선, “전자적 증거의 수집과 증거능력에 관한 몇 가지 검토”, 형사법의 신동향 제16호 (2008)

박소연, “디지털 증거물의 수집 및 보관과정에서 접근제한 확보방안”, 석사학위논문, 서울대학교(2016)

박혁수, “개정 형사소송법상 디지털 증거의 증거능력-관련성, 신뢰

성, 진정성, 원본성을 중심으로", 해외연수검사 연구논문집 제25집(2010)
서강윤, "원격지 디지털 증거 수집을 위한 프레임워크", 고려대학교 정보보호연구원 디지털포렌식연구센터(2019)
송희식, "증거법이론에 있어서 인식과 진술-증거법 일반이론의 모색-", 형사법의 신동향 통권 39호(2013)
양근원, "디지털 증거의 특징과 증거법상의 문제 고찰", 경희법학 제41권 제1호(2006. 6.)
오기두, "관련성 없는 전자증거의 수집과 영장주의", 사법논집 제65집(2017)
오길영, "디지털검증의 현재와 그 부당성", 민주법학, 통권 48호(2012. 3.)
원용기, "디지털 증거에 대한 계층적 접근 방안 연구", 석사학위논문, 서울대학교(2016)
이상미, "관련성 없는 디지털 증거 삭제시 이중해쉬를 이용한 무결성 입증 방안", 석사학위논문, 서울대학교(2016)
이성진, "디지털 포렌식스 기술 발전 방안", 디지털 포렌식 연구(2007. 11.)
이숙연, "디지털 증거 및 그 증거능력과 증거조사방안-형사절차를 중심으로 한 연구-", 사법논집 제53집(2011)
이숙연, "디지털 증거의 증거능력과 증거조사방안", 재판자료 제133집 형사법 실무연구Ⅱ(2016)
이정인, "디지털 증거의 관리연속성(Chain of Custody)과 적법절차의 원리에 관한 연구", 석사학위논문, 서울대학교(2019)
장상귀, "디지털 증거의 증거능력에 관한 연구", 법학실무연구회(2009. 5.)
정교일, "디지털 증거의 압수와 공판정에서의 제출방안", 형사법의 신동향 통권 제25호(2010)
최성필, "디지털 증거의 증거능력에 관한 비교법적 연구", 국외훈련

검사 연구논문집 제26집 (2011), 57
하기봉, “디지털 포렌식에 의한 디지털 증거의 증거능력”, 석사학위 논문, 성균관대학교 국가전략 대학원(2012)
황석근·조한혁, “디지탈 서명과 해쉬 함수”, 정보보호학회지 제2권 제1호(1992. 3.)

□ 외국 자료

Eoghan Casey, Digital Evidence and Computer Crime, 2nd edition
Peter Lyman & Hal R. Varian, U.C. Berkely, "How Much Storage is Enough?", ACM Queue vol.1, no.4 June 2003.
Wade Trappe & Lawrence C. Washington, Introduction to Cryptography with Coding Theory, Pearson(2013)

□ 판결 및 규정

대법원 2007. 12. 13. 선고 2007도7257 판결
대법원 2013. 7. 26. 선고 2013도2511 판결
대법원 2015. 7. 16.자 2011모1839 전원합의체 결정
서울중앙지방법원 2007. 4. 16. 선고 2006고합1365, 1363, 1364, 1366, 1367(각 병합) 판결
광주지방법원 2014. 11. 11. 선고 2014고합180 등 판결
디지털 증거 수집 및 분석 규정<대검예규 991호 2019. 5. 20. 시행>

[첨부] 현장조사확인서 양식

[별지 제2호 서식] 현장조사확인서

National Digital Forensic Center

[현장조사확인서]

이미지파일 정보

사건번호	*2019지원0000_1호_○○주식회사*
증거번호	*증1호 홍길동(대표이사)의 노트북*
압수장소	*서울 서초구 반포대로*
사 용 자	*홍길동*
조 사 자	*조사자*
시간설정	PC 설정시간 : *2019. 01. 01. 00:00:00* KST 시간 : *2019. 01. 01. 00:00:00*
이미지파일 생성일시	*2019. 01. 01. 00:00:00*
이미지파일명	*증1호_홍길동(대표이사)_노트북.dd*

해시값

이미지파일	
전자정보상세목록 파일	

※ Hash Value : 해시값은 데이터를 고유하게 식별하는 고정 길이의 값으로 해시함수의 결과로 생성된다. 해시함수는 입력 데이터의 크기와 무관하게 일정한 길이를 가진 값을 출력하며, 입력이 다른 경우 다른 결과가 나타난다. 만약 원본에서 조금이라도 변경이 되면 계산되는 해시값이 완전히 달라지기 때문에, 일반적으로 디지털증거의 무결성을 입증하는 수단으로 사용되고 있다.

- 위 해시값은 *홍길동(대표이사)*의 디지털기기(*노트북*)에서 압수한 전자정보에 대한 해시값이고, 그에 대한 전자정보상세목록을 교부(□출력 □복사) 받았음을 확인합니다.
- 위 압수·수색·검증 절차에서 압수한 전자정보는 수사 또는 재판 목적 소멸 시 폐기됨을 고지받았음을 확인합니다.

확인 일시 및 장소 :

확인자 성명 : (서명)

확인자 생년월일 :

확인자 연락처 :

피압수자(임의제출자 등)와의 관계 : 본인, 기타 ( )

Abstract

Methods for Examination of Evidence that conforms to the nature of Digital Evidence

Park, Chanseok
The Graduate School
of Convergence Science and Technology
Seoul National University

The aim of criminal proceedings is to determine specific legal relations, that is, whether or not a crime is established, and to determine the appropriate type and amount of punishment if a crime is established. These legal relations presuppose a certain factual relationship, and the data used to confirm the factual relationship is evidence. Evidence encompasses three meanings. That is, ① **the method of proof** referring to the objects or people themselves(eg: witness, evidentiary documents, article of evidence) that become the data of fact recognition, ② **the evidential data** indicating what they learned by investigating the method of proof(eg: the witness' testimony, the nature of

article of evidence), and ③ **the evidence results** that include the evidential data and the other non-verbal data obtained through examination of evidence(eg: the expression or attitude of a witness during the examination of a witness).

Digital evidence can be defined as "information that can be trusted in court as stored or transmitted in binary form." This concept focuses on 'the evidential data' among the above three meanings of evidence.

In the investigation and judicial practice about digital evidence in Korea, identity, integrity, and reliability should be met as requirements for the admissibility of evidence, and in the case of duplicating, serching or printing digital data storage media or hard copy or imaging, etc, by moving to the office of an investigative agency, the Supreme court says that in principle, the confiscated person or lawyer should be given an opportunity to participate in such a series of processes. In practice, when collecting digital evidence, a hash value is calculated and a confirmation written in it is issued to the participants to deal with issues such as identity.

However, as shown by the controversy about the CCTV video storage device of the Ferry Sewol, when the confiscated person cannot participate when collecting digital evidence for the first time, distrust may arise over the time and subsequent analysis process of the first collection of digital evidence.

Therefore, this paper first examines the hierarchical structure of

digital evidence, and then proposes the following three ways to improve the Methods for Examination of Evidence that best suits the nature and characteristics of digital evidence.

The first is not to provide evidence of documents printed from digital storage media that is confiscated article(= corresponds to ‘the method of proof’ that requires verification of identity, integrity, reliability, etc), but to collect and submit ‘0 or 1’ digital form of information itself(= correspons to ‘the evidential data’) to the court.

In this case, the file itself which is information in digital form(primary evidence) and a screen or document reproduced in a program, such as a document viewer(secondary evidence) are submitted together, which can be compared to document written in a foreign language or a technical code(primary evidence) and a translation or a result of appraisal(secondary evidence).

The second is the improvement of the technical sealing measure to secure the authenticity of digital evidence submitted as primary evidence as above. Currently, the hash value of the file itself, which is the evidence, is calculated and a confirmation letter is issued to the participants. In addition to the file as evidence, let’s include ‘the time of collecting digital file that can be objectively verified' to parameters of the hash function. If the time of collecting is acquired by an authorized method and included to the parameters of the hash function, the time of collecting the digital evidence can be objectively guaranteed even if there is no participant at the collection site. As the technical means, NTP or TSA can be considered.

The third is a virtual machine. In order to gain confidence in the above series of evidence collection and analysis processes, a system that performs all procedures such as file collection, analysis, and time check is implemented as a virtual machine, and all actions performed in the virtual machine are recorded. After that, the hash value for the virtual machine itself and the hash value for the behavior record are calculated and preserved. As a result, it is possible to secure trust in the subject of the forensic investigation and the investigation process.

As above, the improvement measures for the deficiencies in the current practice regarding the collection and investigation of digital evidence were reviewed at the theoretical level. When the electronic system of criminal procedure is completed soon, the investigation of digital evidence in the way proposed will be smoothly conducted in the courtroom.

.....

Key words: digital evidence, admissibility of evidence, hash function, time of collecting, NTP, TSA, virtual machine

Student Number: 2019-29821