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 증거 선별 압수 개념의 변화에 따른 문제점과 그 개선방안에 관한 연구

2023년 2월

서울대학교 융합과학기술대학원

수리정보과학과 디지털포렌식학 전공

오 중 경

디지털 증거 선별 압수 개념의 변화에 따른 문제점과 그 개선방안에 관한 연구

지도교수 이 병 영

이 논문을 이학석사 학위논문으로 제출함
2022년 12월

서울대학교 융합과학기술대학원
수리정보과학과 디지털포렌식학 전공
오 중 경

오 중 경의 석사 학위논문을 인준함
2023년 1월

위 원 장 _____ 이 광 근 _____ (인)

부위원장 _____ 이 병 영 _____ (인)

위 원 _____ 박 상 철 _____ (인)

국문초록

디지털 증거의 원칙적 선별 압수에 대한 내용이 형사소송법 제106조 제3항에 신설된 이후로 수사기관이 디지털 증거를 수집하는 방법은 정보저장매체에 저장된 정보를 파일 단위로 선별하고 논리이미징하는 방식으로 수행되어왔다. 그러나 디지털 환경의 변화와 함께 압수현장에서 디지털 증거를 선별하는 방식도 달라지고 있다. 데이터베이스 형태 저장 방식의 등장과 클라우드 및 웹 서비스 이용량 증가로 압수 현장에서는 파일 단위 선별 압수 방식보다 정보 단위 선별 압수 방식이 필요한 경우가 많아진 것이다. 이는 기존의 선별 압수 개념에도 변화가 필요하다는 것을 의미한다.

그러나 현재 디지털 증거 수집과 관련된 법률 및 규정들은 정보 단위 선별이 필요한 압수 현장의 상황을 반영하지 못하고 있으며, 현장에서 사용되는 디지털 증거 수집 도구 또한 정보저장매체에 저장된 데이터를 파일 단위로 선별하는 기능 위주로 지원하고 있어 압수 과정에서 동일성, 무결성, 신뢰성 등 디지털 증거 특유의 증거능력 인정요건에 관한 문제가 발생하고 있다. 따라서 이러한 문제를 개선하고 보완할 수 있는 기술적·법률적 연구가 필요하다.

이에 본 논문에서는 정보 단위 선별 압수와 관련된 압수 사례들을 조사하고, 현재 검찰에서 현장 선별 압수가 어떠한 방식으로 진행되고 있는지 확인하였다. 각 사례들을 통해 정보 단위 선별 압수 과정이 기존의 파일 단위 선별 압수 과정과는 절차상·내용상의 차이가 있다는 것을 확인하였으며, 현장 업무수행 시 정보 압수라는 특수성을 고려하여 절차를 수행하지 않는다면 디지털 증거의 증거능력 인정요건과 관련된 문제가 발생할 수도 있다는 것을 확인하였다.

따라서 본 논문에서는 선별 압수 과정에서 발생할 수 있는 증거능력 문제를 기술적·법률적으로 보완하고자 하였다. 증거능력 문제에 대한 기술적 보완방안으로 정보 단위 선별이 필요한 상황에서 사용할 수 있는 현장용 압수 도구의 모형을 제안하고, 디지털 증거 수집과 관련된 법률과 규정에 대한 개정안을 제시하는 것으로 법률적 보완방안을 마련하였다. 결과적으로 실무에서 쟁점이 되는 사례를 정리하고 문제에 대한 해결책을 제시함으로써 현장에서 디지털포렌식 업무를 수행하는 수사관들에게 도움이 될 수 있는 연구를 진행하였다.

주요어 : 디지털포렌식, 압수, 선별, 정보, 데이터베이스, 증거능력
학 번 : 2021-24042

목 차

제 1 장 서 론 ····· 1

제 1 절 연구의 배경 및 필요성 ····· 1

1. 연구의 배경 ····· 1

2. 연구의 필요성 ····· 3

제 2 절 연구의 방법 및 목적 ····· 6

1. 연구의 방법 ····· 6

2. 연구의 목적 ····· 7

제 2 장 선별 압수 개념의 변화 ····· 9

제 1 절 선별 압수 관련 판례 및 규정 ····· 9

1. 선별 압수 관련 판례 ····· 9

2. 선별 압수 관련 규정 ····· 13

제 2 절 선별 압수 개념의 변화 ····· 16

1. 압수수색 현장에서의 변화 ····· 16

2. 법률 및 판례에서의 변화 ····· 18

3. 피압수자 등 참여인의 입장 변화 ····· 22

제 3 장 디지털 증거 압수 사례 ····· 25

제 1 절 압수 대상에 따른 구분 ····· 25

1. 압수 사례 1 ····· 25

2. 압수 사례 2 ····· 26

3. 압수 사례 3 ····· 27

제 2 절 사례별 압수 절차 및 방법 ····· 27

1. 압수 사례 1 ····· 27

2. 압수 사례 2 ····· 29

3. 압수 사례 3 ····· 30
4. 각 압수 사례에서 확인된 문제점 ····· 31

제 4 장 디지털 증거의 증거능력 관련 쟁점 ····· 33
제 1 절 증거능력 인정요건 관련 판례 ····· 33
1. 일심회 사건 ····· 33
2. 왕재산 사건 ····· 35
제 2 절 디지털 증거의 증거능력 인정요건 ····· 38
1. 동일성 ····· 38
2. 무결성 ····· 39
3. 신뢰성 ····· 41
제 3 절 정보 선별 압수에서 증거능력 관련 쟁점 ····· 42
1. 동일성 관련 쟁점 ····· 42
2. 무결성 관련 쟁점 ····· 45
3. 신뢰성 관련 쟁점 ····· 47

제 5 장 정보 선별 압수에 따른 증거능력 보완방안 49
제 1 절 기술적 보완방안 ····· 49
1. 도구 개발의 필요성 ····· 49
2. 현장용 메신저 압수 도구 ····· 50
가. 압수 도구 흐름도 ····· 50
나. 압수 도구의 내용 ····· 52
3. 현장용 데이터베이스 압수 도구 ····· 54
가. 압수 도구 흐름도 ····· 54
나. 압수 도구의 내용 ····· 56
4. 현장용 이미지 수집 도구 ····· 58
가. 압수 도구 흐름도 ····· 58
나. 압수 도구의 내용 ····· 60
5. 도구 개발 제안에 따른 기대효과 ····· 61

가. 동일성, 무결성, 신뢰성 등 증거능력 요건 보완 ····· 61
나. 시간적 효율성 확보 ····· 61
다. 참여권 보장 ····· 62
제 2 절 법률적 보완방안 ····· 62
1. 법률 및 규정의 개정 필요성 ····· 62
2. 관련 법규 및 실무 지침 개정 ····· 64
가. 형사소송법 ····· 64
나. 디지털 증거의 수집·분석 및 관리 규정 ····· 66

제 6 장 결 론 ····· 68

참고문헌 ····· 70

Abstract ····· 73

표 목 차

[표 1] 메신저 데이터에 대한 압수 정보 ····· 53
[표 2] 데이터베이스에 대한 압수 정보 ····· 57
[표 3] 현장용 이미지 수집 도구로 압수한 정보 ····· 60

그 림 목 차

[그림 1] 대검찰청, 디지털 증거 수집 및 분석 실적 ····· 2
[그림 2] 경찰청, 디지털 증거 분석 현황 ····· 2
[그림 3] 전자정보의 관련성에 관한 의견진술서 ····· 23
[그림 4] PC 카카오톡 메신저 데이터베이스 파일 ····· 24
[그림 5] 정보 단위 선별 압수 절차 ····· 32
[그림 6] 파일 선별 압수와 정보 선별 압수 과정 비교 1 · 43
[그림 7] 파일 선별 압수와 정보 선별 압수 과정 비교 2 · 46
[그림 8] 파일 선별 압수와 정보 선별 압수 과정 비교 3 · 47
[그림 9] 현장용 메신저 압수 도구의 분석 및 획득 프로세스 51
[그림 10] PC 카카오톡 메신저 압수 결과 ····· 54
[그림 11] 현장용 데이터베이스 압수 도구 프로세스 ····· 55
[그림 12] 데이터베이스 원본 정보 ····· 57
[그림 13] 현장용 이미지 수집 도구 프로세스 ····· 59

제 1 장 서 론

제 1 절 연구의 배경 및 필요성

1. 연구의 배경

유·무선 네트워크의 발달에 따라 온라인 서비스가 우리 생활의 한 축을 담당하게 되면서 개인들은 하루에도 스마트폰, 노트북 등 다양한 디지털 기기들을 사용하고 있으며, 자연스럽게 우리는 삶의 다양한 흔적들을 데이터 형태로 남기게 되었다. 우리가 남기는 흔적들에는 사용자가 직접 저장한 정보뿐만 아니라 Artifact[1] 등 사용자가 인식하지 못하는 사이에 생성된 정보도 포함되며, 기술의 발전에 따라 저장되는 데이터의 종류와 양도 증가하고 있다. 따라서 수사기관이 범죄를 수사하는 과정에서 디지털 포렌식 등 과학수사 기법을 활용하는 것은 필수적인 것이 되었다.

뉴스에서도 형사사건의 결정적인 증거가 휴대전화, PC 등에서 발견되었다는 것을 쉽게 찾아볼 수 있다. '디지털포렌식'이라는 단어도 일반인들에게 널리 알려져 이제는 더 이상 낯설게 느껴지지 않는다. 형사사건 전체 증거에서 디지털 증거가 차지하는 비율이 증가함에 따라 수사기관들도 디지털포렌식을 수사에 적극적으로 활용하고 있다. 해마다 디지털포렌식 압수 및 분석 건수가 증가하고 있다는 사실은 대검찰청 홈페이지에 게시된 [그림 1] '디지털 증거 수집 및 분석 실적'[2]과 경찰청 홈페이지에 게시된 [그림 2] '디지털 증거 분석 현황'[3]을 통해 확인해 볼 수 있다.

---

1) 디지털포렌식에서 아티팩트의 의미는 운영체제나 애플리케이션을 사용하면서 생성되는 흔적을 말한다. (출처 : http://forensic-proof.com/archives/3710 - 'Artifact')
2) 대검찰청, '디지털 증거 수집 및 분석 실적' 대검찰청 홈페이지 검찰연감 (2020)
3) 경찰청, '디지털 증거 분석 현황' 경찰청 홈페이지 (2021)

구 분	분석 건수		
	2020	2019	2018
압 수 수 색	1,949	2,847	2,328
증 거 분 석	6,606	8,940	8,830
기 타	129	78	67
합계	8,684	11,865	11,225

[그림 1] 대검찰청, 디지털 증거 수집 및 분석 실적 (2018~2020)

(단위 : 건)

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

[그림 2] 경찰청, 디지털 증거 분석 현황 (2010~2020)

대검찰청의 '디지털 증거 수집 및 분석 실적'에서는 매체별 증가 건수가 구체적으로 확인되지 않아 그 세부 내용을 정확하게 확인할 수 없으나, 경찰청의 '디지털 증거 분석 현황'을 살펴보면 10년간 전체 분석 건수가 10배나 증가하였고, 세부적으로 개인용 PC를 포함한 스마트폰, CCTV, 데이터베이스 등에 대한 분석이 증가하는 것이 확인된다. 이중 모바일 기기 및 데이터베이스[4]에 대한 분석 지원 건수 큰 폭으로 증가하고 있다는 점

4) 여러 사람에 의해 공유되어 사용될 목적으로 통합하여 관리되는 데이터의 집

에 주목할 필요가 있다. 이 둘의 공통점은 하나의 파일 또는 저장체계 안에 수많은 데이터를 저장하는 데이터베이스 저장 구조로 되어 있다는 것이다. 개인들이 사용하는 스마트폰의 주요 데이터들은 SQLite[5] 소형 데이터베이스(DB) 형태로 저장되어 있으며, 규모가 있는 기업들은 자사가 보유한 정보를 효율적으로 저장하고 관리하기 위하여 데이터베이스(DB) 서버를 구축하여 사용하고 있다.

생산되는 정보량의 증가에 따라 한정된 저장 공간에 데이터를 효율적으로 저장하고 관리하는 것이 중요해지면서 정보를 데이터베이스 형태로 저장하고 관리하는 매체들이 많아졌다. 따라서 포렌식 수사관들은 압수수색 현장에서 파일 단위 선별을 통한 디지털 증거 수집뿐만 아니라, 다양한 정보들이 혼재된 데이터베이스에서 사건과 관련된 정보만을 선별하여 압수해야 할 필요성도 생기게 되었다. 이는 디지털포렌식 압수수색 과정이 종전보다 훨씬 더 복잡해졌다는 것을 의미한다.

2. 연구의 필요성

형사소송법 제106조 제3항은 압수 목적물이 컴퓨터용 디스크 등 정보저장매체일 경우에는 범위를 정하여 출력 복제하여 압수하는 것을 원칙으로 하고 있으며, 원본 매체에 대한 압수는 예외적으로 허용한다고 규정하고 있다. 이는 수사기관이 압수수색 영장 집행 현장에서 컴퓨터 등 정보저장매체로부터 디지털 증거를 수집하는 과정에서 준수하여야 할 기본적인 내용을 규정한 것이며, 적법절차를 준수하면서 압수수색을 통하여 실체적 진실을 발견함과 동시에 피압수자의 인권을 보호하기 위한 것으로 볼 수 있다.[6]

합을 말한다. (출처 : 네이버 지식백과 doopedia - '데이터베이스')

5) SQLite는 클라이언트 응용 프로그램에 내장되어 동작하는 DBMS 소프트웨어로서 퍼블릭 도메인 오픈소스 소프트웨어이다. 안드로이드, iOS, macOS에 기본적으로 포함되어 있다. (출처 : https://namu.wiki/w/SQLite - 'Sqlite')

6) 김용호·이대성, "실무상 디지털증거의 현장압수수색 문제점과 개선방안" 한국

형사소송법[7)]

제106조 (압수)

③ 법원은 압수의 목적물이 컴퓨터용디스크, 그 밖에 이와 비슷한 **정보저장매체(이하 이 항에서 "정보저장매체등"이라 한다)인 경우에는 기억된 정보의 범위를 정하여 출력하거나 복제하여 제출받아야 한다.** 다만, 범위를 정하여 출력 또는 복제하는 방법이 불가능하거나 압수의 목적을 달성하기에 현저히 곤란하다고 인정되는 때에는 정보저장매체등을 압수할 수 있다.

형사소송법에 디지털 증거에 대한 원칙적 선별 압수에 대한 내용이 규정된 이후로 선별 압수에 대한 개념은 포렌식 수사관이 압수수색 영장 집행 현장에서 포렌식 도구를 이용하여 정보저장매체에 저장된 파일을 선별하고 선별된 파일을 복제하는 방식으로 논리이미징 하거나 인쇄하여 수집하는 것을 가리키는 것으로 이해되었으며[8)] 실무에서도 동일한 방식으로 현장 업무 절차가 수행되어왔다. 그러나 2020년 10월 7일 제정된 "검사와 사법경찰관의 상호협력과 일반적 수사준칙에 관한 규정" 제41조 제1항 전자정보의 압수・수색 또는 검증 방법에서는 기존 형사소송법 절차와 다른 변화가 확인된다. 그것은 압수의 대상을 이전과 달리 정보 자체로 규정한 것이다.

형사소송법 제106조 제3항에서는 압수의 대상을 정보저장매체로 보았다. 이는 디지털 증거가 존재하는 기존 압수 현장이 PC, USB 등 파일 기반

정보통신학회논문지 Vol. 17 No. 11 (2013. 11) p.2598

7) 국가법령정보센터 : 형사소송법, 법률 제18862호 (2022. 5. 9. 일부 개정)

8) 오현석, "전자증거의 선별압수와 매체압수에 관한 연구" 서울대학교 석사 학위 논문 (2019. 2) p.4

저장매체 중심의 환경이었기 때문이다. 따라서 수사기관이 디지털 증거 압수하는 방식도 현장에서 발견된 PC 등 정보저장매체에 저장된 파일들 중에서 영장의 범죄사실과 관련된 파일만을 선별한 뒤 이를 복제하고 사본을 가져가는 방식으로[9] 수행되어왔다. 그러나 "검사와 사법경찰관의 상호협력과 일반적 수사준칙에 관한 규정"에서는 기존의 입장을 바꾸어 압수 대상을 매체로 한정하지 않고 정보 자체로 규정하였다. 이러한 변화는 디지털 환경의 변화 등 요인에 따른 것으로 보인다.

검사와 사법경찰관의 상호협력과 일반적 수사준칙에 관한 규정[10] **제41조 (전자정보의 압수·수색 또는 검증 방법)** ① 검사 또는 사법경찰관은 법 제219조에서 준용하는 법 제106조 제3항에 따라 컴퓨터용디스크 및 그 밖에 이와 비슷한 정보저장매체(이하 이 항에서 "정보저장매체등"이라 한다)에 **기억된 정보(이하 "전자정보"라 한다)를 압수하는 경우**에는 해당 정보저장매체등의 소재지에서 수색 또는 검증한 후 범죄사실과 관련된 전자정보의 범위를 정하여 출력하거나 복제하는 방법으로 한다.

네트워크의 발달과 저장 형태의 다양화 등 디지털 환경의 변화로 인하여 압수 현장에서는 파일 형태의 증거가 존재하지 않는 상황도 존재하며, 하나의 파일이 수많은 정보를 가지고 있어서 그 안에서의 관련된 정보만을 분리하여 선별 압수해야 하는 상황도 발생하게 되었다. 이는 선별의 최소

9) 김영미, "디지털(전자) 증거 압수수색에 있어서 '현장' '선별' 압수수색 원칙의 문제점과 기술적, 법적 개선방안 연구 - 형사소송법 제106조 제3항의 개정 필요성 중심으로" 서울대학교 석사 학위 논문 (2022. 1) p.3

10) 국가법령정보센터 : 검사와 사법경찰관의 상호협력과 일반적 수사준칙에 관한 규정, 대통령령 제31089호 (2021. 1. 1)

단위가 파일에서 정보로 바뀌었다는 것을 의미한다. 선별 압수의 대상과 단위가 정보로 바뀐 측면은 현장 수사관들에게 수집 방법에서의 기술적인 부담을 가중하고 있으며, 압수방식과 절차가 기존과는 다른 부분이 있어 증거능력 판단에도 혼란을 주고 있다. 또한, 기존 해시값 검증 절차만으로는 확보된 디지털 증거의 원본성 및 무결성 입증이 어려워 현장 업무 시 고려해야 할 조건들도 많아졌다.

그러나 현재 디지털 증거 수집과 관련된 법률 및 규정들은 정보 단위 선별이 필요한 압수 현장의 상황을 반영하지 못하고 있으며, 현장에서 사용되는 디지털 증거 수집 도구 또한 정보저장매체에 저장된 데이터를 파일 단위로 선별하는 기능 위주로만 지원하고 있다. 따라서 정보의 압수와 관련하여 현장 실무에서 확인되는 문제점을 보완하기 위한 기술적·법률적 연구가 긴급하게 필요한 상황이다.

제 2 절 연구의 방법 및 목적

1. 연구의 방법

본 논문에서는 먼저 선별 압수 개념이 파일 단위에서 정보 단위로 변화하고 있다는 사실을 확인하고자 하였다. 이에 선별 압수와 관련된 대표적인 판례들과 디지털 증거 수집 관련 법률·규정들을 차례대로 확인하였다. 이후 선별 압수 개념의 변화 요인에 대해 살펴보기 위하여 변화가 확인되고 있는 최근 압수수색 현장 상황과 피압수자 등 참여인들의 선별에 대한 입장 변화 그리고 디지털 증거 수집 관련 규정 및 최신 판례들을 확인하였다.

이후 선별 압수와 관련하여 실무에서 발생하고 있는 증거능력 문제들을 확인하기 위하여 먼저 정보 단위 선별 압수가 필요한 현장 사례들을 조사하고 사례별로 정보에 대한 선별 압수가 어떠한 절차와 방법으로 진행되

고 있는지 조사하였다. 이와 함께 각 사례를 분석하는 것으로 정보 단위 선별 압수 과정과 파일 단위 선별 압수과정의 차이점을 확인하고 정보의 압수와 관련된 문제점을 찾고자 하였다. 단 실무상 현장에서 현물을 봉인하고 추후 분석하는 형태로 압수 절차를 진행하는 모바일포렌식의 특성을 고려하여 모바일 기기에 대한 방법은 본 논문에서는 제외하였다.

이후 디지털 증거의 증거능력 인정요건과 관련된 대표적인 판례를 확인하는 것으로 동일성, 무결성, 신뢰성 등의 디지털 증거 특유의 증거능력 인정요건들이 디지털 증거 수집 절차에서 어떻게 정립되었는지 살펴보았다. 이와 함께 현재 정보 단위 선별 압수 과정에서 동일성, 무결성, 신뢰성 등의 디지털 증거의 증거능력 인정요건과 관련된 문제가 발생하는 구체적인 원인이 무엇인지 검토하였다.

결과적으로 발견된 문제점을 해결하기 위하여 기술적·법률적 보완방안을 제시하였다. 기술적 보완방안으로 '현장용 메신저 압수 도구', '현장용 데이터베이스 압수 도구', '현장용 이미지 수집 도구'에 대한 개발을 제안하였으며, 형사소송법 및 디지털 증거 수집 관련 법률 및 규정들에 대한 개정 의견을 제시하는 것으로 법률적인 보완방안을 마련하였다. 단 기술적 보완방안으로 제안된 도구는 본 논문에서 조사한 정보 단위 선별 압수 사례에 대응할 수 있는 도구로 한정하였으며, 실제 프로그램 개발은 본 논문에서는 제외하였다. 법률적인 보완 방법 또한 디지털 증거 수집 실무와 가장 밀접한 관련성이 있는 형사소송법 및 검찰의 디지털 증거의 수집·분석 및 관리 규정으로 한정하였다.

2. 연구의 목적

디지털 증거가 증거능력을 인정받기 위해서는 원본성, 동일성, 무결성, 신뢰성 등의 인정요건을 만족하여야 한다. 정보 단위 선별 압수의 특성상 도구 및 조작자의 신뢰성과 무결성, 원본과의 동일성 대한 부분이 강조됨에 따라 디지털포렌식 수사관의 현장 업무수행 절차는 더욱 중요해졌다.

압수수색을 통해 확보한 디지털 증거에 대한 절차적인 입증 책임은 검사에게 있지만 기술적인 실무에 대한 부분은 법정 증언 등의 형태로 현장 업무를 수행한 디지털포렌식 수사관이 담당하고 있기 때문이다. 따라서 본 연구를 통해 현재 발생하고 있는 문제들은 확인하고 기술적, 법률적 보완 방법을 함께 모색해보고자 한다.

본 논문에서는 먼저 선별 압수와 관련하여 선별의 개념이 파일 단위에서 정보 단위로 변하게 된 배경과 정보 단위 선별 압수와 관련된 사례들을 조사하고, 정보 단위 선별 압수 과정이 기존의 파일 단위 선별 압수 과정과는 절차상· 내용상 어떠한 차이점 존재하는지 확인하였다. 또한, 정보 단위 선별 압수 과정에서 발생하는 동일성, 무결성, 신뢰성 등 증거능력과 관련된 문제들을 파악하여 현장 압수수색 업무 시 참고할 수 있도록 하였다.

결과적으로 다양한 압수환경에서 정보에 대한 선별 압수가 증거능력을 유지하면서 안정성 있게 진행될 수 있도록 현재 발생하고 있는 문제점들을 기술적·법률적으로 보완할 방안들을 제시하였다. 기술적 보완방안으로 압수 상황의 특성을 고려한 도구의 모형을 제안하고 도구별로 내용·장점 등을 정리하여 추후 현장용 포렌식 도구 개발에 참고가 될 수 있도록 하였으며, 법률적 보완방안으로 형사소송법 및 검찰의 “디지털 증거의 수집·분석 및 관리 규정”에 대한 개정 의견을 제시하여 실무 절차 및 법률 개정 시 참고할 수 있도록 하였다.

제 2 장 선별 압수 개념의 변화

제 1 절 선별 압수 관련 판례 및 규정

1. 선별 압수 관련 판례

디지털 증거는 일반 증거와는 다른 대량성, 복제 용이성, 비가시성 등의 특징[11]을 가지고 있으며 그 특징 중 대량성 및 복제의 용이성은 선별 압수의 필요성과 연결된다. 디지털 증거 압수 현장에서 발견되는 정보저장 매체에는 수사기관이 수사상 필요로 하는 범죄와 관련된 정보뿐만 아니라 무관한 정보들도 포함되어있다. 따라서 수사기관이 사건과 관련된 정보만 선별하여 압수하지 않는다면 범죄와 관련 없는 정보까지 손쉽게 획득할 수 있어 헌법상 보장되고 있는 개인의 통신 자유와 사생활의 자유를 부당하게 침해할 수 있다.

실제적 진실 발견을 위한 수사기관의 증거 수집 활동은 피압수자 개인의 사적 영역을 침해할 수밖에 없으나 디지털 증거 수집을 통한 수사절차는 디지털 증거의 특성 때문에 보통의 압수수색보다 그 침해의 정도가 더 클 수밖에 없다.[12] 이에 따라 법원에서는 형사소송법에 원칙적 선별 압수에 관한 조문이 신설되기 전부터 압수수색 영장 발부 시 영장 발부 사유에 혐의사실과 관련된 부분으로 전자정보 압수 대상을 한정해왔으며, 2011년 7월 18일에는 형사소송법 제106조 제3항에 전자정보의 압수·수색과 관련하여 원칙적 선별 압수 및 예외적 매체 압수를 내용으로 하는 조문이 신설되었다.

---

11) 강미영, “디지털 증거의 증거능력” 외법논집 (2019) p.149-167
12) 조광훈, “디지털 증거의 압수・수색의 문제점과 개선방안” 서울法學 제21권 제3호 (2014. 2) p.703

선별 압수와 관련된 대표적 판례는 형사소송법 제106조 제3항의 신설 이전의 대법원 2011. 5. 26. 자 2009모1190 결정 이른바 '전교조 시국 선언 사건'과 형사소송법 제106조 제3항 신설 이후의 2015. 7. 16. 자 2011모1839 전원합의체 결정, 이른바 '종근당 사건'이 있다. '전교조 시국 선언 사건' 2009모1190 결정에서는 전자정보에 대한 압수・수색영장 집행에 있어 범죄사실과 관련된 것에만 압수해야 한다는 선별 압수의 원칙을 정하였으며, 저장 매체 자체를 압수장소 이외의 장소로 반출할 수 있는 경우를 예외적인 경우로 한정하였다. '전교조 시국 선언 사건' 2009모1190 결정은 형사소송법 제106조 3항의 입법 계기가 되었다[13]. 해당 사건에서 선별 압수와 관련된 결정 요지 원문을 확인하면 다음과 같다.

대법원 2011. 5. 26.자 2009모1190 결정(전교조 시국 선언 사건)[14]

전자정보에 대한 압수·수색영장을 집행할 때에는 원칙적으로 영장 발부의 사유인 **혐의사실과 관련된 부분만을 문서 출력물로 수집하거나 수사기관이 휴대한 저장매체에 해당 파일을 복사하는 방식으로 이루어져야 하고**, 집행현장 사정상 위와 같은 방식에 의한 집행이 불가능하거나 현저히 곤란한 부득이한 사정이 존재하더라도 저장매체 자체를 직접 혹은 하드카피나 이미징 등 형태로 수사기관 사무실 등 외부로 반출하여 해당 파일을 압수·수색할 수 있도록 영장에 기재되어 있고 실제 그와 같은 사정이 발생한 때에 한하여 위 방법이 예외적으로 허용될 수 있을 뿐이다. 나아가 이처럼 저장매체 자체를 수사기관 사무실 등으로 옮긴 후 영장에 기재된 범죄 혐의 관련 전자정보를 탐색하여 해당 전자정보를 문서로 출력하거나 파일을 복사하는 과정 역시 전체적으로 압수·수색영장 집행의 일환에 포함된다고 보아야 한다. 따라서 그러한 경우 **문서출력 또는 파일복사 대상 역시 혐의사실과 관련된 부**

13) 김무석, "디지털 포렌식에서의 참여권 보장 방안" 치안정책연구 제32권 제3호 (2018) p.285

분으로 한정되어야 하는 것은 헌법 제12조 제1항, 제3항, 형사소송법 제114조, 제215조의 적법절차 및 영장주의 원칙상 당연하다. 그러므로 수사기관 사무실 등으로 옮긴 저장매체에서 범죄 혐의 관련성에 대한 구분 없이 저장된 전자정보 중 임의로 문서출력 혹은 파일복사를 하는 행위는 특별한 사정이 없는 한 영장주의 등 원칙에 반하는 위법한 집행이다.

2011모1839 전원합의체 결정 이른바 '종근당 사건'에서도 법원은 2009모1190 결정과 같이 전자정보에 대한 압수・수색영장을 집행하는 데 있어서 범죄혐의와 관련성 있는 것만 압수하여야 한다는 선별 압수 원칙을 재확인하였다. 이후 수사기관이 전자정보에 대한 압수영장 집행하는 방법은 원본을 압수하거나 정보저장매체를 비트스트림(Bit Stream)[15] 형태로 디스크 전체를 물리이미징하는 방법으로 압수하는 것이 아니라 범죄사실과 관련성이 있는 전자정보를 포함하고 있는 최소한의 단위인 파일로 그 범위를 한정하여 선별 수집하는 방법이 사용되고 있다.[16] '종근당 사건'에서 선별 압수와 관련된 결정 요지는 다음과 같다.

대법원 2015. 7. 16.자 2011모1839 전원합의체 결정(종근당 사건)[17]

수사기관의 전자정보에 대한 압수·수색은 원칙적으로 영장 발부의 사유로 된 범죄 혐의사실과 관련된 부분만을 문서 출력물로 수집하거나 수사기관이 휴대한 저장매체에 해당 파일을 복제하는 방식으로 이루어져야 하고, 저장매체 자체를 직접 반출하거나 저장매체에 들어 있는 전

14) 국가법령정보센터 : 대법원 2011. 5. 26.자 2009모1190 결정(전교조 시국 선언 사건)
15) 데이터 통신 회로를 통하여 연속적으로 전송되는 일련의 비트열로 데이터 스트림의 단위를 말한다. (출처 : 한국정보통신기술협회 정보통신용어사전 - '비트스트림')
16) 유상현·이경렬, "디지털 증거의 선별적 압수수색에 관한 LSH(Locality Sensitive Hashing)기법 활용방안 연구" 박사 학위 논문 (2020. 1) p.156

자파일 전부를 하드카피나 이미징 등 형태(이하 '복제본'이라 한다)로 수사기관 사무실 등 외부로 반출하는 방식으로 압수·수색하는 것은 현장의 사정이나 전자정보의 대량성으로 관련 정보 획득에 긴 시간이 소요되거나 전문 인력에 의한 기술적 조치가 필요한 경우 등 범위를 정하여 출력 또는 복제하는 방법이 불가능하거나 압수의 목적을 달성하기에 현저히 곤란하다고 인정되는 때에 한하여 예외적으로 허용될 수 있을 뿐이다.

이처럼 저장매체 자체 또는 적법하게 획득한 복제본을 탐색하여 혐의사실과 관련된 전자정보를 문서로 출력하거나 파일로 복제하는 일련의 과정 역시 전체적으로 하나의 영장에 기한 압수·수색의 일환에 해당하므로, 그러한 경우의 **문서출력 또는 파일복제의 대상 역시 저장매체 소재지에서의 압수·수색과 마찬가지로 혐의사실과 관련된 부분으로 한정되어야 함은 헌법 제12조 제1항, 제3항과 형사소송법 제114조, 제215조의 적법절차 및 영장주의 원칙이나 비례의 원칙에 비추어 당연하다**. 따라서 수사기관 사무실 등으로 반출된 저장매체 또는 복제본에서 혐의사실 관련성에 대한 구분 없이 임의로 저장된 전자정보를 문서로 출력하거나 파일로 복제하는 행위는 원칙적으로 영장주의 원칙에 반하는 위법한 압수가 된다.

전자정보는 복제가 용이하여 전자정보가 수록된 저장매체 또는 복제본이 압수·수색과정에서 외부로 반출되면 압수·수색이 종료한 후에도 복제본이 남아있을 가능성을 배제할 수 없고, 그 경우 혐의사실과 무관한 전자정보가 수사기관에 의해 다른 범죄의 수사의 단서 내지 증거로 위법하게 사용되는 등 새로운 법익침해를 초래할 가능성이 있으므로, **혐의사실 관련성에 대한 구분 없이 이루어지는 복제·탐색·출력을 막는 절차적 조치가 중요성을 가지게 된다.**

17) 국가법령정보센터 : 대법원 2015. 7. 16.자 2011모1839 전원합의체 결정(종근당 사건)

2. 선별 압수 관련 규정

우리나라를 대표하는 수사기관인 검찰과 경찰에서는 실체적 진실을 발견하고 동시에 국민의 인권을 보호할 목적[18]으로 디지털 증거에 대한 압수수색 및 디지털 증거확보에 대한 절차적 방법과 그 과정에서 준수하여야 할 기본적 사항을 각각 대검찰청예규, 경찰청 훈령으로 정하였다. 검찰은 "디지털 증거의 수집·분석 및 관리 규정" 대검찰청예규 제1285호에서, 경찰은 "디지털 증거의 처리 등에 관한 규칙" 경찰청 훈령 제1030호에서 그 내용을 다루고 있다.

형사소송법 제106조 제3항에서 명시한 선별 압수와 관련된 내용은 수사기관의 규정 및 규칙에서도 그 내용을 확인할 수 있다. 검찰은 "디지털 증거의 수집·분석 및 관리 규정" 제20조 제1항에서 선별 압수와 관련하여 "범죄사실과 관련된 전자정보의 범위를 정하여 출력하거나 복제하는 방법으로 한다."라고 규정하고 있으며, 경찰은 "디지털 증거의 처리 등에 관한 규칙" 제9조에서 "디지털 증거의 수집은 수사목적을 달성하는데 필요한 최소한의 범위에서 이루어져야 한다."라고 규정하고 있다. 각 규정과 규칙에서의 선별 압수에 대한 용어 사용에서의 차이는 있으나 압수 대상 및 범위에 대한 제한에 의미는 같은 것으로 보인다.

디지털 증거의 수집·분석 및 관리 규정[19]
제20조(전자정보의 단계적 압수·수색·검증)
① 주임검사등은 <u>**정보저장매체등에 기억된 전자정보**</u>를 압수하는 경우에는 해당 정보저장매체등의 소재지에서 수색 또는 검증한 후 범죄사

18) 국가법령정보센터 : 디지털 증거의 수집·분석 및 관리 규정, 대검찰청예규 제1285호 - 제1조

실과 관련된 전자정보의 범위를 정하여 출력하거나 복제하는 방법으로 한다.

② 제1항에도 불구하고 그에 따른 압수 방법의 실행이 불가능하거나 그 방법으로는 압수의 목적을 달성하는 것이 현저히 곤란한 경우에는 압수·수색 또는 검증 현장에서 정보저장매체등에 들어 있는 전자정보 전부를 복제하여 그 복제본을 정보저장매체등의 소재지 외의 장소로 반출할 수 있다.

③ 제1항 및 제2항에도 불구하고 그에 따른 압수 방법의 실행이 불가능하거나 그 방법으로는 압수의 목적을 달성하는 것이 현저히 곤란한 경우에는 피압수자등이 참여한 상태에서 정보저장매체등의 원본을 봉인하여 정보저장매체등의 소재지 외의 장소로 반출할 수 있다.

디지털 증거의 처리 등에 관한 규칙[20]

제9조(디지털 증거 수집 시 원칙)

디지털 증거의 수집은 수사목적을 달성하는데 필요한 최소한의 범위에서 이루어져야 하며, 「형사소송법」 등 관계 법령에 따른 적법절차를 준수하여야 한다.

형사소송법 제106조 제3항뿐만 아니라 수사기관의 규칙 및 규정들도 선

19) 국가법령정보센터 : 디지털 증거의 수집·분석 및 관리 규정, 대검찰청예규 제1285호 (2022. 5. 18)
20) 국가법령정보센터 : 디지털 증거의 처리 등에 관한 규칙, 경찰청훈령 제1030호 (2021. 8. 30)

별 압수에 관련된 내용을 디지털 증거 수집 시 준수하여야 할 기본적 사항에 포함하고 있다. 법원도 수사기관이 디지털 정보에 대한 압수를 위해 포괄 영장을 청구한다고 판단되면 영장에 별지를 첨부하거나 일부 기각의 등의 방법으로 수사기관의 압수 방법 및 범위 등을 제한하고 있다.[21] 법원이 발부하는 압수수색 영장에 포함된 압수 대상 및 방법의 제한에 관한 영장 별지 내용은 다음과 같다.

[영장 별지][22]

압수 대상 및 방법의 제한

가. 전자정보의 수색·검증

수색·검증만으로 수사의 목적을 달성할 수 있는 경우, 압수 없이 수색·검증만 함.

나. 전자정보의 압수

(1) 원칙

<u>저장매체의 소재지에서 수색・검증 후 혐의사실과 관련된 전자정보만을 문서로 출력하거나 수사기관이 휴대한 저장매체에 복사하는 방법으로 압수할 수 있음.</u>

(2) 저장 매체의 하드카피·이미징(이하 '복제'라 한다)이 허용되는 경우

(가) 집행현장에서의 복제

출력・복사에 의한 집행이 불가능하거나, 압수의 목적을 달성하기에 현저히 곤란한 경우에 한하여, 저장매체 전부를 복제할 수 있음.

21) 윤신자·이상진, "전자정보의 압수·수색절차 개선방안 연구" 경찰학연구 제13권 제4호 (2013) p.235

22) 손지영·김주석, "디지털 증거의 증거능력 판단에 관한 연구" 대법원 사법정책

(나) 저장 매체의 원본 반출이 허용되는 경우

1) 위 (가)항의 경우 중 집행현장에서의 저장 매체의 복제가 불가능하거 나 현저히 곤란할 때에 한하여, 피압수자 등의 참여하에 저장 매체 원본을 봉인하여 저장 매체의 소재지 이외의 장소로 반출할 수 있음.

2) 위 1)항의 방법으로 반출한 원본은 피압수자 등의 참여하에 개봉하여 복제한 후 지체 없이 반환하되, 특별한 사정이 없는 한 원본 반출일로부터 10일을 도과하여서는 아니 됨.

(다) 위 (가), (나)항과 같이 복제한 저장 매체에 대하여는, 혐의사실과 관련 된 전자정보만을 출력 또는 복사하여야 하고, 전자정보의 복구나 분석 을 하는 경우 신뢰성과 전문성을 담보할 수 있는 방법에 의하여야 함.

(라) 위 (다)항에 의하여 증거물 수집이 완료되고 복제한 저장 매체를 보전할 필요성이 소멸된 후에는 혐의사실과 관련 없는 전자정보를 지체없이 삭제, 폐기하여야 함.

(다) 압수・수색의 전체 과정을 통하여 피압수자 등의 참여권이 보장되어야 하며, 참여를 거부하는 경우에는 신뢰성과 전문성을 담보할 수 있는 상당한 방법으로 압수・수색이 이루어져야 함.

(라) 위 (다)항에 의하여 증거물 수집이 완료되고 복제한 저장매체를 보전할 필요성이 소멸된 후에는 혐의사실과 관련 없는 전자정보를 지체없이 삭제, 폐기하여야 함.

제 2 절 선별 압수 개념의 변화

1. 압수수색 현장에서의 변화

연구원 연구총서 2015-08호 p.75-76

디지털 증거 수집 시 관련성 있는 정보만 선별하여 압수해야 한다는 내용이 여러 판례를 통해 확인된 이후, 선별 압수의 원칙은 형사소송법 및 수사기관의 디지털 증거 수집 관련 규정 형태로 조문화되었다. 법원 또한 영장 별지를 통해서 포괄 압수 등을 제한함에 따라 선별 압수는 디지털 증거 압수수색의 원칙으로 자리 잡았다. 이후 수사기관이 디지털 증거를 수집하는 방법은 정보저장매체에서 사건과 관련된 정보를 파일로 단위로 선별하여 논리이미징하는 방식으로 수행되고 있다. 따라서 현장용 압수수색 도구들은 매체에 저장된 정보를 파일 단위로 선별하는 기능 위주로 개발되었으며, 압수 기법들도 키워드 검색, 유형별 파일 분류 기능 등 한정된 시간에 파일을 신속하고 정확하게 선별하는 기능 위주로 발전해왔다.

그러나 현재 압수수색 현장의 디지털 환경은 빠르게 변화하고 있으며 그 내용 또한 복잡해지고 있다. 웹 기반 시스템, 클라우드, 데이터베이스 저장체계 등은 구조가 복잡하여 압수 대상 시스템에 대한 전문 지식 없이는 현장 대응이 어렵다. 기존의 포렌식 절차와 방법만으로는 압수 집행이 어려운 상황이 많아진 것이다. 현장 상황이란 본래 예외적인 부분이 많지만 이러한 압수 현장의 커다란 변화는 현장에서 디지털 증거 선별 압수 절차를 수행하는 포렌식 수사관들을 더욱 어렵게 하고 있다.

선별 압수 개념의 변화는 실제 압수 현장에서도 확인되고 있다. PC에서는 내용 선별이 필요한 메신저 데이터가 SQLite DB 형태로 발견되고 있으며, 압수 대상 데이터가 데이터베이스 서버에 존재하여 DBMS[23]를 통해 데이터베이스에 접속하고 사건과 관련된 정보만 오피스 파일 형태로 추출하는 방식의 압수가 필요한 상황도 존재한다. 또한, 웹 기반 시스템에서 저장된 정보를 수집하기 위해 관련 정보만을 파일로 내려받거나 캡처하는 방법을 사용하기도 한다. 단순히 파일을 선별하고 복제하는 방식이

23) 데이터베이스에 접근하여 데이터베이스에 대한 정의, 조작, 제어 등을 가능하게 하는 데이터베이스 관리 소프트웨어. (출처 : 한국정보통신기술협회 정보통신용어사전 - ‘DBMS’)

아닌 정보 자체에 대한 선별 압수가 필요한 상황이 많아진 것이다.

압수수색 대상 시스템의 환경 변화와 선별 압수 원칙에 따라 포렌식 수사관이 압수하는 디지털 증거는 더 이상 저장 매체에 저장된 파일 자체로 한정할 수 없다. 정보는 파일 형태로만 존재하는 것은 아니며, 얼마든지 원본에서 분할될 수 있는 특징이 있으므로 선별 방식에 따라 압수 당일에도 파일 형태로 생성될 수 있기 때문이다. 따라서 정보 단위의 선별 절차를 거쳐 획득한 디지털 증거에 대한 원본 동일성과 무결성은 압수 과정에서 사용되는 도구의 신뢰성, 수집자의 신뢰성에 크게 의존할 수밖에 없으며, 원본 출처에 대한 정보 및 압수 과정에 대한 증명이 필수적으로 요구될 수밖에 없다.

2. 법률 및 판례에서의 변화

2011. 5. 26.자 2009모1190 결정 이른바 '전교조 시국 선언 사건'과 2015. 7. 16.자 2011모1839 전원합의체 결정 이른바 '종근당 사건'의 각 결정 요지에는 선별 압수와 관련하여 "혐의사실과 관련된 부분만을 수사기관이 휴대한 저장매체에 해당 파일을 복사하는 방식으로 이루어져야 하고"[24]라며 언급하여 전자정보 선별의 단위를 파일로 규정하였다. 따라서 위 결정에 영향을 받은 형사소송법 제106조 제3항 및 "검찰의 디지털 증거 수집·분석 및 관리 규정"은 선별의 최소 단위를 파일로 정하고 있는 것으로 보인다. 그러나 2020년 10월 7일 제정되어 2021년 1월 1일 시행된 "검사와 사법경찰관의 상호협력과 일반적 수사준칙에 관한 규정"에서는 선별의 최소 단위에 대한 기존과는 다른 시각이 확인된다. 그것은 전자정보 압수에서 압수 목적물을 기존의 입장과는 다르게 정보 자체로 특정한 점이다. 해당 규정 제41조는 전자정보의 압수·수색 또는 검증 방법에 대하여 다음과 같이 규정하고 있다.

24) 국가법령정보센터 : 대법원 2011. 5. 26.자 2009모1190 결정(전교조 시국 선언 사건)

검사와 사법경찰관의 상호협력과 일반적 수사준칙에 관한 규정[25)]

제41조 (전자정보의 압수・수색 또는 검증 방법)

① 검사 또는 사법경찰관은 법 제219조에서 준용하는 법 제106조 제3항에 따라 컴퓨터용디스크 및 그 밖에 이와 비슷한 정보저장매체(이하 이 항에서 "정보저장매체등"이라 한다)에 기억된 정보(이하 "전자정보"라 한다)를 압수하는 경우에는 해당 정보저장매체등의 소재지에서 수색 또는 검증한 후 범죄사실과 관련된 전자정보의 범위를 정하여 출력하거나 복제하는 방법으로 한다.

기존의 형사소송법 제106조 제3항은 전자정보 압수와 관련하여 압수의 목적물이 정보저장매체인 경우에는 기억된 정보의 범위를 정하여 출력하거나 복제하여 제출하라고 규정하여, 압수의 목적물을 디스크 등 저장 매체로 보고 사건과 관련된 파일 단위의 선별 압수 방식을 요구하였다. 그러나 "검사와 사법경찰관의 상호협력과 일반적 수사 준칙에 관한 규정" 제41조 제1항에서는 압수의 목적물을 정보 자체로 보았다. 정보의 압수에서 정보의 범주란 정보저장매체 속의 저장된 파일 뿐만 아니라 클라우드 및 데이터베이스 서버 등에 저장된 정보 자체를 포함한다.

웹 기반 서비스 및 클라우드 사용이 증가함에 따라 디지털 증거 압수 현장에서는 정보저장매체 실물을 볼 수 없는 사례도 있으며, 웹 기반 업무 시스템을 사용하는 회사의 PC 하드디스크에서는 업무와 관련된 정보가 담긴 파일이 발견되지 않기도 한다. 또한, 서버나 애플리케이션은 데이터를 효율적으로 관리·저장하기 위해 데이터베이스 형식의 저장 방식을 많

25) 국가법령정보센터 : 검사와 사법경찰관의 상호협력과 일반적 수사준칙에 관한 규정, 대통령령 제31089호 (2021. 1. 1)

이 사용하고 있다. 따라서 압수 현장에서는 클라우드, 웹 서비스, 데이터베이스 등에서 사건과 관련된 정보만을 수집하기 위해 정보 자체를 선별 압수할 필요성이 생기게 되었다.

최근 대법원 결정에서도 선별 압수 개념의 변화와 관련된 내용이 확인되고 있다. 대법원 2022. 5. 31.자 2016모587 결정에서는 수사기관이 인터넷 서비스업체인 카카오톡 본사 서버에 저장된 준항고인의 카카오톡 대화 내용에 대하여 압수·수색한 사안에서 수사기관이 카카오톡 대화 내용 등을 압수할 때 사건과 관련된 내용만을 선별하지 않고 전체 데이터를 압수한 것은 위법이라고 판시하였다. 이는 법원에서도 하나의 파일 안에 사건과 관련 없는 데이터가 혼재된 메신저 데이터의 특성을 인정하고, 정보 단위 선별이 필요함을 인정한 의미 있는 결정으로 보인다. 해당 결정 원문에 내용을 살펴보면 다음과 같다.

<u>대법원 2022. 5. 31.자 2016모587 결정 [준항고인용결정에대한재항고]</u>[26)]

1. 사안의 개요

나. 수사기관은 2014. 5. 26. 11:55경 카카오를 상대로 이 사건 압수· 수색영장에 기하여 피의자인 준항고인의 카카오톡 대화내용 등이 포함된 위 '압수할 물건'에 대한 압수·수색(이하 '이 사건 압수·수색'이라 한다)을 실시하였다.

[중략]

라. 카카오 담당자는 2014. 5. 26. 수사기관의 이 사건 압수·수색영장 집행에 응하여 준항고인의 카카오톡 대화내용이 저장되어 있는 서버에서 2014. 5. 20. 00:00부터 2014. 5. 21. 23:59까지 준항고인의 대화

내용(이하 '이 사건 전자정보'라 한다)을 모두 추출하여 수사기관에 이메일로 전달하였다. 카카오 담당자는 이 사건 전자정보 중에서 압수 · 수색영장의 범죄사실과 관련된 정보만을 분리하여 추출할 수 없었으므로 위 기간의 모든 대화내용을 수사기관에 전달하였는데, 이 사건 전자정보에는 준항고인이 자신의 부모, 친구 등과 나눈 일상적 대화 등 혐의사실과 관련 없는 내용이 포함되어 있다.

[중략]

3. 대법원의 판단

원심이 인터넷서비스업체인 카카오 본사 서버에 보관된 이 사건 전자정보에 대한 이 사건 압수 · 수색영장의 집행에 의하여 전자정보를 취득하는 것이 참여권자에게 통지하지 않을 수 있는 형사소송법 제122조 단서의 '급속을 요하는 때'에 해당하지 않는다고 판단한 것은 잘못이나, 그 과정에서 압수·수색영장의 원본을 제시하지 않은 위법, 수사기관이 카카오로부터 입수한 전자정보에서 범죄 혐의사실과 관련된 부분의 선별 없이 그 일체를 출력하여 증거물로 압수한 위법, 그 과정에서 서비스이용자로서 실질적 피압수자이자 피의자인 준항고인에게 참여권을 보장하지 않은 위법과 압수한 전자정보목록을 교부하지 않은 위법을 종합하면, 이 사건 압수·수색에서 나타난 위법이 압수 · 수색 절차 전체를 위법하게 할 정도로 중대하다는 원심의 결론을 수긍할 수 있다.

디지털(전자) 증거 선별 압수와 관련된 기존의 연구에서 김영미는 "형사소송법 제106조 제3항이 압수 대상을 정보저장매체로 규정하고 '정보'(information)로 규정하지 아니하고 있으나, 판례와 다수 학설은 압수수색 대상이 정보가 됨을 인정하고 있는 것으로 판단되며, 향후 논란의 소지를 방지하기 위해 '정보'가 압수수색 대상임을 법 개정을 통해 명시함이 바람

26) 국가법령정보센터 : 대법원 2022. 5. 31.자 2016모587 결정

직해 보인다."라고 주장하였다.[27] 이처럼 정보의 압수 개념의 도입과 함께 파일 단위의 선별에서 정보 단위로 선별 압수 개념이 변화되고 있는 모습이 판례 및 논문에서도 확인되고 있다.

3. 피압수자 등 참여인의 입장 변화

압수수색 현장에서는 압수수색 과정에 참여하는 피압수자, 변호인, 전문입회인[28] 등 참여인들의 변화가 확인되고 있다. 그 변화는 선별 과정에 대한 관심과 참여도가 높아지고 있다는 것이다. 개인정보보호에 대한 인식이 강화되고 디지털포렌식이라는 용어가 대중들에게 널리 알려짐과 함께 최근 압수 현장에서는 개인의 사생활과 관련된 메신저, 이메일 데이터에 대한 압수와 관련하여 피압수자 등 참여인들이 선별 과정에 적극적으로 참여하길 원하는 모습이 확인되고 있다.

실무상 압수 현장에서 선별 압수가 가능한 상황에서는 참여인에게 다음과 같이 선별에 관한 참여권을 보장하고 있다. 포렌식 수사관은 선별 압수 규정에 따라 포렌식 도구를 이용하여 피압수자들의 정보저장매체에서 사건과 관련된 파일을 키워드, 기간 등으로 1차 선별한다. 이후 선별된 정보에 대하여 피압수자 등 참여인과 함께 관련성 여부를 확인하는 기회를 부여한다. 최종적으로 선별된 압수 대상에 대하여 논리이미징을 실시하고 피압수자에게 상세목록을 교부한 뒤 현장조사확인서에 서명을 받는다.

"디지털 증거의 수집·분석 및 관리 규정" 제22조 제2항은 압수·수색·검증 과정에 참여한 참여인이 압수 대상 전자정보와 사건의 관련성에 관하여 의견을 제시한 때에는 이를 조서에 적어야 한다고 규정하여 상세 목록

---

27) 김영미, "디지털(전자) 증거 압수수색에 있어서 '현장' '선별' 압수수색 원칙의 문제점과 기술적, 법적 개선방안 연구 - 형사소송법 제106조 제3항의 개정 필요성 중심으로" 서울대학교 석사 학위 논문 (2022. 1) p.19

28) 권양섭, "디지털포렌식 전문입회인 제도의 필요성과 운영방안" 디지털포렌식연구 (2020) p.426-435

교부 후 참여인에게 관련성에 대한 의견 진술권 또한 보장하고 있다. 따라서 현장에서는 압수한 데이터의 관련성에 관하여 이의가 있는 경우 참여인들이 적극적으로 의견을 진술하는 모습이 확인되기도 한다. 전자정보의 관련성에 관한 의견진술서 양식은 [그림 3]과 같다.

[별지 제14호 서식] 전자정보의 관련성에 관한 의견진술서

【전자정보의 관련성에 관한 의견진술서 】

의견진술인	성 명		생 년 월 일	
	연 락 처		사건과의 관계	
의견진술 대상 전자정보	매체 종류 (제조사,모델)		이미지 파일명	
	20 . . . 00:00 부터 20 . . . 00:00 까지 (장소)에서 집행한 위 매체에 기억된 전자정보 중 일부			

◎ 참여권 보장에 관한 의견 유무 (있음 □ / 없음 □)

(의견 기재)

◎ 전부 복제본 또는 매체 원본 반출에 관한 의견 유무 (있음 □ / 없음 □)

(의견 기재)

◎ 개개 전자정보의 압수에 관한 의견 유무 (있음 □ / 없음 □)

(의견 기재)

위 의견진술인은 위 일시, 장소에서 있었던 전자정보에 대한 압수·수색·검증과 관련하여 위와 같이 의견을 진술합니다.

20 . . .

위 작성자 : (서명)

[그림 3] 전자정보의 관련성에 관한 의견진술서[29]

현재 압수수색에서 현장에서 가장 쟁점이 되는 부분은 PC에서 카카오톡 등 메신저 데이터가 발견되었을 때이다. PC 카카오톡의 경우 메시지 대화 내용은 [그림 4]와 같이 EDB 형식의 암호화된 SQLite 형태로 분리 저장되어 있다. 따라서 사건과 관련된 카카오톡 메시지 일부 내용만을 증거로 수집하고자 할 때는 복호화 작업과 함께 전체 메시지 내용을 오피스 파일 형태로 추출[30]하고 선별하는 방식이 사용된다. 그러나 메신저 데이

29) 국가법령정보센터 : 디지털 증거의 수집·분석 및 관리 규정 - 별지 제14호 서식
30) 이주호·이태명, “디지털증거의 선별압수에 따른 원본성 및 동일성 증명에 관

터에 대한 현장 선별기능을 지원하는 도구가 없어 실무에서는 데이터 전체가 들어있는 파일들을 가선별[31]하여 봉인한 이후, 추후 참관을 통해 선별 과정 참여의 기회를 부여하는 방식으로 사건 관련 정보를 선별 압수하고 있다.

Users > user > AppData > Local > Kakao > KakaoTalk > users > 48a81776801a873db58818b76bf8eec9aef8c812 > chat_data

이름	수정한 날짜	유형	크기
chatLogs_257448664.edb	2022-09-05 오후 1:11	EDB 파일	64KB
chatLogs_415920246.edb	2022-10-18 오전 9:20	EDB 파일	2,352KB
chatLogs_489533627.edb	2022-09-23 오전 7:59	EDB 파일	132KB
chatLogs_534625951.edb	2022-09-20 오후 7:01	EDB 파일	60KB
chatLogs_607613071.edb	2021-09-17 오후 4:51	EDB 파일	44KB
chatLogs_648182338.edb	2022-10-13 오전 9:32	EDB 파일	72KB
chatLogs_901082558.edb	2022-09-01 오전 8:56	EDB 파일	56KB
chatLogs_18353909141250.edb	2021-11-06 오후 4:57	EDB 파일	44KB
chatLogs_22247937441791.edb	2022-06-03 오후 4:32	EDB 파일	44KB
chatLogs_24388492347417.edb	2020-12-14 오후 12:43	EDB 파일	32KB
chatLogs_33416029035882.edb	2022-09-01 오전 8:56	EDB 파일	92KB
chatLogs_33416029035882.edb-shm	2022-09-05 오후 12:22	EDB-SHM 파일	32KB
chatLogs_33416029035882.edb-wal	2022-09-05 오후 12:49	EDB-WAL 파일	37KB
chatLogs_41179727420641.edb	2022-02-22 오후 2:28	EDB 파일	44KB
chatLogs_41456013561403.edb	2021-09-05 오후 12:11	EDB 파일	44KB
chatLogs_48080958374296.edb	2020-10-12 오후 11:49	EDB 파일	32KB
chatLogs_49633674289352.edb	2022-10-16 오전 10:20	EDB 파일	108KB
chatLogs_56497904023666.edb	2022-02-17 오후 4:25	EDB 파일	52KB

[그림 4] PC 카카오톡 메신저 데이터베이스 파일

PC 카카오톡은 카카오톡 모바일 앱 계정과 연동 가능한 장점이 있어 기업에서 업무용 메신저로도 많이 사용되고 있다. 그러나 이러한 장점 때문에 PC에 저장된 카카오톡 데이터베이스 파일 속에는 업무와 관련된 내용뿐만 아니라 관련성이 없는 개인의 사생활이 담긴 대화 내용도 다수 포함될 수 있으며, 따라서 피압수자는 메신저 데이터 파일에 저장된 대화 내용이 수사기관에 의해 압수된다는 사실에 민감할 수밖에 없다. 이처럼 압수수색 현장에서 피압수자 등 참여인들의 참여권에 관한 입장 변화가 확인되고 있다. 이는 곧 디지털 증거 압수 절차 수행 시 정보 단위 선별 절차가 중요해지고 있다는 사실과 연결된다.

한 연구" 디지털포렌식연구 (2020) p.252-268

31) 압수수색 현장에서 사건과 관련이 있는 전자정보만 선별 압수하는 것이 불가능한 경우 전체 전자정보 중에서 일부만을 부분 복제하여 현장 이외의 장소로 반출하는 것을 말한다. 디지털 증거의 수집·분석 및 관리 규정 - 제3조(정의) 제6항 '가선별'

제 3 장 디지털 증거 압수 사례

제 1 절 압수 대상에 따른 구분

디지털 환경의 변화에 따라 전자정보 압수 절차에서 선별 대상이 파일에서 정보로 변화·확장되어 가고 있다. 그러나 기존 파일 단위의 선별 개념이 필요 없게 된 것이 아니다. 현재까지도 대다수 일반적인 압수수색 현장에서는 PC, USB 등 전통적으로 사용되어 왔던 저장매체들이 많이 사용되고 있으며 그 속에 저장된 문서파일 등이 사건 해결에 중요한 증거로 발견되고 있기 때문이다.

압수수색 현장에서 포렌식 수사관은 한정적인 시간 내에 정확하고 신속하게 디지털 증거를 수집해야 한다. 따라서 압수 대상 정보의 저장 형태와 특성을 정확하게 파악하고 현장 상황에 적합한 도구와 방법을 사용하여 포렌식 절차를 수행할 필요가 있다. 이는 수사의 정확성 및 신속성과도 연관되며 동일성, 무결성, 신뢰성 등 디지털 증거의 증거능력 인정요건과도 관련된 문제이기 때문이다.

이에 본 장에서는 먼저 정보 단위 선별 압수가 필요한 압수 사례들을 압수 대상별로 구분하였다. 이후 사례별로 압수 대상 디지털 증거의 특징과 선별 압수 과정에서 고려되어야 할 문제들을 확인하였다. 이와 함께 현재 디지털포렌식 수사관들이 현장에서 디지털 증거를 선별하고 수집하는 방법들을 조사함으로써 선별 압수 과정에서의 나타나는 쟁점들과 증거능력 인정요건과 관련된 문제점들을 확인하였다.

1. 압수 사례 1

OO 사건 수사와 관련하여 A 회사에 대한 압수수색 영장이 발부되었다.

압수수색의 목적은 임직원들의 사건 관련 내용 검토 및 외부인과 공모 여부 등 사실관계를 확인하기 위함이며, 압수수색 영장에 기재된 압수수색 대상은 사건 관련 정보를 담고 있는 파일 및 메일, 메신저로 특정되었다. 현장을 통제한 이후 사내 전산팀으로 이동하여 전산 담당자와의 인터뷰를 통해 사내 IT 인프라 시스템을 조사하였다. 그 결과 A 회사는 중소기업으로 임직원은 15명으로 확인되고, 직원들 개인마다 노트북이 1대씩 지급되고 있으며, 그룹웨어 내 웹 메일계정이 개인마다 제공되고 업무용 메신저로 사내 메신저와 PC 카카오톡이 사용되고 있다는 것이 확인되었다. 이후 포렌식 수사관이 특정 대상자 노트북을 탐색한 결과 회사 내부 메신저 데이터는 암호화되지 않은 텍스트 형태로, PC 카카오톡 데이터는 암호화된 데이터베이스 형태로 PC에 저장된 것이 확인되어 PC에 저장된 메신저 데이터에 대한 압수가 진행되었다.

2. 압수 사례 2

OO 사건 수사와 관련하여 OO 사업을 하는 B 회사에 대한 압수수색 영장이 발부되었다. 압수수색의 목적은 회사가 보관하고 있는 OOO 중량 관련 계측데이터를 확보하는 것이다. 현장 통제 이후 사내 전산팀으로 이동하여 담당자와 사내 IT 인프라 관련하여 조사한 결과, B 회사는 중소기업으로 임직원은 25명으로 확인되고, 임직원 개인에게 업무용 PC가 1대씩 지급되며, 서울에 있는 지사 사무실에 그룹웨어 및 ERP[32] 서버를 직접 구축하여 본사에서 원격으로 관리하고 있다는 사실을 확인하였다. 사건에 핵심이 되는 OOO 측량 관련 데이터는 ERP 서버에 저장되어 관리되고 있었으며, 계측데이터 관리 웹페이지에서 5년 기간의 계측데이터가 확인되어 데이터 추출을 시도하였으나 웹페이지에 별도 데이터 추출 및 다운로드 옵션은 제공되지 않는 것으로 확인되었다.

---

32) 최적화된 기업 활동을 위해 인력·생산재·물류·회계 등 기업 자원을 전체적으로 관리하는 전산 시스템을 말한다. (출처 : 한국정보통신기술협회 정보통신용어사전 - 'ERP')

3. 압수 사례 3

OO 사건 수사와 관련하여 C 회사에 대하여 압수수색 영장이 발부되었다. 압수수색의 목적은 범죄혐의와 관련된 사실관계 확인을 위해 회사 직원들 간의 대화가 담긴 메신저 및 이메일 확보하는 것이다. 현장을 통제한 뒤 회사의 사내 IT 인프라를 조사한 결과 C 회사는 회사 규모가 작아 별도로 IT 전산팀을 운영하지 않고, 그룹웨어 호스팅 서비스 등을 사용하지 않는 대신 '협업 툴'인 슬랙(slack)[33]을 이용하여 직원들 간의 업무 관련 내용 공유 및 메신저 기능을 사용하고 있는 것이 확인되었다. 슬랙 웹페이지에 저장된 직원들 간의 대화 내용을 확보하기 위하여 추출 방법을 찾아보았으나 협업 툴인 슬랙(slack)은 각 구독 서비스 레벨(플랜)별로 데이터 Export 제한을 두고 있었고, 현재 회사가 구독하고 있는 레벨에서는 개인 간의 대화 내용에 대한 데이터 추출기능을 지원하지 않는 것이 확인되었다.

제 2 절 사례별 압수 절차 및 방법

1. 압수 사례 1

압수 사례 1의 쟁점은 임직원 PC에서 사건과 관련된 문서파일을 압수하는 것 이외에, PC에서 발견된 PC 카카오톡 및 사내 메신저 데이터에서 사건과 관련된 정보만을 선별하여 압수하는 것이다. 기업에서는 DLP[34]

---

33) Slack Technologies가 개발한 클라우드 기반 협업용 도구이다. 웹 앱이며, 직장인들의 업무용 도구로 많이 사용되고 채팅, 워크플레이스 등의 기능을 제공한다. (출처 : https://namu.wiki/w/%EC%8A%AC%EB%9E%99 - '슬랙')

34) Data Loss Prevention의 약자로 데이터 손실을 방지해 주는 기술로 데이터의 흐름 즉, 데이터 이동 경로를 감시하여 기업 내부의 중요 정보와 데이터 유출을 감시하고 기록하며 데이터 이동 경로를 감시 중에 유출이 감지되었을 땐 이를 경고 혹은 차단하면서 데이터를 보호한다. (출처 : 한국정보통신기술협회 정보통신용어사전 - 'DLP')

솔루션을 통해 PC에 설치할 수 있는 메신저 사용을 제한하고 사내 데이터가 외부로 유출되는 것을 방지하고 추적한다. 그러나 제한 정책을 두지 않는 곳에서는 PC 카카오톡, 텔레그램 등 여러 외부 메신저들이 발견되기도 한다. 해당 압수 현장의 피압수처도 별도의 DLP 솔루션을 사용하고 있지 않아, 사내 메신저 외에 PC 카카오톡이 업무용으로 사용 중인 것을 확인할 수 있었다.

메신저는 대화 내용 등의 수·발신 데이터를 서버에 저장하여 관리하기도 하지만 저장 공간 등의 한계 등 이유로 수·발신 데이터를 PC에 저장하기도 하며 프로그램 구성에 따라 차이는 있으나 데이터를 주로 텍스트 형태 또는 SQLite DB 형태 등으로 저장하고 있다. PC에서 발견되는 PC 카카오톡 데이터 또한 카카오톡 서버에 저장되는 것과는 별도로 PC를 통해 확인 카카오톡 데이터들을 PC 내부에 EDB 확장자를 가진 암호화된 데이터베이스 형태로 저장하고 있다.

메신저는 일상적으로 사용되므로 메신저 데이터 속에는 사건과 관련된 대화 내용뿐만 아니라 관련성이 없는 개인적인 내용도 포함되어 있다. 따라서 현장에서는 메신저 데이터가 담긴 데이터베이스 파일 등을 확인하고 사건과 관련된 내용만을 선별하는 압수가 진행되어야 한다. 그러나 현재 포렌식 수사관들에게 배포된 현장용 압수 도구는 PC 속에서 발견되는 메신저 데이터에 대한 현장 선별기능을 지원하지 않고 있다.

해당 사건에서도 도구 등의 기술적인 한계로 현장 선별을 진행하지 못하였다. 따라서 PC 카카오톡의 경우 암호화된 형태로 저장된 수·발신 데이터 전체 폴더를 추출한 뒤 봉인하고, 추후 피압수자 참관하에 데이터 복호화 및 선별하는 방식으로 압수를 진행하였다. 또한, 텍스트 형태로 저장된 해당 회사의 사내 메신저 데이터도 전체가 내용이 담긴 텍스트 파일을 복제한 이후 참관 과정에서 필요한 부분을 제외하고 사건 관련 대화만 오피스 파일 형태로 저장하는 방식으로 선별 압수 절차를 진행하였다.

2. 압수 사례 2

압수 사례 2의 쟁점은 회사가 보관하고 있는 OOO 측량 관련 계측데이터가 웹 기반의 사용자 환경에서 추출되지 않아 회사가 운영하는 ERP 서버 데이터베이스에 직접 접속하여 관련 정보에 대한 선별 압수가 필요한 상황이다. 기업들이 사용하고 있는 ERP 시스템의 데이터 저장 구조는 일반적으로 관계형 데이터베이스[35] 형태로 구성되어 있다. 데이터베이스는 RDBMS(관계형 데이터베이스 관리시스템)에 의해 관리·운영되며 권한 있는 사용자들이 데이터베이스 내의 정보에 접근하여 사용할 수 있도록 지원한다. 대표적으로 사용되는 RDBMS의 종류에는 ORACLE, MYSQL SQL-SERVER 등이 있으며 관리자 화면에서 SQL[36] 쿼리 명령을 통해 전체 데이터 조회가 가능하다.

해당 사건에서는 전산 관리자로부터 ERP 데이터베이스 서버 접속 권한을 부여받은 뒤 서버의 데이터베이스에 직접 접속하여 압수수색을 실시하였다. 해당 기업의 ERP 시스템은 내부 데이터베이스를 오라클 DBMS로 구축하여 모듈별로 관련 데이터를 데이터베이스 테이블에 저장하고 있었다. 수색을 통해 압수 대상인 계측데이터가 특정 데이터베이스 테이블에 저장된 것을 확인하였으며, 데이터베이스 원본 압수수색을 통해 사용자 화면에서 확인되는 5년 기간 데이터보다 더 많은 기간의 데이터를 확보할 수 있었다.

---

35) 관계형 모델에 따라 키와 값을 table 형태로 구성한 데이터베이스, 관계형 데이터베이스는 데이터를 단순한 table 형태로 저장하여 일반적으로 사용자가 이해하기 쉬우며, 구조화된 질의 언어 SQL을 이용하여 저장된 데이터를 관리(검색, 추가, 갱신, 삭제)함으로써 데이터를 쉽게 이용할 수 있다는 장점이 있다. 그뿐만 아니라 특정 표(table)에 대한 접근 권한 관리 등 다양한 보안 기능을 제공하여 데이터 공유 환경에서 효과적이다. (출처 : 한국정보통신기술협회 정보통신용어사전 - '관계형 데이터베이스')

36) 관계형 데이터베이스 관리하기 위해 설계된 특수 목적의 프로그래밍 언어이다. (출처 : https://aws.amazon.com/ko/what-is/sql/ - 'SQL')

그러나 현재 포렌식 수사관들이 현장용으로 사용하는 대다수 포렌식 도구는 데이터베이스 접속 및 쿼리를 통한 DB 선별 압수 기능을 지원하지 않는다. 따라서 본 건 압수 현장에서는 피압수처의 전산팀에서 사용하는 데이터베이스 관리 도구를 이용하였다. 계측데이터를 조회하는 SQL 쿼리(Query)[37]를 직접 작성하여 데이터를 조회한 뒤 오피스 파일 형태로 데이터를 추출하고 추출된 파일을 별도 포렌식 도구로 이미징하는 방식으로 선별 압수를 진행하였다. 또한, 오피스 파일로 선별된 압수된 정보에 대한 원본과의 동일성· 무결성을 확보하기 위해 서버 접속 정보 등을 촬영하고 메모로 남기는 한편, 사용된 쿼리 및 로그 데이터 등도 함께 수집하였다.

3. 압수 사례 3

압수 사례 3의 쟁점은 피압수처 회사가 이용하고 있는 '협업 툴'인 슬랙(Slack)에서 사건과 관련된 대화 내용을 압수하는 것이다. 코로나19 팬데믹으로 인해 재택근무로 전환한 기업이 많아지면서 IT 회사를 중심으로 '협업 툴'[38]을 사용하는 곳이 많아졌다. '협업 툴'은 회사가 직원에게 시간 및 장소, 작업 방식 등을 선택할 수 있도록 하여 업무 유연성을 늘려준다는 장점이 있어 재택근무가 확산하는 시기부터 점점 사용량이 증가하였으며 현재까지도 많은 기업에서 사용되고 있다. 그러나 수사기관의 관점에서 '협업 툴'은 압수수색에 제약이 되기도 한다. 그 이유는 '협업 툴' 구독자는 웹페이지 서비스 이용 권한만 있을 뿐 데이터 관리 주체가 아니므로 내부 구조에 대한 접근이 제한되어 있기 때문이다. 따라서 '협업 툴'에 저장된 정보에 대한 압수는 데이터 확인 및 추출에 있어서 많은 제약을 받

---

37) 특정한 정보를 요청하는 문자열을 기반으로 질의문이다. 쿼리는 대개 데이터베이스에 저장된 특정한 내용을 찾기 위해 사용된다.
(출처 : https://namu.wiki/w/%EC%BF%BC%EB%A6%AC - '쿼리')

38) 서비스용 소프트웨어형 클라우드를 기반으로 팀 커뮤니케이션, 할 일 및 일정 관리, 파일 공유, 노트작성, 프로젝트 관리 등 지식노동자들의 원활한 업무를 도와주는 서비스를 의미한다. 유명한 '협업 툴'로는 슬랙, microsoft teams, notion 등이 있다. (출처 : https://namu.wiki/w/%ED%98%91%EC%97%85%ED%88%B4 - '협업 툴')

을 수밖에 없다.

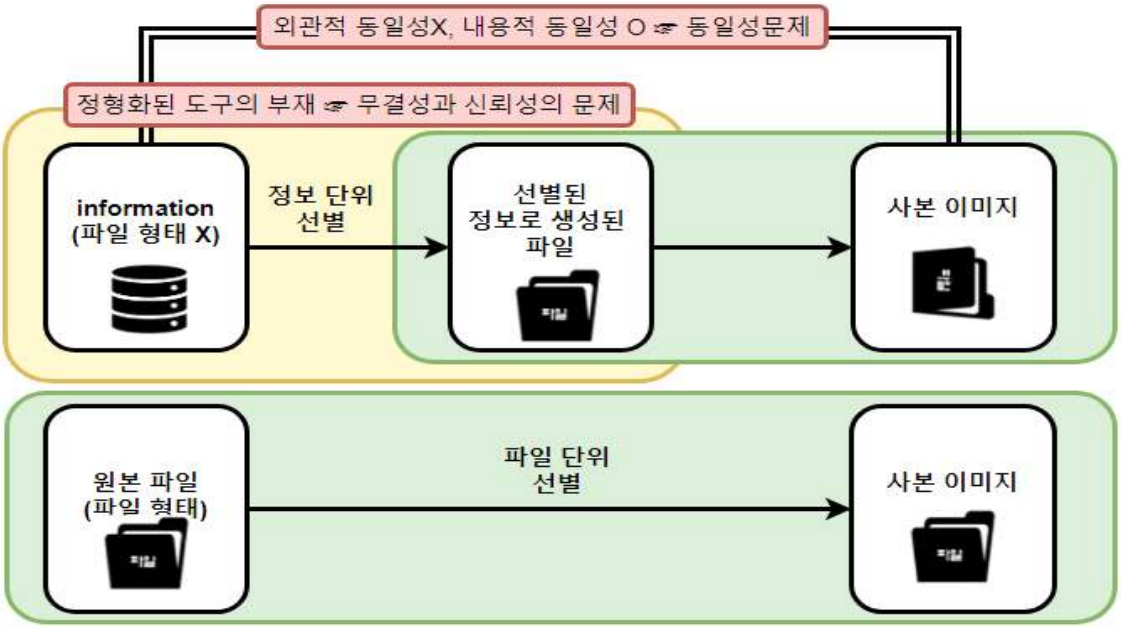
그러나 현재 포렌식 수사관들이 현장용으로 사용하는 대다수 도구는 파일이 아닌 웹상에서 확인되는 정보에 대한 압수기능을 지원하지 않는다. 따라서 웹에 있는 정보를 파일 형태로 추출하여 논리이미징하는 형태로 압수하고 있다. 그러나 압수 대상 시스템의 한계로 데이터 추출 자체가 어렵고, 협조가 원활하지 않은 상태에서는 증거 수집 방법에 제한을 받을 수밖에 없다. 위 사례에서도 현재 회사가 구독하고 있는 레벨에서는 개인 간의 대화 내용에 대한 데이터 Export 기능을 사용할 수 없었으며, 회사로부터도 별다른 협조를 얻을 수 없어 슬랙에 저장된 대화 내용에 대하여 피압수자의 참관 하에 각 대화 화면별로 캡처를 진행하고 캡처한 그림 파일을 이미징하는 방식으로 압수를 진행하였다.

4. 각 압수 사례에서 확인된 문제점

압수 사례 1과 2를 통하여 압수 대상 정보는 데이터베이스 등 여러 가지 형태로 저장되어 있을 수 있으며, 선별 압수의 원칙에 따라 사건과 관련된 정보만 분할해서 가져오거나 일부만 떼어내는 방식으로 선별 압수해야 하는 상황[39]이 존재함을 확인하였다. 따라서 데이터베이스와 같이 사건 관련 정보와 무관한 정보가 혼재된 매체를 압수할 때는 사건과 관련된 정보만을 선별하고 추출하는 작업이 필수적이며, 현장 선별 절차를 거쳐 최종 압수하게 되는 데이터는 매체에 원래 존재하던 파일이 아닌 현장 선별 과정을 거쳐 압수 당일 생성한 파일일 수도 있다는 점을 확인하였다. 압수 사례 3에서는 압수 대상 데이터의 저장 형태 및 시스템 환경에 따라 압수 대상 정보가 정보저장매체에 저장된 단일 파일 형태가 아닐 수 있으며, 현장 상황에 따라서 캡처 방식 등 다양한 방법으로 선별 압수가 가능하다는 것을 확인하였다. 결과적으로 정보의 선별 압수는 원본과 사본이

39) 이주호·이태명, “디지털증거의 선별압수에 따른 원본성 및 동일성 증명에 관한 연구” 디지털포렌식연구 (2020) p.254

내용적 동일하나 외형적으로는 다를 수 있어 동일성 문제가 발생할 수 있다는 점을 발견하였다.



[그림 5] 정보 단위 선별 압수 절차

또한, 압수 사례 1~3번에서 공통으로 확인된 문제점은 기존의 파일 단위 선별 압수가 가능한 상황에서는 하나의 도구 프로세스 안에서 선별 및 압수가 진행되었던 것과는 달리, 정보 단위 선별이 필요한 상황에서는 전체 압수 과정 중 일부 절차가 현장용 포렌식 프로그램 밖에서 진행되고 있다는 점이다. 이는 현재 현장용으로 사용되는 압수 도구들이 데이터베이스를 선별하고, 웹상에서만 확인되는 정보를 압수하는 기능을 지원하지 않기 때문이다. 결과적으로 현재 정보 단위 선별 압수 절차는 도구의 한계로 인해 [그림 5]와 같이 데이터를 분할·추출·캡처하여 파일로 만드는 '파일화 과정'과 파일로 저장된 정보를 이미징하는 '이미징 과정' 두 단계로 구분되어 진행되고 있다는 것을 확인하였다. 따라서 디지털 증거 압수 단계에서 동일성, 무결성, 신뢰성에 유의하여 절차를 수행하지 않는다면 법정에서 [그림 5]와 같이 증거능력과 관련된 다툼이 발생할 수 있을 것으로 보인다.

제 4 장 디지털 증거의 증거능력 관련 쟁점

제 1 절 증거능력 인정요건 관련 판례

수사기관이 압수 현장에서 수집한 디지털 증거가 법정에서 증거로서 가치를 인정받기 위해서는 증거 수집 절차의 적법성이 확보되어야 하며 동일성, 무결성, 신뢰성 등의 증거능력 문제 또한 해결되어야 한다. 이는 디지털 증거가 유체물인 증거와는 다르게 원본의 복제 또는 변경이 쉽게 가능한 특성이 있기 때문이다. 증거능력 개별 요건에 대해서는 학자들의 다양한 의견들이 있으나 핵심적인 내용은 크게 다르지 않다.

경찰청과 대검찰청의 훈령과 지침에서도 디지털 증거의 무결성과 신뢰성, 보관의 연속성, 동일성 등에 대하여 각각 규정하고 있다. 각 수사기관의 훈령과 지침에 규정된 디지털 증거의 증거능력 인정요건들은 디지털 증거가 쟁점이 된 판례들을 통해 정립되어 규정 형태로 발전한 것이다. 디지털 증거의 증거능력 인정요건과 관련된 대표적 판례는 대법원 2007. 12. 13. 선고 2007도7257 판결 이른바 '일심회 사건', 대법원 2013. 7. 26. 선고 2013도2511 판결인 '왕재산 사건'이 있다.

1. 일심회 사건

'일심회 사건'에서 검찰은 피고인들을 국가보안법 위반죄 등 혐의로 기소하였다. 검찰은 피고인들이 '일심회'라는 이적단체를 구성 및 가입하여 활동한 사실과 함께 국가기밀을 탐지·수집하고 북한 공작원으로부터 지령을 받은 사실 등 국가보안법 위반죄과 관련하여 기소한 내용을 입증하기 위하여 압수한 디지털 저장매체로부터 이미징한 이미지파일에서 출력한 문건을 법원에 증거로 제출하였다. 그러나 피고인 측은 수사 과정에서 원본이 변경되었을 가능성이 있다고 주장하며 디지털 증거의 증거능력을 문제

삼았다.[40]

대법원은 이 사건에서 “디지털 저장매체로부터 출력된 문건이 증거로 사용되기 위해서는 디지털 저장매체 원본에 저장된 내용과 출력된 문건의 동일성이 인정되어야 하고, 이를 위해서는 디지털 저장매체 원본이 압수 시부터 문건 출력 시까지 변경되지 않았음이 담보되어야 한다.”[41]라고 판시하여 증거능력을 인정하기 위한 특별한 요건으로 동일성 및 무결성을 요구하였다. 이와 함께 “디지털 저장매체 원본과 하드카피 또는 이미징한 매체 사이에 자료의 동일성도 확인하는 과정에서 이용한 컴퓨터의 기계적 정확성, 프로그램의 신뢰성, 입력·처리·출력의 각 단계에서 조작자의 전문적인 기술 능력과 정확성이 담보되어야 한다.”[42]라고 판시하여 신뢰성의 개념 또한 정의하였다. ‘일심회 사건’ 판결을 통해서 확인된 디지털 증거의 증거능력 인정요건인 동일성, 무결성, 신뢰성과 관련된 원문의 내용은 다음과 같다.

대법원 2007. 12. 13. 선고 2007도7257 판결 (일심회 사건)[43]

압수물인 디지털 저장매체로부터 출력된 문건이 증거로 사용되기 위해서는 **디지털 저장매체 원본에 저장된 내용과 출력된 문건의 동일성이 인정되어야 할 것인데**, 그 동일성을 인정하기 위해서는 **디지털 저장매체 원본이 압수된 이후 문건 출력에 이르기까지 변경되지 않았음이 담보**되어야 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 동

40) 손지영·김주석, “디지털 증거의 증거능력 판단에 관한 연구” 대법원사법정책연구원연구총서 2015-08호 p.127
41) 국가법령정보센터 : 대법원 2007. 12. 13. 선고 2007도7257 판결
42) 국가법령정보센터 : 대법원 2007. 12. 13. 선고 2007도7257 판결

일성도 인정되어야 한다. 나아가 법원 감정을 통해 디지털 저장매체 원본 혹은 '하드카피'·'이미징'한 매체에 저장된 내용과 출력된 문건의 동일성을 확인하는 과정에서 이용된 컴퓨터의 기계적 정확성, 프로그램의 신뢰성, 입력·처리·출력의 각 단계에서 조작자의 전문적인 기술능력과 정확성이 담보되어야 한다.

기록에 의하여 살펴보면, 국가정보원에서 피고인들 혹은 가족, 직원이 입회한 상태에서 원심 판시 각 디지털 저장매체를 압수한 다음 입회자의 서명을 받아 봉인하였고, 국가정보원에서 각 디지털 저장매체에 저장된 자료를 조사할 때 피고인들 입회하에 피고인들의 서명무인을 받아 봉인 상태 확인, 봉인 해제, 재봉인하였으며, 이러한 전 과정을 모두 녹화한 사실, 각 디지털 저장매체가 봉인된 상태에서 서울중앙지방검찰청에 송치된 후 피고인들이 입회한 상태에서 봉인을 풀고 세계적으로 인정받는 프로그램을 이용하여 이미징 작업을 하였는데, 디지털 저장매체 원본의 해쉬(Hash) 값과 이미징 작업을 통해 생성된 파일의 해쉬 값이 동일한 사실, 제1심 법원은 피고인들 및 검사, 변호인이 모두 참여한 가운데 검증을 실시하여 이미징 작업을 통해 생성된 파일의 내용과 출력된 문건에 기재된 내용이 동일함을 확인한 사실을 알 수 있는바, 그렇다면 출력된 문건은 압수된 디지털 저장매체 원본에 저장되었던 내용과 동일한 것으로 인정할 수 있어 증거로 사용할 수 있고, 같은 취지의 원심의 판단은 정당하다.

2. 왕재산 사건

'왕재산 사건'에서 검찰은 피고인들을 각각 국가기밀 탐지·수집, 회합, 이

43) 국가법령정보센터 : 대법원 2007. 12. 13. 선고 2007도7257 판결, "국가보안법위반(간첩)·국가보안법위반(잠입·탈출)·국가보안법위반(잠입·탈출)교사·국가보안법위반(찬양·고무등)·국가보안법위반(회합·통신등)·국가보안법위반(회합·통신등)교사·국가보안법위반(자진지원·금품수수)('일심회' 국가보안법 위반 사건)"

적표현물 소지, 편의 제공, 통신 연락, 제3국에서의 특수 잠입·탈출 등 국가보안법 위반 혐의로 기소하면서 피고인들의 범죄사실을 입증하기 위하여 압수한 디지털 저장매체로부터 이미징한 이미지파일에서 출력한 문건을 법원에 증거로 제출하였다. 그러나 이에 대하여 피고인 측에서는 해시값 산출 누락 등의 이유로 제출된 디지털 증거의 증거능력을 문제 삼았다.[44]

대법원은 이 사건에서 "압수물인 컴퓨터용 디스크 그 밖에 이와 비슷한 정보저장매체에 입력하여 기억된 문자정보 또는 그 출력물을 증거로 사용하기 위해서는 정보저장매체 원본에 저장된 내용과 출력 문건의 동일성이 인정되어야 하고, 이를 위해서는 정보저장매체 원본이 압수 시부터 문건 출력 시까지 변경되지 않았다는 사정, 즉 무결성이 담보되어야 한다."[45]라고 하면서 동일성과 함께 '일심회 사건' 판례에서는 사용하지 않았던 무결성이라는 표현을 처음 사용하였으며, 디지털 증거의 동일성 요건은 무결성 요건과 상호 보완적인 관계라는 것을 명시하였다.

또한, 동일성·무결성 증명 방법에 관하여 해시 검증 프로그램을 이용하여 "해쉬(Hash)값이 동일함을 검증하는 것이 원칙이나, 그와 같은 방법에 의한 증명이 불가능하거나 현저히 곤란한 경우에는, 디지털 증거 압수 절차에 참여한 수사관이나 전문가 등의 증언에 의해 정보저장매체 원본과 하드카피 또는 이미징한 매체 사이의 해시값이 동일하거나 정보저장매체 원본이 최초 압수 시부터 밀봉되어 증거 제출 시까지 전혀 변경되지 않았다는 등의 사정을 증명하는 방법 또는 법원이 그 원본에 저장된 자료와 증거로 제출된 출력 문건을 대조하는 방법 등으로도 그와 같은 무결성·동일성을 인정할 수 있으며, 반드시 압수·수색 과정을 촬영한 영상녹화물 재생 등의 방법으로만 증명하여야 한다고 볼 것은 아니다."[46]라고 하여

---

44) 손지영·김주석, "디지털 증거의 증거능력 판단에 관한 연구" 대법원사법정책연구원연구총서 2015-08호 p.129
45) 국가법령정보센터 : 대법원 2013. 7. 26. 선고 2013도2511 판결
46) 국가법령정보센터 : 대법원 2013. 7. 26. 선고 2013도2511 판결

무결성·동일성에 대한 증명은 다양한 방법으로도 가능하다는 것을 명시하였다. ‘일심회 사건’ 판결을 통해 확인된 디지털 증거의 증거능력 인정요건으로 동일성, 무결성, 신뢰성에 관한 내용은 ‘왕재산 사건’ 판결에서도 재차 확인된다. ‘왕재산 사건’의 판결 요지는 다음과 같다.

대법원 2013. 7. 26. 선고 2013도2511 판결 (왕재산 사건)[47]

압수물인 컴퓨터용 디스크 그 밖에 이와 비슷한 정보저장매체(이하 ‘정보저장매체’라고만 한다)에 입력하여 기억된 문자정보 또는 그 출력물(이하 ‘출력 문건’이라 한다)을 증거로 사용하기 위해서는 **정보저장매체 원본에 저장된 내용과 출력 문건의 동일성이 인정되어야 하고, 이를 위해서는 정보저장매체 원본이 압수 시부터 문건 출력 시까지 변경되지 않았다는 사정, 즉 무결성이 담보되어야 한다.**

특히 정보저장매체 원본을 대신하여 저장매체에 저장된 자료를 ‘하드카피’ 또는 ‘이미징’한 매체로부터 출력한 문건의 경우에는 정보저장매체 원본과 ‘하드카피’ 또는 ‘이미징’한 매체 사이에 자료의 동일성도 인정되어야 할 뿐만 아니라, **이를 확인하는 과정에서 이용한 컴퓨터의 기계적 정확성, 프로그램의 신뢰성, 입력·처리·출력의 각 단계에서 조작자의 전문적인 기술능력과 정확성이 담보되어야 한다**.

이 경우 출력 문건과 정보저장매체에 저장된 자료가 동일하고 정보저장매체 원본이 문건 출력 시까지 변경되지 않았다는 점은, 피압수·수색 당사자가 정보저장매체 원본과 ‘하드카피’ 또는 ‘이미징’한 매체의 해쉬(Hash) 값이 동일하다는 취지로 서명한 확인서면을 교부받아 법원에 제출하는 방법에 의하여 증명하는 것이 원칙이나, 그와 같은 방법에 의한 증명이 불가능하거나 현저히 곤란한 경우에는, 정보저장매체 원본에 대한 압수, 봉인, 봉인해제, ‘하드카피’ 또는 ‘이미징’ 등 일련의 절차에

참여한 수사관이나 전문가 등의 증언에 의해 정보저장매체 원본과 '하드카피' 또는 '이미징'한 매체 사이의 해쉬 값이 동일하다거나 정보저장매체 원본이 최초 압수 시부터 밀봉되어 증거 제출 시까지 전혀 변경되지 않았다는 등의 사정을 증명하는 방법 또는 법원이 그 원본에 저장된 자료와 증거로 제출된 출력 문건을 대조하는 방법 등으로도 그와 같은 무결성·동일성을 인정할 수 있으며, 반드시 압수·수색 과정을 촬영한 영상녹화물 재생 등의 방법으로만 증명하여야 한다고 볼 것은 아니다.

제 2 절 디지털 증거의 증거능력 인정요건

1. 동일성

일반적으로 디지털 정보는 복제뿐만 아니라 변경 및 삭제도 쉬운 특성이 있으므로 증거를 취득하고 보존할 때 훼손이나 조작 가능성을 방지하여야 할 필요성이 제기된다. 또한, 증거 수집 및 분석과정에서 부주의로 인한 증거의 훼손이 발생할 가능성도 있으므로 수집한 디지털 증거의 원본 동일성에 관한 문제는 증거능력 판단에서 중요한 쟁점이다.[48] 디지털 증거의 증거능력 인정요건에서의 동일성 문제의 핵심 쟁점은 디지털 증거가 원본이 아닌 복제본이 증거로 제출된 경우 그 원본과 복제본이 서로 일치하여야 한다는 것이다.[49]

---

47) 국가법령정보센터 : 대법원 2013. 7. 26. 선고 2013도2511 판결, "국가보안법 위반(반국가단체의 구성등)·국가보안법 위반(간첩)·국가보안법 위반(자진지원·금품수수)·국가보안법 위반(특수잠입·탈출)·국가보안법 위반(찬양·고무등)·국가보안법 위반(회합·통신등)·국가보안법 위반(편의제공)"

48) 손지영·김주석, "디지털 증거의 증거능력 판단에 관한 연구." [JPRI] 연구보고서(2015) p.17

49) 박혁수, "개정형사소송법상 디지털 증거의 증거능력" 해외연수검사논문집(2009. 7) p.384

형사소송법 제106조 제3항은 디지털 증거의 원칙적 선별 압수 및 예외적 매체 압수에 관한 내용을 선언하고 있다. 이에 따라 포렌식 수사관들은 압수 현장에서 포렌식 도구를 이용하여 사건과 관련된 파일만을 선별하고 선별된 파일만을 논리이미징하는 방식으로 디지털 증거를 수집하고 있다. 결과적으로 실무상 선별 압수에서의 원본과의 동일성이란 원본 매체에 있던 원본 파일과 선별 압수한 논리이미지에 포함된 사본 파일이 동일하다는 것을 의미한다.

동일성 입증에는 일반적으로 해시 함수[50]를 활용한다. '일심회 사건' 및 '왕재산 사건' 판결에서도 "출력 문건과 정보저장매체에 저장된 자료가 동일하고 정보저장매체 원본이 문건 출력 시까지 변경되지 않았다는 점은, 피압수 당사자가 정보저장매체 원본과 하드카피 또는 이미징한 매체의 해시(Hash)값이 동일하다는 취지로 서명한 확인서면을 교부받아 법원에 제출하는 방법에 의하여 증명하는 것이 원칙"[51]이라고 규정하였다. "검찰의 디지털 증거의 수집·분석 및 관리 규정" 제5조에도 "디지털 증거는 법정에서 원본과의 동일성을 재현하거나 검증하는 데 지장이 초래되지 않도록 수집·분석 및 관리되어야 한다."라고 규정하여 동일성 요건을 별도로 규정하고 있다.

2. 무결성

디지털 증거 수집 절차에 있어서 무결성이란 최초 수집된 원본성을 가진 증거가 법정에 제출되기까지 변경이나 훼손이 없어야 한다는 것을 말한다. 디지털 증거가 수집되고 분석 및 보관을 거쳐 법원에 제출되기까지는 많은 사람의 행위가 개입된다. 따라서 각 행위마다 압수된 원본 데이터가

---

50) 해시 알고리즘(hash algorithm) 또는 해시 함수 알고리즘(hash函數algorithm)은 임의의 길이의 데이터를 고정된 길이의 데이터로 매핑하는 함수이다.
(출처 : 한국정보통신기술협회 정보통신용어사전 - '해시 함수')
51) 국가법령정보센터 : 대법원 2007. 12. 13. 선고 2007도7257 판결

무결하게 유지되고 있다는 절차적 보증이 필요하다.[52] 동일성과 원본성이 저장매체에 저장된 원본 정보를 디지털 증거로 수집하는 과정까지를 다루는 문제였다면 무결성의 문제는 수사기관에 의해 원본과 동일하게 수집된 증거가 법정에 제출되기까지의 증거처리 및 보관 과정에 관한 문제인 것이다.

무결성과 관련된 판례 중 '일심회 사건' 판결에서는 무결성 개념을 언급하고 단어에 대한 직접적인 언급은 없었으나, '왕재산 사건' 판결에서는 "압수물인 컴퓨터용 디스크 그 밖에 이와 비슷한 정보저장매체에 기억된 문자 정보 또는 그 출력물을 증거로 사용하기 위해서는 정보저장매체 원본에 저장된 내용과 출력 문건의 동일성이 인정되어야 하고, 이를 위해서는 정보저장매체 원본이 압수 시부터 문건 출력 시까지 변경되지 않았다는 사정, 즉 무결성이 담보되어야 한다."[53]라고 판시하면서 무결성 용어를 처음으로 언급하였다.

실무에서는 선별된 디지털 증거의 무결성을 보완하기 위하여 피압수자 참여하에 선별 완료된 디지털 증거에 대하여 해시값을 계산하고, 해시값이 기재된 '현장조사확인서'에 참여인의 서명을 받고 있다. 또한, 법정에서 무결성에 대하여 다툼이 있는 경우 현장에서 압수 절차를 수행한 포렌식 수사관이 법정 증언 절차 등을 통하여 압수한 이미지 파일 및 개별 파일의 해시값과 피압수자에게 교부한 이미지 파일과 개별 파일의 해시값을 비교하는 방식으로 무결성을 검증하고 있다. "검찰의 디지털 증거의 수집·분석 및 관리 규정" 제6조에도 "디지털 증거는 압수·수색·검증한 때로부터 법정에 제출하는 때까지 훼손 또는 변경되지 아니하여야 한다."라는 무결성 요건을 별도로 규정하고 있다.

---

52) 양근원, "디지털 증거의 특징과 증거법상의 문제 고찰" 경희법학 제41권 제1호 (2006. 6.) p.179
53) 국가법령정보센터 : 대법원 2013. 7. 26. 선고 2013도2511 판결

3. 신뢰성

디지털 증거는 변조가 용이하고 의도적, 비의도적 조작에 취약한 특성이 있으므로 신뢰성이 보장될 필요가 있다. 따라서 수집된 디지털 증거가 신뢰성을 인정받기 위해서는 디지털포렌식 절차가 전문가에 의해 진행되었다는 인적 신뢰성과 수집·분석과정에 검증된 도구가 사용되었다는 도구적 신뢰성이 요구된다. 또한, 증거가 수집된 이후에는 절차적으로 보관의 연속성을 보장하는 방법이 사용되어야 한다.[54]

'일심회 사건'과 '왕재산 사건'에서 법원은 "정보저장매체 원본을 대신하여 저장매체에 저장된 자료를 '하드카피' 또는 '이미징'한 매체로부터 출력한 문건의 경우에는 정보저장매체 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 기술 능력과 정확성이 담보되어야 한다."[55]라고 판시하여 신뢰성의 개념을 인정하였다.

도구적 신뢰성과 관련하여 현재 검찰에서는 현장용 디지털포렌식 압수도구로 개발된 'CFT'[56]와 'DFT'[57]를 현장 압수업무를 수행하는 디지털포렌 수사관들에게 배포하여 실무에서 적극적으로 활용하게 하고 있으며, 'EnCase'[58], 'X-Ways Forensics'[59] 등 해외에서 신뢰성이 입증된 유명 포렌식 도구 또한 구매하여 분석업무에 활용하고 있다.

인적 신뢰성과 관련하여 검찰에서는 디지털포렌식 담당 수사관을 지정하

---

54) 손지영·김주석, "디지털 증거의 증거능력 판단에 관한 연구" [JPRI] 연구보고서 (2015) p.33
55) 국가법령정보센터 : 대법원 2013. 7. 26. 선고 2013도2511 판결
56) Computer Forensic Tool, 국가보안기술연구소가 개발한 현장용 디지털포렌식 도구
57) Digital Forensic Tool, 국가보안기술연구소가 개발한 현장용 디지털포렌식 도구
58) Guidance Software 社가 개발한 디지털포렌식 분석 도구
59) X-ways Software Technology 社가 개발한 핵사 에디터 기반 디지털포렌식 분석도구

여 디지털 증거 압수·수색 및 분석, 기술적 자문, 법정 증언 등 디지털 증거의 수집 및 분석과 관련된 업무를 전담하게 하고 있으며, 디지털포렌식 수사관의 자격과 임명, 교육 등을 “디지털 증거의 수집·분석 및 관리 규정”에 명시하여 디지털포렌식 전문 수사관의 인력관리 및 전문성 강화를 위해 노력하고 있다. 검찰의 “디지털 증거의 수집·분석 및 관리 규정” 제7조에서도 “디지털 증거는 디지털포렌식 전문가에 의해 신뢰할 수 있는 도구와 방법으로 수집·분석 및 관리하여야 한다.”라는 신뢰성 요건을 별도로 규정한 것을 찾아볼 수 있다.

제 3 절 정보 선별 압수에서 증거능력 관련 쟁점

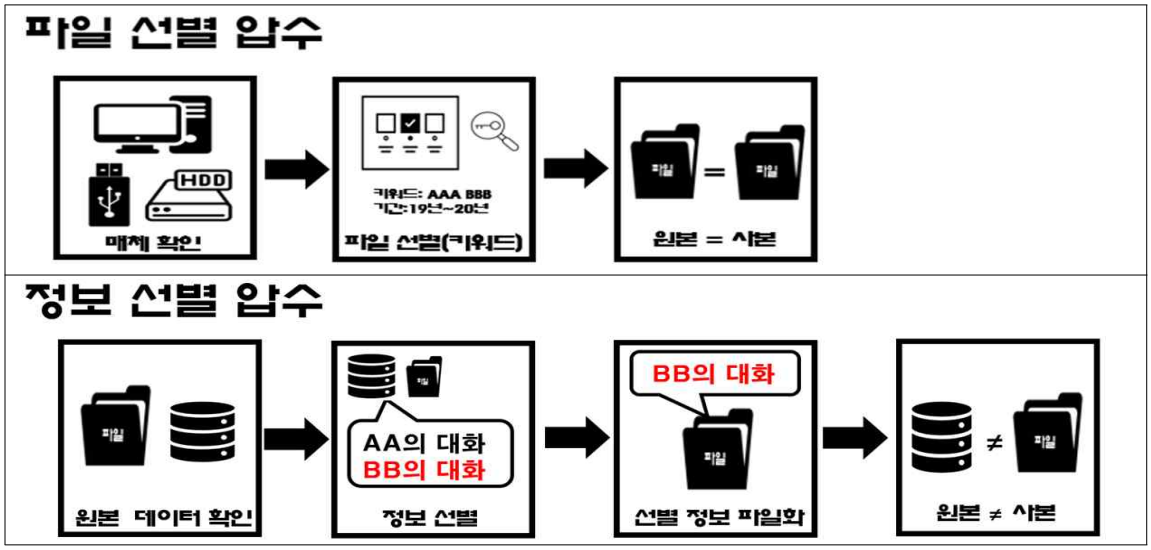
1. 동일성 관련 쟁점

디지털 증거는 복사를 통해 원본의 완벽한 복제가 가능하므로 특별한 사정이 없으면 원본와 사본이 정확히 일치한다. 따라서 일반적으로 디지털 증거에 대한 선별 압수는 원본과 동일하게 복제된 사본을 압수하는 형태로 진행되고 있다. 또한, 압수 과정에 피압수자를 참여시키고, 압수종료와 함께 이미지 파일 및 개별 파일들에 대한 해시값이 기재된 상세목록을 교부하며, ‘현장조사확인서’[60] 및 ‘참관 및 전자정보상세목록 교부 확인서’[61]에 서명을 받는 방식으로 원본과 사본의 동일성 문제를 보완하고 있다.

그러나 디지털 환경의 변화 따라 선별의 개념이 정보저장매체에서 파일 단위로 선별하는 것에서 정보 단위로 선별하는 것으로 변하고 있다. 데이터베이스와 같은 저장 형태는 대량의 정보를 효과적으로 관리하기 위한

60) 디지털포렌식 수사관이 포렌식 절차 수행 시 현장에서 작성하는 보고서로 현장에서 압수한 이미지파일 및 해시값에 관한 정보가 포함되어 있음 (국가법령정보센터 : 디지털 증거의 수집·분석 및 관리 규정 - 별지 제2호 서식)
61) 디지털포렌식 절차 참관 및 전자정보상세목록 교부에 관한 내용 그리고 압수한 이미지 파일과 그 해시값에 관한 정보가 포함되어 있음 (국가법령정보센터 : 디지털 증거의 수집·분석 및 관리 규정 - 별지 제8호 서식)

저장체계이므로 하나의 데이터베이스 파일 내에 수많은 정보를 가지고 있다. 따라서 사건과 관련 정보만을 추출하기 위해서는 SQL 쿼리 명령을 통해 정보 단위 선별이 필요하다. 또한, 클라우드 및 웹서비스 기반 시스템의 등장은 압수 대상 원본이 정보저장매체에 저장된 파일 형태가 아닐 수 있다는 것을 보여주었다. 클라우드 및 웹서비스에 존재하는 데이터를 수집하기 위해서는 원본 정보를 파일로 형태로 내려받아 저장하는 작업이 필수적으로 수반되기 때문이다. 그러므로 정보 단위 선별 압수는 정보저장매체에 이미 존재하였던 원본 파일을 그대로 복제하여 사본 형태로 압수하였던 기존의 압수방식과는 차이가 있다. 이는 기존의 해시값 검증 방법만으로는 동일성 증명이 어렵다는 것을 뜻하기도 한다. 파일 단위 선별 압수와 정보 단위 선별 압수의 차이점은 [그림 6]과 같다.



[그림 6] 파일 선별 압수와 정보 선별 압수 과정 비교 1

파일 단위 선별 압수 과정에서는 포렌식 도구를 이용하여 선별된 원본 파일을 시간 정보 등의 메타데이터까지 동일하게 복제하는 방식으로 압수하였다. 따라서 원본과 사본의 동일성은 해시 검증만으로도 확인되었다. 그러나 정보의 압수에서 원본이란 파일이 아닌 사건과 관련된 정보 자체를 말하고, 압수한 결과물은 데이터 분할 등의 선별 과정을 거쳐 현장에서 생성된 파일이므로 원본과 사본이 내용상 동일성은 있으나 외관상의

형태적 동일성[62]은 없는 형태이다. 따라서 기존의 해시 검증 방법만으로는 원본과 사본의 동일성을 증명하기 어려울 수밖에 없다.

2020년 발표된 이주호, 이태명의 논문[63]에서는 카카오톡 선별 압수와 관련하여 카카오톡 DB 자체를 원본으로 보지 않고 원본에서 관련 정보만 선별하여 생성한 파일을 원본으로 인정한 뒤 해시값을 계산하는 방법으로 동일성 문제를 해결하였다. 이는 수시로 변할 수 있는 데이터베이스의 특성상 스냅샷(Snapshot)[64]의 개념을 적용하여 원본의 개념을 새로 정의한 것으로 보인다. 그러나 원본은 압수 현장에서 확인된 정보 그 자체로 이해하여야 하며 선별 과정을 거쳐 파일로 생성한 오피스 파일 자체가 원본일 수는 없다.

정보 단위 선별 압수에 있어서 동일성 문제의 쟁점은 내용상의 동일성은 인정되나 외관상의 형태적 동일성이 없는 디지털 증거에 대하여 원본과의 동일성을 어떠한 방식으로 보완하여야 하는가에 대한 것이다. 2012년 발표된 이상원의 논문[65]에서는 “원본의 내용을 그대로 전사한 사본이 증거능력 인정받기 위해서는 ‘원본의 존재’, ‘원본 제출의 불능 또는 곤란’, ‘정확한 전사’라는 세 가지 요건을 갖추어야 한다.”라고 하였다.[66] 따라서 정보 단위 선별 압수 절차에서는 압수한 사본에 대한 원본 동일성 문제를 해시값을 검증하는 방법만으로 해결할 것이 아니라 압수 시 원본의 존재와 관련된 출처정보, 추출과정에 대한 자료 등을 함께 확보하는 방법을 통해 보완[67]해야 할 것으로 보인다.

---

62) 이주호·이태명, “디지털증거의 선별압수에 따른 원본성 및 동일성 증명에 관한 연구” 디지털포렌식연구 (2020. 9) p.263
63) 이주호·이태명, “디지털증거의 선별압수에 따른 원본성 및 동일성 증명에 관한 연구” 디지털포렌식연구 (2020. 9)
64) 사진을 찍듯이 특정 시점에 스토리지의 파일 시스템을 포착해 보관하는 기술을 의미한다. (출처 : https://ko.wikipedia.org/wiki/스냅샷_(기억_장치) - ‘스냅샷’)
65) 이상원, “전자증거와 원본증거의 법칙” 형사법의 신동향 (2012)
66) 이상원, “전자증거와 원본증거의 법칙” 형사법의 신동향 (2012) p.62
67) 박상준, “디지털 증거의 원본성과 동일성에 관한 기술적 고찰” 미발표논문 1p

2. 무결성 관련 쟁점

대검찰청 “디지털 증거의 수집·분석 및 관리 규정” 제6조는 디지털 증거의 무결성과 관련하여 “디지털 증거는 압수·수색·검증한 때로부터 법정에 제출하는 때까지 훼손 또는 변경되지 아니하여야 한다.”라고 규정하였다. 즉 무결성은 수사기관이 압수수색을 통해 사건 관련 디지털 증거를 수집한 이후부터 법정에 제출할 때까지 지켜져야 하며, 압수된 이후 증거물 보관 과정에 어떠한 변경도 되지 않았다는 것을 보증하기 위한 절차적인 방법 및 수단이 필요하다는 의미를 포함하고 있다.

무결성의 개념은 앞서 확인하였던 ‘왕재산 사건’ 판결에서 처음 언급된 개념이다. ‘왕재산 사건’ 판결에서는 “압수물인 컴퓨터용 디스크 그 밖에 이와 비슷한 정보저장매체에 입력하여 기억된 문자정보 또는 그 출력물을 증거로 사용하기 위해서는 정보저장매체 원본에 저장된 내용과 출력 문건의 동일성이 인정되어야 하고, 이를 위해서는 정보저장매체 원본이 압수 시부터 문건 출력 시까지 변경되지 않았다는 사정, 즉 무결성이 담보되어야 한다.”[68]고 판시하면서 무결성의 개념을 직접 언급하는 한편 동일성을 인정받기 위해서는 무결성이 전제되어야 한다고 하였다.

그러나 디지털 환경의 변화에 따라 디지털포렌식 절차에서 선별의 개념이 정보저장매체에서 파일 단위로 사건 관련 정보를 선별하는 것에서 정보 단위로 선별하는 것으로 변화하고 있다. 따라서 ‘왕재산 사건’ 판결을 통해 정립된 무결성 개념도 압수환경의 변화에 따라 변경이 필요할 것으로 보인다. 한국정보통신기술협회[69] 정보통신 용어사전에서는 무결성에 대하여 “신뢰할 수 있는 서비스 제공을 위해서 의도하지 않은 요인에 의해 데이터, 소프트웨어, 시스템 등이 변경되거나 손상되지 않고 완전성,

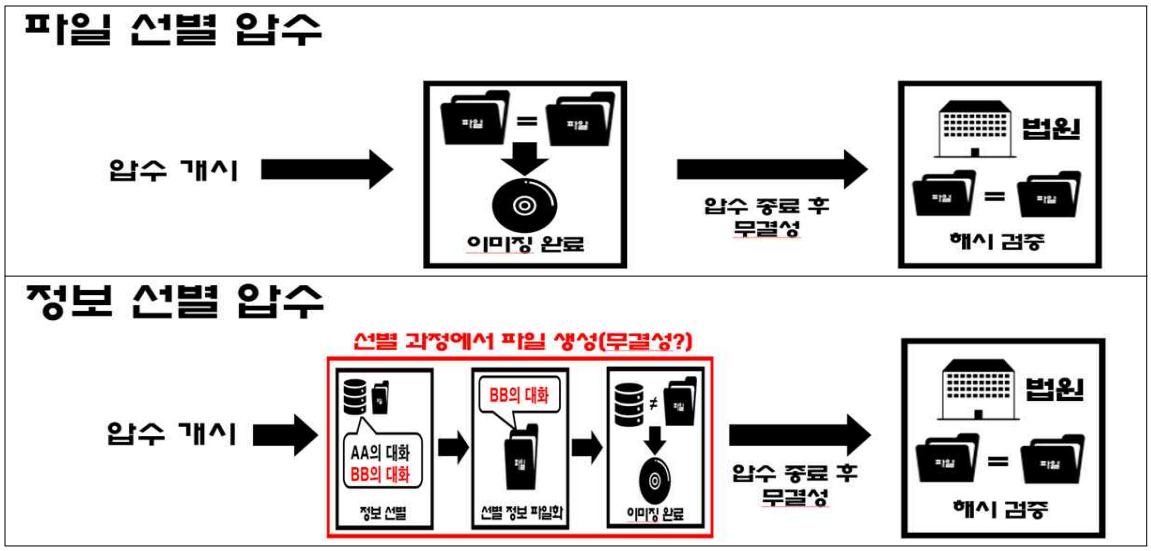
---

68) 국가법령정보센터 : 대법원 2013. 7. 26. 선고 2013도2511 판결

69) 1988년에 설립된 국내 유일의 정보통신 단체표준 제정기관이며 표준화 활동 및 표준 제품의 시험인증을 위해 만들어진 단체.
(출처 : https://ko.wikipedia.org/wiki/한국정보통신기술협회)

정확성, 일관성을 유지함을 보장하는 특성”[70]이라고 정의하고 있다. 정보의 압수는 원본 파일을 동일하게 복제하는 절차가 아닌 선별 과정 자체가 중요하므로 무결성은 수집된 이후 과정뿐만 아니라 원본 데이터에서 관련 정보만을 선별하여 수집하는 과정에서도 지켜져야 한다.

‘왕재산 사건’ 판결에서는 무결성의 범위를 수사기관이 전자정보를 압수한 이후부터 법정에 제출할 때까지로 한정하고, 압수 과정은 무결성의 범위에서 제외하였다. 해당 사건에서는 정보저장매체 원본을 봉인하여 압수한 이후 포렌식 도구를 이용하여 물리이미징하고 관련된 파일만 선별 복제하는 방식으로 포렌식 절차를 완료하였으며, 비트스트림 방식으로 물리이미지를 생성하는 단계와 파일 단위로 선별하는 절차가 검증된 포렌식 프로그램을 통해 진행되었다. 따라서 해당 판례에서는 압수 과정에서의 무결성은 고려되지 않은 것으로 보인다.



[그림 7] 파일 선별 압수와 정보 선별 압수 과정 비교 2

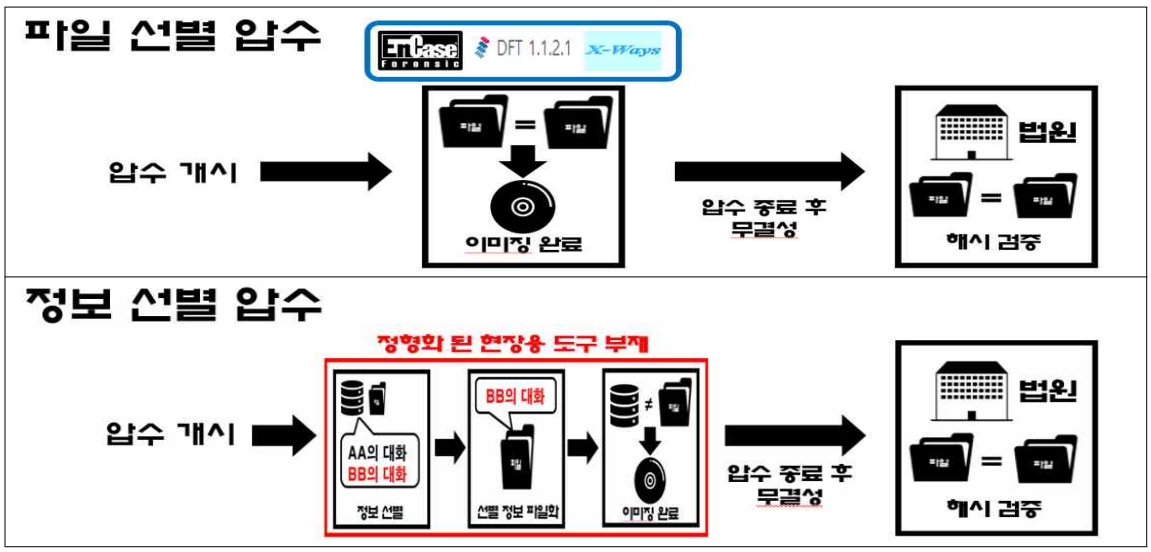
파일 단위의 선별 압수의 경우는 원본 파일과 사본 파일이 외관상이나 내용상으로 동일하다. 그러나 정보의 압수에서 압수 대상 원본은 파일 형태가 아니라 정보 자체이므로 [그림 7]과 같이 원본 정보와 사본 파일이

70) 한국정보통신기술협회 정보통신용어사전 - ‘무결성’

내용상으로는 같으나 외관상으로는 다를 수밖에 없다. 또한, 도구의 한계로 원본 데이터에서 정보만을 추출하고 선별하는 과정이 포렌식 도구 없이 수작업으로 진행되는 예도 있어 선별 과정에서 데이터 손상이나 누락이 발생할 가능성도 존재한다. 압수 과정에서도 무결성에 대한 개념이 필요한 현재 상황에서 정보 단위 선별 압수 과정을 통해 압수한 디지털 증거에 대한 무결성 보장을 위해서는 현장용 도구의 개발 등 기술적인 보완이 필요할 것으로 보인다.

3. 신뢰성 관련 쟁점

대검찰청 "디지털 증거의 수집·분석 및 관리 규정" 제7조는 디지털 증거의 신뢰성 관련하여 다음과 같이 규정하고 있다. "디지털 증거는 디지털 포렌식 전문가에 의해 신뢰할 수 있는 도구와 방법으로 수집·분석 및 관리하여야 한다." 이는 디지털포렌식 절차에서의 도구의 신뢰성과 포렌식 수사관의 자격을 정의한 것이다.



[그림 8] 파일 선별 압수와 정보 선별 압수 과정 비교 3

현재 포렌식 수사관들이 현장용으로 사용 중인 압수 도구들은 대부분 파일 선별기능에 중점을 두고 있다. 따라서 정보 단위 선별 압수 시 원본

선별 및 획득단계는 포렌식 이외의 도구 등을 이용하여 [그림 8]과 같이 진행되고 있다. 선별된 정보를 현장용 포렌식 도구가 저장할 수 있는 최소 단위인 파일 형태로 저장하고, 포렌식 도구를 이용하여 이미징 및 해시값을 생성하는 방식으로 디지털 증거 압수 절차가 진행되는 것이다. 그러나 압수 개시부터 이미징이 완료되어 종료되기까지 압수 전체 과정이 자동화된 도구를 통해 진행되는 것이 아니므로 압수 과정에서 데이터 누락이나 오염 등의 위험에 노출될 우려가 있다.

또한, 현재 실무에서는 정보 단위 선별 압수 과정에서 발생하는 동일성, 무결성, 신뢰성 등 증거능력과 관련된 문제들을 '현장조사확인서' 및 '참관 및 전자정보상세목록 교부 확인서'에 참여인의 서명을 받는 방식으로 보완하고 있다. 그러나 기술적으로 해결할 수 있는 문제를 참여인의 서명을 받는 방식으로만 보완하려는 것은 정확성과 절차를 중시하는 디지털포렌식 원칙과는 거리가 있어 보인다.

도구의 신뢰성 문제는 증거능력 요건에서도 중요한 부분이다. 신뢰성 있는 도구 사용은 동일성 및 무결성과도 연결된 문제이기 때문이다. 그러므로 압수 개시 단계부터 데이터 선별 및 획득까지 압수 전 과정을 하나의 프로세스로 담을 수 있는 현장용 도구가 필요하다. 이는 정보 단위로 선별 압수하는 과정에서 발생하는 외형적 동일성이 없는 사본에 관한 문제와 선별 작업이 포렌식 도구 없이 수작업으로 진행되어 선별 과정에서 데이터 손상이나 누락이 발생할 수 있는 문제들을 자연스럽게 해결할 수 있는 대안이 될 것이다. DFT와 같은 현장용 압수 도구의 개발과 꾸준한 연구가 현장 선별 압수 방식의 보편화에 영향을 준 것처럼 현재의 디지털 환경에 맞는 현장 도구 개발이 필요한 시점이다.

제 5 장 정보 선별 압수에 따른 증거능력 보완방안

제 1 절 기술적 보완방안

1. 도구 개발의 필요성

디지털 환경은 계속해서 변화하고 있다. 실시간으로 대량 생산되는 정보를 효율적으로 저장하고 관리하기 위하여 데이터베이스와 같이 하나의 저장체계 안에 대량의 데이터를 저장하는 형태가 많아질 것이며, 클라우드 및 웹서비스 기반 시스템 사용은 앞으로도 더욱 증가할 것이다. 따라서 디지털포렌식 수사관은 다양한 현장 상황에 유연하게 대응할 수 있는 능력을 길러야 한다.

정보 단위 선별 압수방식과 파일 단위 선별 압수방식은 기술적·절차적으로 다른 부분이 존재한다. 그러나 현재 압수수색 현장에서 사용되는 현장용 포렌식 압수 도구는 정보저장매체에 저장된 파일을 기간 및 키워드 검색을 통해 선별하는 기능을 위주로만 지원하고 있다. 그러므로 웹이나 클라우드, 데이터베이스에 저장된 정보에 대한 압수가 증가하고 있는 현시점에서 현장용 압수 도구의 기능 개선과 개발이 이루어지지 않는다면 증거능력과 관련된 문제가 지속적으로 발생할 수밖에 없다.

현장용 압수 도구의 역할은 사용자의 편리성뿐만 아니라 복잡한 압수 절차를 자동화하고 하나의 프로세스로 통합하여 수집된 증거의 신뢰성 보장했다는 점에 있다. 현재 검찰에서는 디지털포렌식 담당 수사관들에게 현장용 포렌식 압수 도구로 DFT를 배포하고 있다. 디지털포렌식 수사관이 압수장소에 도착하여 현장을 통제한 이후부터 사건과 관련된 파일을 선별 압수하고 상세 목록을 교부하기까지 모든 절차들을 자동화하는 기능을 갖춘 도구를 사용하는 것으로 압수 과정에 발생할 수 있는 증거능력 관련

문제들을 극복해온 것이다. 따라서 정보 단위 선별 압수가 필요한 상황에서도 압수수색이 개시된 이후부터 선별 과정을 거쳐 압수가 종료되기까지 모든 과정을 하나로 통합할 수 있는 도구가 필요하다. 또한, 해당 도구가 원본성 증명을 위한 신용적 정황성[71] 확보와 관련된 원본 메타데이터 자동 수집기능까지 갖춘다면 증거능력 관련된 동일성, 무결성, 신뢰성 문제를 극복하는 데에도 도움이 될 것이며 현장에서 압수수색을 진행하는 포렌식 수사관들에게도 많은 도움이 될 것이다.

도구의 개발과 연구를 위해서는 시간과 비용이 많이 소요된다. 그러나 실무에서 발생하는 문제를 개선하기 위한 도구의 개발과 지속적인 연구가 있었기 때문에 현재의 선별 압수 절차도 비교적 안정적으로 정착될 수 있었다. 따라서 정보 단위 선별 압수를 지원하는 현장용 도구의 개발이 필요하다. 이에 본 장에서는 앞에서 확인했던 압수 사례들 통해 현재 도입이 필요성 있는 '현장용 메신저 압수 도구', '현장용 데이터베이스 압수' 도구, '현장용 이미지 수집 도구'에 대한 개발을 제안하였다. 위 도구들의 프로세스와 도구가 필요한 기능 등을 제시하는 것으로 정보 단위 선별 압수에서 발생하는 증거능력 문제에 대한 기술적인 보완방안을 마련하였다.

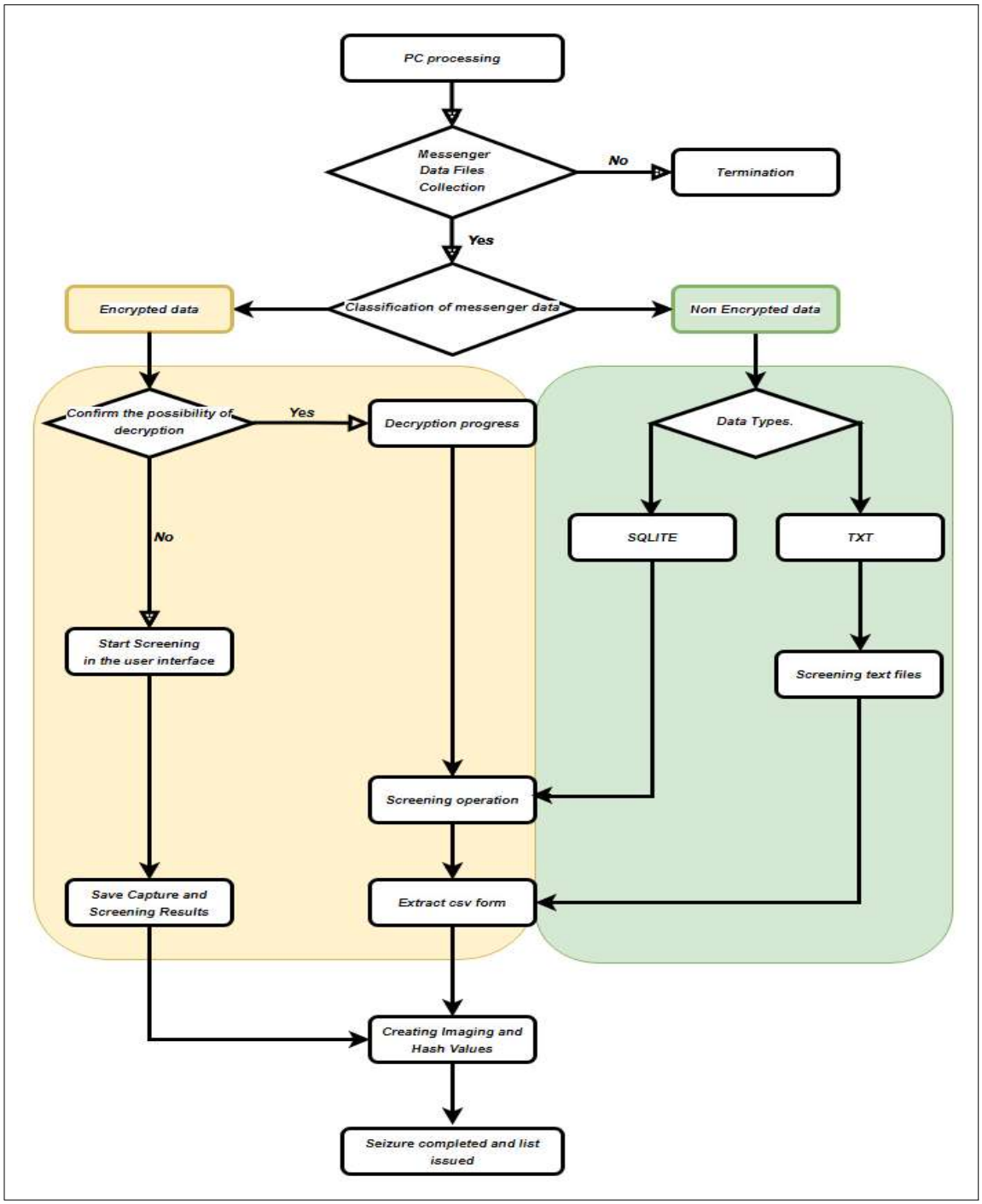
2. 현장용 메신저 압수 도구

가. 압수 도구 흐름도

현장용 메신저 데이터 압수 도구는 PC에 저장된 메신저 데이터 파일을 탐지하여 종류별로 분류하고, 암호화된 데이터에 대한 복호화 기능과 현장 선별기능을 지원하는 도구이다. 현장용 메신저 압수 도구의 분석 및 획득 프로세스는 [그림 9]와 같다.

---

71) 이주호·이태명, "디지털증거의 선별압수에 따른 원본성 및 동일성 증명에 관한 연구" 디지털포렌식연구 (2020) p.261



[그림 9] 현장용 메신저 압수 도구의 분석 및 획득 프로세스

먼저 프로세싱을 통하여 분석 대상 PC에서 메신저 데이터 존재 여부를 확인하고 탐지된 메신저 데이터를 종류별로 분류한다. 이후 분류된 메신저 데이터에 대한 암호화 상태를 확인하고 복호화가 필요한 경우 복호화

를 진행한다. 복호화 직후 데이터를 선별할 수 있는 화면을 구성하여 메신저 내용을 선별하는 절차를 진행한다. 메신저 내용 선별 방법은 채팅방, 기간, 대화 상대, 키워드 등을 기준으로 관련된 내용만 체크박스를 선택하는 방식을 사용한다. 최종 선별된 메신저 데이터는 CSV 형태로 저장하고, 선별데이터가 원본에서 추출된 것임을 확인할 수 있는 정보 또한 함께 수집하여 이미징하는 것으로 압수 프로세스를 종료한다.

나. 압수 도구의 내용

현재 압수수색 현장에서 사용되는 포렌식 도구 중에서 PC에서 발견된 메신저[72]에 대한 현장 선별 압수를 지원하는 도구는 포렌식 전문 기업에서 개발한 도구가 일부 존재하는 것으로 확인된다. 그러나 네트워크 API[73]를 이용하여 원격지 서버에 저장된 정보까지 함께 가져오기 때문에 압수영장의 범위 따라 도구 사용이 제한적일 수 있다. 본 논문에서 제안하는 현장용 메신저 압수 도구는 압수 현장에서 발견되는 PC에서 저장된 메신저 데이터 파일을 탐지하고 선별기능을 지원하여 메신저 데이터를 오피스 파일 형태로 선별 압수하는 기능을 기본으로 한다.

PC에서 저장된 메신저 데이터 파일은 일반적으로 데이터베이스(SQLite) 또는 텍스트 파일 형식이다. 따라서 위 파일들에는 사건과 관련된 대화 내용뿐만 아니라 무관한 정보도 혼재되어 있어 선별이 필요하다. 그러나 현재 현장용 압수 도구로 사용되는 포렌식 도구들이 메신저 데이터에 대한 선별기능을 지원하지 않고 있어 실무에서는 메신저 데이터에 대한 현장 선별 압수를 진행하지 않고 메신저 관련 파일 전체를 봉인한 뒤 검찰청에 마련된 참관실에서 사후 참관 절차를 통해 선별 압수를 진행하고 있

---

72) PC에서 발견되는 메신저 종류로는 PC 카카오톡, PC 텔레그램, 기업 전용 사내 메신저 등이 있다.

73) 응용 프로그램 프로그래밍 인터페이스. 프로그래밍에서, 프로그램을 작성하기 위한 일련의 부(Sub) 프로그램, 프로토콜 등을 정의하여 상호 작용을 하기 위한 인터페이스 사양을 말한다. (출처 : https://namu.wiki/w/API - 'API')

다. 또한, 참관과정에서 대화 내용을 선별하는 절차가 전체 내용을 엑셀 등 오피스 파일로 추출하고 관련성 없는 정보를 제거하는 형태로 진행되고 있어 데이터 손상의 우려가 있으며, 압수 과정에서 원본 출처정보 등 동일성 증명에 관한 정보 등을 충분히 수집하지 않는다면 증거능력 관련 문제가 생길 우려도 존재한다.

이에 제안하는 현장 메신저 압수 도구는 압수 당일 현장에서 선별 압수가 가능한 도구를 목표로 하였다. 또한, 선별된 정보가 어떤 원본으로부터 복제되었다는 출처정보를 자동 수집하고, 압수 전체 과정을 하나의 압수 도구 프로세스 형태로 자동화하는 것으로 정보 단위 선별 압수 과정에서 발생하는 원본과의 동일성, 무결성, 신뢰성에 대한 문제를 해결하였다. 메신저 데이터에 대한 선별 압수의 결과는 [그림 10]의 형태로 정의하였으며, 해당 도구가 동일성을 보완을 위해 자동 수집 및 기록해야 할 출처정보와 압수 시각 등의 정보들은 [표 1]과 같이 정리하였다.

분류	정보
메신저 종류	카카오톡(PC)
압수 시작 시각	2022. 10. 03 08:17 (UTC+09:00)
압수 종료 시각	2022. 10. 03 12:50 (UTC+09:00)
원본 출처 파일	/KakaoTalk/users/ea4a91e463bc1c33b0ee9d33ee3f644bea976b52/chat_data/chatLogs_142938683652507.edb /KakaoTalk/users/ea4a91e463bc1c33b0ee9d33ee3f644bea976b52/chat_data/chatLogs_142938683652623.edb /KakaoTalk/users/ea4a91e463bc1c33b0ee9d33ee3f644bea976b52/chat_data/chatLogs_142938683652444.edb • • •
선별 완료 파일	김 0 0_카카오톡 선별. CSV
해시값(MD5)	76930CD937046A5495E388B7AA82FF66
파일 크기	17.20 MB
참여인 정보	김 0 0

[표 1] 메신저 데이터에 대한 압수 정보

메시지

순번	App	상태	종류	날짜	본문	수신자	발신자	상대방	메시지 ID	채팅방	저장된 파일 이름	출처 정보
185	카카오톡 (PC)	생성	답장 수신	생성 일시 : 2022-09-30 19:59:08	내용 : 전 일정보고 다시 말씀드리겠습니다 ㅋ		이름 : [redacted]		2882311 8482112 04096	3225646 0127137 5		//KakaoTalk/users/ea4a91e463bc1c33b0ee9d33ee3f644bea976b52/chat_data/chatLogs_3225646012713 75.edb
186	카카오톡 (PC)	생성	수신	생성 일시 : 2022-09-30 20:57:35	내용 : 탁구 이제 끝남 ㅋㅋ		번호 : [redacted] 이름 :		2882341 2692908 46208	2481208 6342569 2		//KakaoTalk/users/ea4a91e463bc1c33b0ee9d33ee3f644bea976b52/chat_data/chatLogs_2481208634256 92.edb //KakaoTalk/users/ea4a91e463bc1c33b0ee9d33ee3f644bea976b52/TalkUserDB.edb
187	카카오톡 (PC)	생성	수신	생성 일시 : 2022-09-30 20:57:43	내용 : 아니 나중에 가지러 갈게 ㅋㅋ		번호 : [redacted] 이름 :		2882341 3388743 49568	2481208 6342569 2		//KakaoTalk/users/ea4a91e463bc1c33b0ee9d33ee3f644bea976b52/chat_data/chatLogs_2481208634256 92.edb //KakaoTalk/users/ea4a91e463bc1c33b0ee9d33ee3f644bea976b52/TalkUserDB.edb
188	카카오톡 (PC)	생성	발신	생성 일시 : 2022-09-30 20:57:54	내용 : 아 네넵 넵넵요	[redacted] 9869			2882341 4274918 99392	2481208 6342569 2		//KakaoTalk/users/ea4a91e463bc1c33b0ee9d33ee3f644bea976b52/chat_data/chatLogs_2481208634256 92.edb //KakaoTalk/users/ea4a91e463bc1c33b0ee9d33ee3f644bea976b52/TalkUserDB.edb

[그림 10] PC 카카오톡 메신저 압수 결과[74]

3. 현장용 데이터베이스 압수 도구

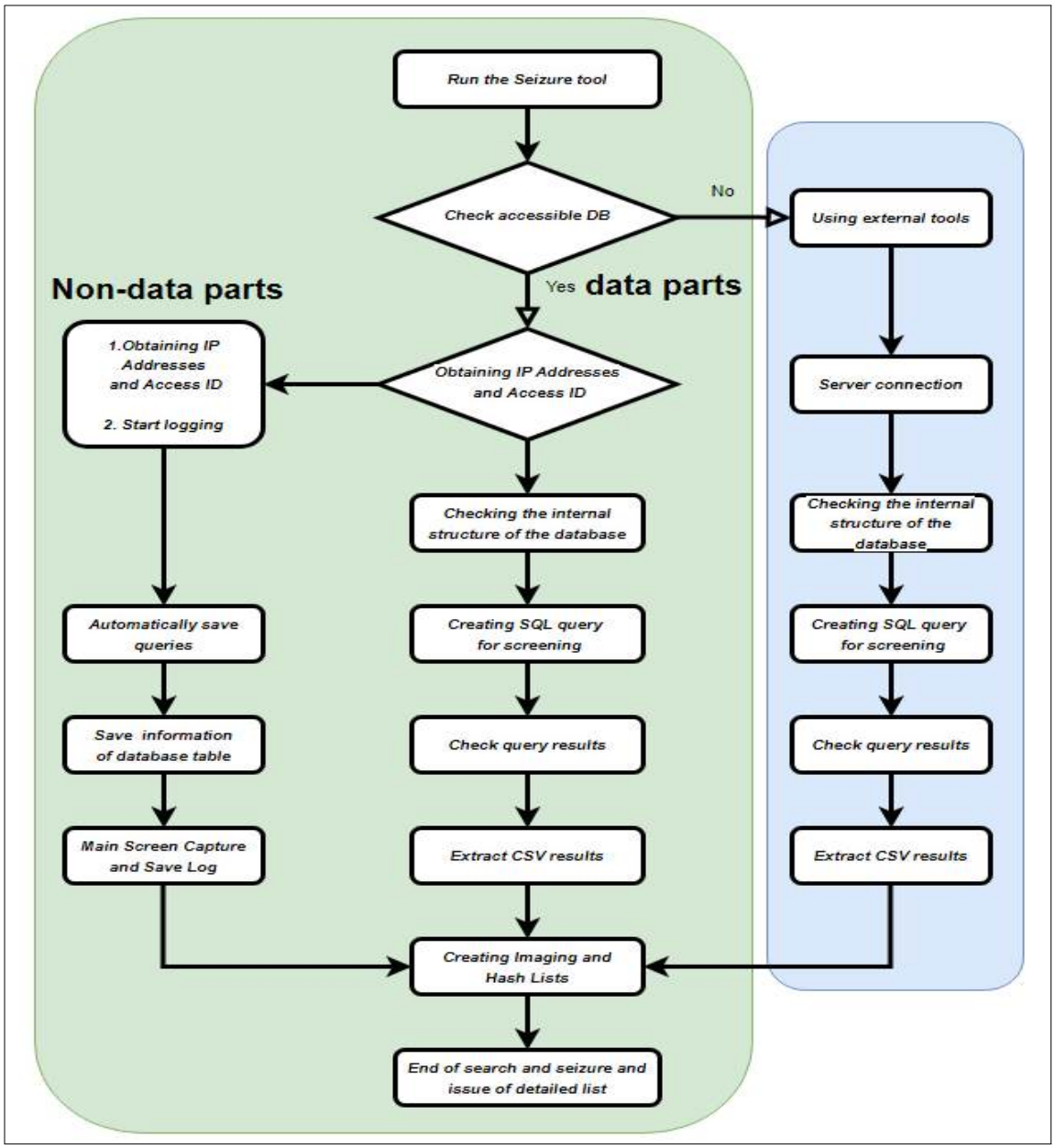
가. 압수 도구 흐름도

현장용 데이터베이스 압수 도구는 ODBC[75]를 기능을 이용하여 단일 도구로 압수 대상 정보가 저장된 ORACLE, MSSQL, MYSQL 등 다양한 종류의 데이터베이스에 접속할 수 있고, 도구 내 SQL 쿼리 사용 통해 사건과 관련 정보 선별기능을 지원하며, 최종적으로 선별된 데이터를 오피스 파일 형태로 저장하여 원본성 보완 자료들과 함께 이미지 형태 압수를 지원하는 도구이다.

압수 도구의 흐름은 다음과 같다. 먼저 DB 접근 권한을 획득한 뒤 도구를 실행하여 DB 접속 가능 여부를 확인한다. DB 접속 이후 데이터 탐색하고 기간 키워드 등을 고려하여 SQL문을 작성한 뒤, 작성된 SQL문을

74) GMD소프트社의 MD-RED 소프트웨어로 카카오톡 PC 버전을 분석한 결과
75) Open DataBase Connectivity, 마이크로소프트가 만든 데이터베이스에 접근 소프트웨어의 표준 규격이다. 각 데이터베이스의 차이를 ODBC 드라이버가 흡수하므로 사용자는 접속하는 데이터베이스 관리 시스템의 종류와 상관없이 권한만 있다면 접근할 수 있다. (출처 : 한국정보통신기술협회 정보통신용어사전 - 'ODBC')

실행하여 데이터를 선별하는 절차를 진행한다. 최종 선별된 메신저 데이터는 CSV 형태로 저장하고, 선별된 데이터가 원본에서 추출된 것임을 확인할 수 있는 정보 또한 함께 수집하여 이미징하는 것으로 압수 프로세스를 종료한다. 현장용 데이터베이스 압수 도구의 세부 프로세스는 [그림 11] 와 같다.



[그림 11] 현장용 데이터베이스 압수 도구 프로세스

나. 압수 도구의 내용

현재 압수수색 현장에서 사용되는 현장용 포렌식 도구 중에서 데이터베이스에 대한 현장 선별 압수를 지원하는 도구는 대검찰청에서 개발된 포렌식어카운팅[76]과 관련된 도구[77]들이 존재한다. 그러나 회계가 아닌 다른 분야에 범용적으로 사용되는 현장용 압수 도구는 확인되지 않는다. 일반적으로 데이터베이스를 관리할 수 있는 도구 중에서는 Toad Data Point[78] 등 상용프로그램이 존재하나 사용을 위해서는 설치과정이 필요하므로 데이터 오염 등의 문제로 현장 압수 도구로 사용하는 것은 한계가 있다.

현재 실무에서 데이터베이스 현장 선별 압수는 서버에 원격 접속이 가능한 데이터베이스 관리자 PC에서 실무자가 사용하는 DBMS 프로그램을 이용하여 DB에 접속하고 쿼리문 작성 및 실행과정을 거쳐 관련 정보를 선별한 뒤, 추출된 CSV[79] 파일을 포렌식 도구를 이용해 이미징하는 방식으로 절차를 진행하고 있다. 그러나 원본에서 관련 정보만을 선별하여 추출하는 과정과 이미징하는 과정이 분리되어 있어 증거 수집 과정에서 무결성 및 신뢰성과 관련된 문제가 발생할 수 있으며, 압수 과정에서 선별된 데이터와 함께 원본 출처정보 등 동일성 확보자료 등을 충분히 수집하지 않는다면 동일성 문제 또한 생길 우려가 있다.

본 논문에서 제안하는 현장용 데이터베이스 압수 도구는 압수 현장에서

---

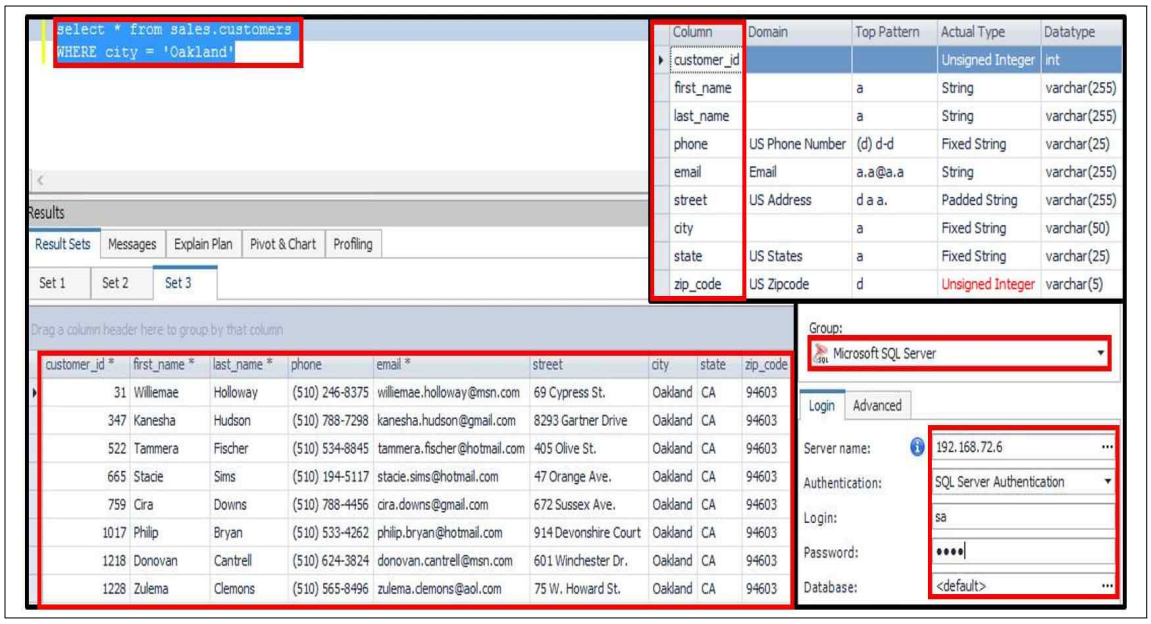
76) 기업에서 일어나는 일련의 회계부정 사건들에 대한 부정을 법정에서 증명하기 위해 적법한 절차에 따라 회계증거를 수집하고 분석하는 행위 또는 과정. (출처 : https://yum-history.tistory.com/272 - '디지털포렌식 어카운팅')

77) 대검찰청에서 개발한 포렌식어카운팅 도구로는 FAST, FAAT 가 있다.

78) 데이터베이스 개발자, 관리자, 데이터 분석가가 SQL을 사용하여 관계형 및 비관계형 데이터베이스를 관리하는데 사용하는 퀘스트의 데이터베이스 관리 도구. (출처 : https://blog.naver.com/quest_kor/221245536082 - 'Toad')

79) CSV 형식의 파일은 텍스트 파일로 저장되어 문서 처리기나 편집기에서 열람하고 편집할 수 있다. 애플리케이션에서 범용적으로 사용되는 형식이다. (출처 : 한국정보통신기술협회 정보통신용어사전 - 'CSV')

발견된 데이터베이스에 대한 선별 압수를 지원하는 도구이다. 데이터베이스 접속부터 선별, 최종 이미징 단계까지 압수 전 과정을 하나의 도구의 프로세스 내에서 진행하는 것으로 정보를 선별하여 추출하는 과정과 이미징하는 과정이 분리되어 발생하는 무결성, 신뢰성 문제를 해결하고자 하였다. 또한, 선별된 압수데이터와 함께 [그림 12]에서 확인되는 원본 대한 정보들을 [표 2]와 같은 형태로 수집하는 기능을 자동화하여 선별된 정보에 대한 원본과의 동일성, 무결성 문제를 해결하였다.



[그림 12] 데이터베이스 원본 정보[80]

분류	정보
DB 종류 및 버전	SQL-SERVER v.2012
선별 시작 시각	2022. 10. 05 08:17 (UTC+09:00)
선별 종료 시각	2022. 10. 05 18:50 (UTC+09:00)
서버명	9KNUUNL
서버 IP	192.168.72.6
데이터베이스명	USER.DB
선별 완료 파일	유저정보_선별.CSV
사용된 SQL 쿼리	쿼리문.TXT

80) Quest社의 Toad Data Point 도구로 SQL Server에 접속한 화면

해시값(MD5)	76930CD937046A5495E388B7AA82FF66
파일 크기	112 MB
참여인 정보	김 0 0

[표 2] 데이터베이스에 대한 압수 정보

4. 현장용 이미지 수집 도구

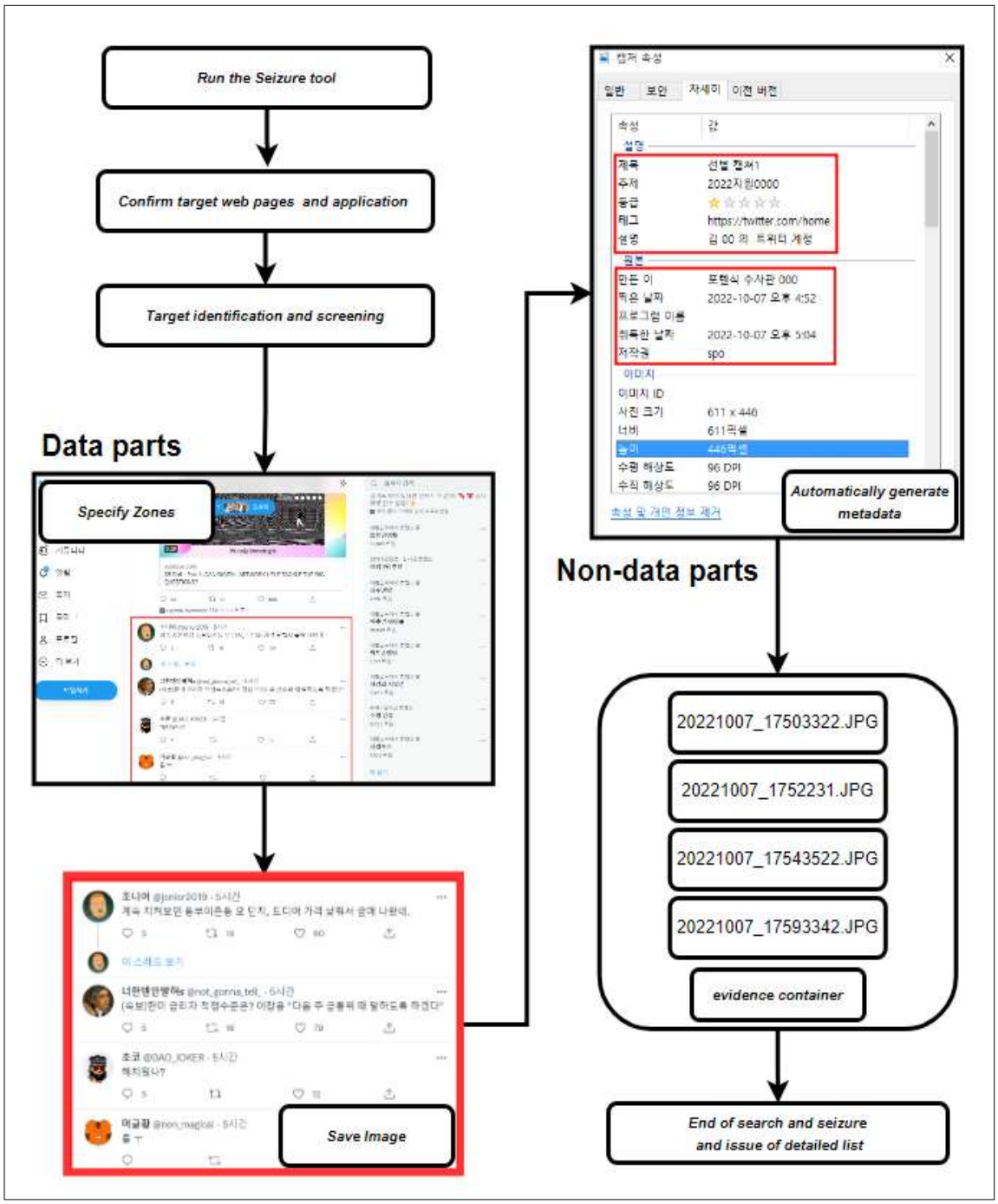
가. 압수 도구 흐름도

본 논문에서 제안하는 현장용 이미지 수집 도구는 웹페이지 및 애플리케이션에 저장된 정보에 대하여 화면 캡처 기술을 이용하여 이미지 형태 증거 수집을 지원하는 도구이다. 클라우드 및 웹서비스 기반 시스템 사용이 증가함에 따라 압수수색 현장에서는 압수 대상 정보가 정보저장매체에 파일 형태로 저장되어 있지 않고 웹이나 애플리케이션에 저장된 형태로 발견되고 있다.

압수 대상 정보가 저장된 웹페이지에 해당 정보를 파일로 추출하는 기능이 있는 경우에는 관련 정보들을 파일화하여 수집하는 작업이 어렵지 않으나 해당 웹페이지나 애플리케이션이 다운로드 추출기능을 제공하지 않은 상황에서는 압수 방법에 제한을 받을 수밖에 없다. 현재 실무에서도 웹에 저장된 데이터가 추출기능 제한 등의 이유로 다운로드가 불가능한 상황에서는 사건과 관련 정보만을 캡처 도구를 이용하여 이미지 형태로 저장하고 그 이미지 파일들을 포렌식 프로그램으로 이미징하는 방식으로 정보의 압수를 진행하고 있다.

압수 도구의 흐름은 다음과 같다. 먼저 수집 대상 정보가 확인되는 웹페이지를 확인한다. 이미지 수집 도구를 실행하고 사건 관련 정보가 있는 웹페이지를 스크롤 캡처 및 자동 캡처 등의 기능을 이용하여 이미지 형태로 수집하는 동시에 파일의 내부에 출처정보를 메타데이터 형태로 기록하여 수집한다. 최종적으로 수집된 이미지들을 확인하고 하나의 이미지 파

일 형태로 압수하는 것으로 압수 프로세스를 종료한다. 현장용 이미지 수집 도구 세부 프로세스는 [그림 13]과 같다.



[그림 13] 현장용 이미지 수집 도구 프로세스

나. 압수 도구의 내용

캡처 기능을 지원하는 상용 소프트웨어들은 다수 존재한다. 그러나 현장 여건상 압수 과정에서 개별적으로 생성되는 이미지 파일에 대한 관리가 어려운 점이 있으며 원본에서 사건과 관련된 정보만을 캡처하여 파일을 만드는 과정과 캡처한 파일을 이미징하는 과정이 분리되어 있어 무결성 및 신뢰성과 관련된 문제가 생길 수 있다. 또한, 압수 과정에서 선별된 데이터와 함께 원본 출처정보 등 동일성 확보자료 등을 충분히 수집하지 않는다면 원본과의 동일성 문제가 발생할 우려도 존재한다.

이에 제안된 현장용 이미지 수집 도구는 웹페이지 및 애플리케이션에 존재하는 정보에 대하여 캡처 방식으로 선별하고 파일화하는 과정부터 최종적으로 이미징하는 과정까지 압수 전 과정을 하나의 프로세스에 구현하여 압수 절차가 두 단계로 분리되어 발생하는 무결성, 신뢰성 문제를 해결하고자 하였다. 또한, 원본 출처정보 및 획득 시간 등의 메타데이터 정보를 이미지 파일의 EXIF[81]영역에 자동 저장하는 것으로 정보 선별 압수과정에서 발생하는 동일성에 대한 문제를 해결하고자 하였다. 본 도구를 이용하여 압수 절차 진행 시 도구 내에서 자동으로 생성되는 출처정보, 선별 시간 등 도구가 수집해야 할 정보들은 [표 3]과 같다.

분류	정보
대상 웹페이지	https://twitter.com/home?lang=ko
계정 정보	****@NAVER.COM
선별 시작 시각	2022. 10. 13 08:17 (UTC+09:00)
선별 종료 시각	2022. 10. 13 18:50 (UTC+09:00)
선별 압수 완료 파일	20221007_17503322. JPG 등 33건.dd

81) 디지털카메라 등에서 사용되는 이미지 파일 메타데이터 포맷으로, 카메라가 촬영한 사진, 녹음파일에 시간 등의 각종 정보를 담기 위해 개발되었다. 즉, JPEG, TIFF 6.0과 RIFF, WAV 포맷에 이미지나 소리에 대한 메타 정보를 추가로 기록할 수 있다. (출처 : 한국정보통신기술협회 정보통신용어사전 - ‘EXIF’)

해시값(MD5)	76930CD937046A5495E388B7AA82FF66
파일 크기	112 MB
참여인 정보	김 0 0

[표 3] 현장용 이미지 수집 도구로 압수한 정보

5. 도구 개발 제안에 따른 기대효과

가. 동일성, 무결성, 신뢰성 등 증거능력 요건 보완

논문에서 제안된 '현장용 메신저 압수 및 분석 도구', '현장용 데이터베이스 압수 도구', '현장용 이미지 수집 도구'의 공통적인 특징은 데이터 선별부터 이미징까지 과정을 하나의 도구로 대응할 수 있다는 점이다. 데이터 선별 등의 절차가 포렌식 도구 밖에서 수작업으로 진행되어 예기치 못한 상황 등으로 데이터가 손상되는 문제를 방지하고, 선별 절차와 이미징 절차가 나뉘어 진행되는 것을 통합하여 도구적 신뢰성 및 데이터 무결성을 확보하고자 하였다. 이와 함께 선별 압수된 정보가 원본과 같다는 동일성 증명과 관련된 데이터 수집을 도구를 통해 자동화하는 것으로 동일성을 문제 또한 해결하고자 하였다.

나. 시간적 효율성 확보

현재 현장용 압수 도구로 사용되는 포렌식 도구는 PC에서 발견되는 메신저에 대한 복호화 및 현장 선별기능을 지원하지 않고 있다. 따라서 실무상 메신저 데이터에 대한 압수는 대상 PC에서 메신저 데이터 파일 전체를 복제하여 저장 매체에 봉인한 후 추후 참관 과정을 통해 선별 압수하는 방식으로 진행되고 있다. 한정된 인력으로 운영되는 디지털포렌식팀의 특성상 메신저 데이터에 대한 압수가 위와 같은 방식으로 진행된다면, 압수수색마다 참관 업무가 누적될 수밖에 없다. 또한, 참관 절차를 거쳐 데이터가 압수 완료되기까지 시간이 지체됨에 따라 소요되는 시간적 비용도 적지 않을 것이다. 따라서 메신저 데이터에 대한 현장 선별을 가능하

게 하는 도구는 현장에서 신속한 참여권 보장뿐만 아니라 선별 절차에 드는 시간적 비용을 줄여 업무의 효율성을 높여 줄 것이다.

다. 참여권 보장

현재 PC에서 발견되는 메신저 데이터 압수 절차는 복호화 및 선별 등의 문제로 검찰청 내 디지털포렌식팀 참관실 등에서 사후 참관 절차가 필요하다. PC에서 발견되는 카카오톡 등 메신저 데이터들은 사건과 관련된 정보뿐만 아니라 무관한 개인적인 정보도 다수 저장하고 있어 피압수자들은 선별 과정에 참여 의사를 적극적으로 표시하고 있다. 그러나 현장에서 선별 과정 참여 의사가 확인되더라도 검찰청 내에서 진행되는 선별 절차에 대하여 시간적 부담 등의 사유로 참여 의사를 포기하는 사례도 확인되고 있다. 따라서 현장용 선별 도구가 개발되어 현장에서 메신저 데이터에 대한 선별 압수가 가능하다면 피압수자의 참여권을 충분히 보장할 수 있을 것으로 기대된다.

제 2 절 법률적 보완방안

1. 법률 및 규정의 개정 필요성

앞에서 확인한 기술적 보장방안에서는 압수 상황별로 필요한 현장용 선별 압수 도구를 제안하는 것으로 정보 단위 선별 압수 시 발생하는 증거능력과 관련된 문제를 해결하고자 하였다. 그러나 도구 개발을 통한 기술적인 보완만으로는 문제 해결에 한계가 있을 수밖에 없다. 빠르게 변화하는 디지털 환경의 특성상 수사기관의 대응 방법은 필연적으로 후행적일 수밖에 없으며, 모든 압수 현장에서 범용적으로 사용할 수 있는 도구를 만들기란 불가능에 가깝기 때문이다. 따라서 정보 선별 압수 절차 따른 디지털 증거의 증거능력 인정요건 보완을 위해서는 기술적인 방법뿐만 아니라 형사소송법 및 실무와 밀접한 디지털 증거 수집 관련 규정 등에 대

한 개정을 통한 법률적인 보완도 필요하다.

법률적인 보완에 대한 첫 번째 내용은 디지털 증거의 선별 압수 대상에 대한 것이다. 정보를 효율적으로 저장하고 관리하기 위하여 데이터베이스 같이 하나의 저장체계 안에 대량의 데이터를 저장하는 형태가 증가할 것이며, 클라우드 및 웹서비스 기반 시스템 사용이 많아짐에 따라 압수 대상 정보가 저장매체에 저장된 파일 형태가 아닌 상황도 늘어날 것이다. 따라서 선별 압수 대상은 정보저장매체에 저장된 파일에서 정보로 다시 정의되어야 한다. 또한, 선별의 최소 단위도 파일에서 정보로 바뀌어야 한다.

두 번째 내용은 정보 선별 압수에 따라 원본과 내용적 동일성만 있는 사본에 대하여 그것이 원본에서 추출되었다는 것을 증명하기 위한 신용적 정황성[82] 확보에 관한 문제이다. 해당 문제를 도구 개발을 통한 기술적 방안으로 해결하고자 하나 모든 상황에서 사용할 수 있는 도구를 만들기란 현실적인 어려운 점이 있으므로 정보 선별 압수 시 원본과의 동일성 증명을 위하여 필요한 조치 내용과 필요 조치에 따른 협조 요구에 관하여 규정할 필요성이 있다.

세 번째 내용은 원격 압수에 관한 것이다. 클라우드 및 웹서비스 기반 시스템 사용자가 증가함에 따라 압수수색 현장에서는 압수 대상 정보가 PC 등에 파일 형태로 저장되어 있지 않고 웹상에서만 확인되는 경우가 증가하고 있다. 따라서 해당 시스템에서 사건과 관련된 정보를 압수할 때에는 압수장소에서 서버 원격으로 접속하여 확인되는 자료를 내려받거나 캡처하는 방법으로 압수해야 할 필요성이 있으므로 원격 압수의 근거를 마련할 필요가 있다.

---

82) 이주호·이태명, “디지털증거의 선별압수에 따른 원본성 및 동일성 증명에 관한 연구” 디지털포렌식연구 (2020) p.261

2. 관련 법규 및 실무 지침 개정

위와 같은 점을 반영하여 “형사소송법”과 “검찰의 디지털 증거 수집·분석 및 관리 규정”에 대하여 다음과 같이 개정안을 제시해보고자 한다.

가. 형사소송법

형사소송법 (개정안)

제106조 (압수)

① 법원은 필요한 때에는 피고사건과 관계가 있다고 인정할 수 있는 것에 한정하여 증거물 또는 몰수할 것으로 사료하는 물건 또는 컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체(이하 이 항에서 “정보저장매체등”이라 한다)에 기억된 정보(이하 이 항에서 “전자정보”라 한다)를 압수할 수 있다. 단, 법률에 다른 규정이 있는 때에는 예외로 한다.

② 법원은 압수할 물건을 지정하여 소유자, 소지자 또는 보관자에게 제출을 명할 수 있다

③ 법원은 압수의 목적물이 전자정보인 경우에는 정보저장매체등에 기억된 정보의 원본과의 동일성 및 무결성을 담보할 수 있는 도구 또는 방법을 사용하여 범위를 정하여 복제하여 제출받아야 하고, 전자정보가 정보통신망으로 연결된 서버의 정보저장매체등 등 압수 장소 이외의 공간에 존재하는 것이 확인될 경우에는 원격 접속하여 제출받을 수 있다. 다만, 범위를 정하여 복제하는 방법이 불가능하거나 압수의 목적을 달성하기에 현저히 곤란하다고 인정되는 때에는 정보저장매체등이나

정보저장매체등의 전체 사본을 압수할 수 있다. ④ 법원은 제3항에 따라 정보를 제공받은 경우 개인정보 보호법 제2조 제3호에 따른 정보 주체의 요청 시 압수 절차에 대한 참여의 기회를 제공해야 한다.

본 논문에서 제안하는 형사소송법 개정안은 제106조 제1항 및 제3항에서 압수의 대상을 정보저장매체나 파일이 아닌 정보로 규정하였다. 즉 압수 목적물을 저장 매체가 아닌 정보 자체로 규정함으로써 디지털 환경의 변화로 데이터 저장 형태가 다양해지고, 개인정보자기결정권 및 개인정보보호를 중요시하는 사회적 분위기에 따라 선별 압수의 대상이 파일이 아닌 정보로 변화·확장되고 있는 실무의 상황을 반영하였다.

정보 단위 선별 압수 절차에 따라 확보된 대부분의 압수 결과물은 압수 현장에서 정보 자체를 오피스 파일이나 캡처 형태로 저장한 파일일 수밖에 없다. 따라서 해시값 검증만으로는 원본과의 동일성 및 무결성 검증이 어렵다는 점을 고려하여 형사소송법 제106조 제3항 전단에서 “정보저장매체 등에 기억된 정보 압수 시 원본과의 동일성 및 무결성을 담보할 수 있는 도구 또는 방법을 사용하여 범위를 정하여 제출받아야 한다.”라고 규정하였다. 이를 통해 디지털 증거 수집 시 사용되는 도구의 신뢰성 및 수집 방법 신뢰성을 강조하는 한편 원본 출처정보 등 동일성 및 무결성 증명에 필요한 자료도 함께 수집할 수 있는 근거를 마련하였다.

서버 및 클라우드 사용이 증가함에 따라 디지털 증거가 존재하는 장소를 물리적인 장소로만 한정할 수 없으므로, 형사소송법 제106조 제3항 후단에 “전자정보가 정보통신망으로 연결된 서버의 정보저장매체 등 압수장소 이외의 공간에 존재하는 것이 확인되는 경우에는 원격 접속하여 제출받을 수 있다.”라고 규정하여 원격 압수의 근거를 마련하였다. 또한, 개인정보자기결정권 및 개인정보보호와 관련하여 강조되고 있는 디지털 증거 압수

수색 참여권과 관련하여 형사소송법 제106조 제4항에 선별 과정 참여에 관한 권리를 직접 규정하여 디지털 증거 압수·수색 과정에서 피압수자의 참여권을 충분히 보장하고자 하였다.

나. 디지털 증거의 수집·분석 및 관리 규정

디지털 증거의 수집·분석 및 관리 규정 (개정안) 제6조(디지털 증거의 무결성 유지) 디지털 증거는 압수・수색・검증 과정부터 법정에 제출하는 때까지 훼손 또는 변경되지 아니하여야 한다. 제20조(전자정보의 단계적 압수·수색·검증) ① 주임검사 등은 정보저장매체 등에 기억된 전자정보를 압수하는 경우에는 해당 정보저장매체등의 소재지에서 수색 또는 검증한 후 범죄사실과 관련된 전자정보의 범위를 정하여 선별 압수하는 방법으로 한다. ② 주임검사 등은 제1항에 따른 선별 압수 시 전자정보의 출처증명 기타 법정에서 디지털 증거의 정확성과 신뢰성의 입증에 필요한 범위 내의 전자정보 등을 함께 압수할 수 있으며, 관련 내용에 대하여 피압수자에게 협조를 요구할 수 있다.

검찰의 “디지털 증거의 수집·분석 및 관리 규정”은 디지털 증거의 수집·분석에 대한 절차와 방법과 관련하여 비교적 구체적으로 규정되어있으며, 최근에 개정되어 디지털 증거의 수집 부분 중심으로 세부적인 보완이 필

요할 것으로 보인다.

정보의 선별 압수는 원본에 저장된 파일을 동일하게 복제하는 것만을 가리키는 것이 아니므로 '왕재산 사건' 판결을 통해 정립된 무결성 개념도 압수환경의 변화에 따라 변경이 필요하다. 무결성은 수집된 이후 과정뿐만 아니라 원본 데이터에서 관련 정보만을 선별하여 수집하는 과정에서도 지켜져야 한다. 따라서 제6조(디지털 증거의 무결성 유지)에서 무결성 개념의 적용 시점을 압수・수색・검증 과정부터 법정에 제출하는 때까지로 개정하였다.

제20조(전자정보의 단계적 압수·수색·검증) 제1항 후단의 "전자정보의 범위를 정하여 출력하거나 복제하는 방법으로 한다."를 "선별 압수하는 방법으로 한다."라고 폭넓게 규정함으로써 압수 방법을 원본 파일과 동일하게 복제, 출력하는 것에서 벗어나 원본이 어떠한 형태여도 동일성과 무결성만 유지하는 방식 선별 압수하면 내용적 동일성만을 가진 사본이라도 증거능력을 인정받을 수 있도록 하였다.

제20조 제2항에서는 정보 단위 선별 압수 절차에 따라 확보된 압수 결과물이 압수 현장에서 생성된 오피스 파일 형태나 캡처 형태일 경우, 기존 해시 검증 방법만으로는 원본과의 동일성, 무결성 검증이 어려운 점을 고려하여 압수된 정보가 원본에서 현출된 것임을 증명하는 자료를 함께 확보하도록 규정하였다. 또한, 원본 동일성 증명 자료 확보와 관련하여 피압수자에게 협조 요구할 수 있는 내용 또한 명시하여 본 규정을 통해 법정에서 원본과의 동일성을 재현 및 검증이 원활하게 진행되고 현장에서도 신속한 압수수색이 진행될 수 있도록 하였다.

제 6 장 결 론

디지털 환경의 변화로 데이터의 저장 형태가 다양해지고, 개인정보자기결정권 및 개인정보보호를 중요시하는 사회적 분위기에 따라 디지털 증거 압수에서 선별 개념의 변화 또한 불가피해졌다. 그 변화 내용은 선별의 최소 단위가 파일 단위에서 정보 단위로 변화하고 있다는 것이다. 따라서 본 논문에서는 정보 단위의 선별 절차를 거쳐 수집된 디지털 증거에 대한 원본 동일성과 무결성은 수집 도구와 분석관의 신뢰성에 크게 의존할 수 밖에 없으며, 현장 절차 수행 시 원본 출처정보 등 원본과의 동일성을 증명할 수 있는 정보가 함께 수집되지 않는다면 증거능력 인정요건 관련 문제가 발생할 수 있다는 것을 확인하였다.

이러한 문제들이 발생하는 근본적인 원인은 현재 디지털 증거 수집과 관련된 법률 및 현장용 증거 수집 도구들이 정보저장매체에 저장된 파일만을 대상으로 선별 압수하는 과거의 압수 환경에 머물고 있다는 점에 있다. 따라서 디지털 환경 변화에 밀접한 관련이 있는 디지털 수사 분야는 변화에 신속하게 대응할 필요가 있다. 사건 해결에 필요한 디지털 증거가 수집 과정상 발생한 문제로 증거능력을 상실해버린다면 이는 국민에게 피해로 고스란히 돌아갈 것이기 때문이다. 따라서 디지털 증거를 수집·분석을 통해 수사 지원 업무 수행하는 디지털포렌식 수사관들에게는 현재 상황에 맞는 명확한 절차적 기준과 신뢰성 있는 도구가 필요하다.

본 논문에서는 디지털포렌식 수사관이 최근 압수 현장에서 경험하게 되는 정보 단위 선별 압수와 관련된 사례들을 조사하고 증거능력 관련 문제점을 지적하며 확인된 문제들을 기술적·법률적으로 해결하고자 하였다. 증거능력 문제에 대한 기술적 보완방안으로 정보 단위 선별이 필요한 상황에 사용할 수 있는 압수 도구의 모형을 제안하고, 관련 법률과 규정의 개정을 통해 정보의 선별 압수라는 특수적인 상황을 법률적으로 보완하는 것으로 증거능력과 관련된 문제가 해결될 수 있다는 가능성을 확인하였

다. 이를 토대로 본 주제에 대한 논의와 연구가 진행된다면 현장 업무를 수행하는 수사관들에게 큰 도움이 될 것으로 보인다.

본 논문에서는 실무에서 발견된 문제점을 극복할 수 있는 현장용 압수 도구들의 모형을 제안하였으나 프로그래밍을 통한 도구 개발까지는 다루지 못하였다. 따라서 추후 연구에서는 실무에서 직접 사용할 수 있는 도구에 대한 개발이 진행되어야 할 것이다. 또한, 법률로써 실무에 관한 모든 내용을 세부적으로 규정하는 것은 한계가 있으므로 형사소송법 및 디지털 증거 수집 관련 규정 개정과 함께 포렌식 수사관들이 압수 현장에서 참고할 수 있는 현장 실무 지침 및 압수 기법 등 매뉴얼 제작에 관한 연구도 함께 진행되어야 할 것이다.

참 고 문 헌

[논문 및 자료]

[1] ‘디지털 증거 수집 및 분석 실적’ 대검찰청 홈페이지 검찰연감 (2020)

[2] ‘디지털 증거 분석 현황’ 경찰청 홈페이지 정보공개자료실 (2021)

[3] “디지털 증거의 수집·분석 및 관리 규정” 대검찰청예규 제1285호

[4] “디지털 증거의 처리 등에 관한 규칙” 경찰청훈령 제1030호

[5] “검사와 사법경찰관의 상호협력과 일반적 수사준칙에 관한 규정” 대통령령 제31089호

[6] “형사소송법” 법률 제18862호

[7] 대법원 2007. 12. 13. 선고 2007도7257 판결

[8] 대법원 2013. 7. 26. 선고 2013도2511 판결

[9] 대법원 2011. 5. 26.자 2009모1190 결정

[10] 대법원 2015. 7. 16.자 2011모1839 결정

[11] 대법원 2022. 5. 31.자 2016모587 결정

[12] 김용호·이대성, “실무상 디지털 증거의 현장 압수수색 문제점과 개선방안” 한국정보통신학회논문지 Vol. 17, No. 11 (2013)

[13] 오현석, “전자증거의 선별압수와 매체압수에 관한 연구” 석사 학위 논문 (2019)

[14] 김영미, “디지털(전자) 증거 압수수색에 있어서 ‘현장’ ‘선별’ 압수수색 원칙의 문제점과 기술적, 법적 개선방안 연구 - 형사소송법 제106조 제3항의 개정 필요성 중심으로” 석사 학위 논문 (2022)

[15] 조광훈, “디지털 증거의 압수・수색의 문제점과 개선방안” 서울法學 제21권 제3호 (2014)

[16] 김무석, “디지털포렌식에서의 참여권 보장방안” 치안정책연구 제32권 제3호 (2018)

[17] 유상현·이경렬, “디지털 증거의 선별적 압수수색에 관한 LSH(Locality Sensitive Hashing)기법 활용방안 연구” 박사 학위 논문 (2020. 01)

[18] 윤신자·이상진, “전자정보의 압수·수색절차 개선방안 연구” 경찰학연구 8 제13권 제4호

[19] 손지영·김주석, “디지털 증거의 증거능력 판단에 관한 연구” 대법원 사법정책연구원 연구총서 2015-08호 (2015)

[20] 권양섭, “디지털포렌식 전문입회인 제도의 필요성과 운영방안” 디지털포렌식연구 (2020)

[21] 이주호·이태명, “디지털증거의 선별압수에 따른 원본성 및 동일성 증명에 관한 연구” 디지털포렌식연구 (2020)

[22] 박혁수, “개정형사소송법상 디지털 증거의 증거능력” 해외연수검사논문집 (2009. 7)

[23] 양근원, “디지털 증거의 특징과 증거법상의 문제 고찰” 경희법학 제41권 제1호 (2006. 6.)

[24] 이상원, “전자증거와 원본증거의 법칙” 형사법의 신동향 (2012)

[25] 강미영, “디지털 증거의 증거능력” 외법논집 (2019)

[26] 손지영·김주석, “디지털 증거의 증거능력 판단에 관한 연구” [JPRI] 연구보고서(2015)

[27] 박상준, “디지털 증거의 원본성과 동일성에 관한 기술적 고찰” 미발표논문

[인터넷사이트]

[1] https://aws.amazon.com/ko/what-is/sql/ - ‘SQL’

[2] http://forensic-proof.com/archives/3710 - ‘artifact’, ‘아티팩트’

[3] 네이버 지식백과 doopedia - ‘데이터베이스’

[4] https://namu.wiki/w/SQLite - ‘Sqlite’

[5] https://goblinforensics.tistory.com/106 = ‘논리적 증거 이미지’

[6] 한국정보통신기술협회 정보통신용어사전 - ‘DBMS’

[7] 한국정보통신기술협회 정보통신용어사전 - ‘ERP’, ‘기업자원관리’

[8] https://blog.naver.com/quest_kor/221245536082 - ‘Toad’

[9] 한국정보통신기술협회 정보통신용어사전 - ‘DLP’

[10] 한국정보통신기술협회 정보통신용어사전 - ‘관계형 데이터베이스’

[11] 한국정보통신기술협회 정보통신용어사전 - ‘CSV’

[12] https://ko.wikipedia.org/wiki/스냅샷_(기억_장치) - ‘스냅샷’

[13] https://namu.wiki/w/%EC%BF%BC%EB%A6%AC - ‘쿼리’

[14] https://namu.wiki/w/%ED%98%91%EC%97%85%ED%88%B4 - ‘협업툴’

[15] 한국정보통신기술협회 정보통신용어사전 - ‘해시 함수’

[16] 한국정보통신기술협회 정보통신용어사전 - ‘EXIF’

[17] 한국정보통신기술협회 정보통신용어사전 - ‘비트스트림’, ‘bitstream’

[18] 한국정보통신기술협회 정보통신용어사전 - ‘ODBC’

[19] https://yum-history.tistory.com/272 - ‘디지털포렌식 어카운팅’

[20] https://ko.wikipedia.org/wiki/한국정보통신기술협회 -‘한국정보통신기술협회’

[21] https://namu.wiki/w/%EC%8A%AC%EB%9E%99 - ‘슬랙’, ‘Slack’

[22] 한국정보통신기술협회 정보통신용어사전 - ‘무결성’

[23] https://namu.wiki/w/API - ‘API’

Abstract

A Study on the Problems and Technical and Legal Improvement measures in accordance with the change of method in the selective seizure of digital evidence

OH JUNG KYUNG
Master of Science in Digital Forensics
Department of Mathematical Information Science
The Graduate School of
Convergence Science and Technology
Seoul National University

Currently, the seizure of digital evidence by investigative agencies is carried out according to the principle of selective seizure in accordance with Article 106 (3) of the Criminal Procedure Act. However, depending on the difference in data storage methods, digital evidence is in various forms and may be stored in a form other than a file in the cloud and web services. Therefore, digital forensics investigators need not only file-by-file selective seizure at the digital evidence seizure site, but also to divide only case-related information from the original or extract only a part of it.

However, the current laws related to evidence collection only consider

the seizure situation, which is screened on a file-by-file basis from the storage. In addition, it does not clearly stipulate the procedure for performing selective seizure on an information basis. In addition, the digital forensic tool provided to forensic investigators only functions to select files on the storage. Therefore, technical and legal studies are needed to supplement the problems of digital evidence recognition requirements such as identity, integrity, and reliability that may occur during the screening and seizure process.

In this study, cases of selecting and collecting digital evidence by the information unit were identified. After that, it was confirmed that there were any problems with the current seizure and search procedures and methods used in each case related to identity, integrity, and reliability. As a result, a technical and legal supplementation method was devised to solve the problem of evidence ability occurring in the field in relation to information screening seizure. In addition, the research results were made available to digital forensic investigators who collect digital evidence in the field.

keywords : digital forensics, seizure, selection, information, database, qualifications of evidence
Student Number : 2021-24042