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

이학석사학위논문

디지털 포렌식 절차 모델에 대한 새로운 접근

2015년 8월

서울대학교 융합과학기술대학원
수리정보과학과 디지털포렌식학 전공
김 지 홍

디지털 포렌식 절차 모델에 대한 새로운 접근

지도교수 이 상 원
이 논문을 김 지 홍 석사학위논문으로 제출함

2015년 5월

서울대학교 융합과학기술대학원
수리정보과학과 디지털포렌식학전공
김 지 홍

김지홍의 석사학위논문을 인준함
2015년 6월

위 원 장 이 광 근 (인)
부 위 원 장 이 상 원 (인)
위 원 박 상 준 (인)

국문초록

현대 사회는 디지털 기기 사용의 급증으로 인하여, 거의 모든 생활에 디지털 데이터가 사용된다. 자연스럽게 수사기관도 디지털 데이터에 관심을 가지게 되었고, 이제 디지털 데이터 없이는 범죄 입증이 어렵게 되는 시대에 이르렀다. 하지만, 디지털 데이터는 기존의 유체물과 다른 특징이 있어 압수에 여러 가지 주의점이 요구된다.

그러므로 어떠한 절차로 디지털 데이터를 압수하면 수사의 목적을 달성할 수 있는지를 규정하는 것이 중요한데, 이를 디지털 포렌식 절차 모델이라 한다. 디지털 포렌식은 기술적인 부분뿐만 아니라, 법률적인 부분이 함께 고려해야 하기 때문에 각국의 법률적인 특징에 따라 달라질 수밖에 없다.

2012. 1. 1. 시행된 개정 형사소송법은 디지털 데이터의 압수에 대하여 명문으로 규정하였다. 디지털 데이터 압수 원칙이 기존 실무인 정보저장매체 자체의 압수에서 사건과 관련된 디지털 데이터 압수로 바뀌는 큰 변화였다. 그러나 아직 개정 형사소송법에 대하여 규정에 대한 논의는 많이 있지만, 실제 이를 준수하면서 어떻게 디지털 데이터를 압수해야 하는지에 대한 연구는 거의 없다.

본 논문은 디지털 포렌식 절차 모델과 국내외 디지털 포렌식 현황을 살펴보고, 수사기관 특히, 검찰의 디지털 포렌식 절차를 고찰하면서, 새로운 디지털 포렌식 절차 모델을 제시해보고자 한다.

우리나라의 경우 수사기관인 경찰과 검찰을 중심으로 디지털 포렌식 기관이 있고, 디지털 포렌식 절차는 형사소송법 개정 이전에 형성된 판례의 이론에 기초로 하고 있으나, 이는 개정 형사소송법의 태도에 반하는 부분이 있어 판례 변경이 필요하다. 한편, 검찰은 디지털 수사망(Digital Investigation Network)이라는 시스템을 구축하여 디지털 데이터의 대용량화와 효율적인 디지털 압수물의 활용을 하고 있다.

검찰의 디지털 포렌식 절차는 원칙적으로 압수·수색 준비, 압수·수색 현장에서 정보저장매체 수색, 수색한 정보저장매체에서 사건과 관련된 디지털 데이터 조사, 사건

과 관련된 디지털 데이터의 획득(예외적인 경우 정보저장매체 전체를 이미징하거나, 정보저장매체 자체를 압수), 문서화, 디지털 압수물 시스템에 업로드, (예외적인 경우 분석), 색인, 수사팀에서 검색, 분석, 디지털 압수물 폐기의 순이다.

디지털 데이터는 압수의 대상이고, 피압수자의 협력의무는 명문의 규정이 필요하고, 원격지 압수·수색은 필요성은 있으나, 허용 범위나 방법 등 아직 논의가 더 필요하며, 현장용 디지털 포렌식 도구가 갖추어야 할 기능을 발전시켜야 할 필요가 있겠다. 형사소송법 제106조 제3항에 따라 정보저장매체 자체를 압수하면 압수·수색 영장의 집행은 종료되므로 법원의 디지털 데이터 압수에 대한 태도는 형사소송법 개정으로 변경되어야 한다.

우리나라의 현실에 맞는 디지털 포렌식 절차를 제시하면, 준비(Preparation) → 정보저장매체 수색(Search) → 조사(Examination) → 사건과 관련된 디지털 데이터 획득(Acquisition) → 1차 분석(1st Analysis) → 시스템 업로드, 색인 (System Upload & Index) → 2차 분석(2nd Analysis) → 제출(Presentation) → 디지털 압수물 폐기(Disposal) 순이다.

최근의 해외 동향을 보면, 디지털 포렌식 절차가 피압수자의 권리 보호를 강화하는 방향으로 나아가고 있는 것으로 보인다. 우리나라의 디지털 포렌식 관련 형사소송법 규정은 우리나라에만 있는 '이상한' 규정이 아니라, 우리나라에서 '최초로' 규정된 선진적인 규정인 것이다. 그러므로 수사기관은 형사소송법 개정으로 과거에 비하여 디지털 데이터 압수가 어렵고, 효과적이지 못하다고 불만을 늘어놓을 것이 아니라, 피압수자의 권리를 보호하면서 수사의 목적을 달성하기 위하여 디지털 포렌식 절차를 확립하는 것이 필요하다.

주요어 : 디지털 증거, 디지털 압수물, 디지털 포렌식 절차 모델

학번 : 2013-24050

<제목 차례>

국문초록 ····· 1

제1장 서설 ····· 1

제1절 연구 배경 ····· 1

제2절 연구 목적 ····· 2

제3절 연구 방법 ····· 2

제2장 디지털 포렌식의 의의 ····· 5

제1절 디지털 증거의 의의 및 특징 ····· 5

1. 디지털 데이터의 의의 ····· 5

2. 디지털 증거의 의의 ····· 5

가. 디지털 형태의 정보 ····· 6

나. 저장 전송되는 정보 ····· 6

다. 증거가치 있는 정보 ····· 6

3. '디지털 증거'라는 용어 사용 문제 - 디지털 압수물 ····· 7

제2절 디지털 압수물의 특징 ····· 8

1. 매체독립성 ····· 8

2. 비가시성 ····· 8

3. 취약성 ····· 8

4. 대량성 ····· 9

제3절 디지털 포렌식의 의의 ····· 9

1. 포렌식 사이언스(Forensic Science)의 의의 ····· 9

2. 디지털 포렌식(Digital Forensics)의 의의 ····· 10

3. 디지털 포렌식의 기본 원칙 ····· 10

가. 적법절차의 원칙 ····· 11
나. 동일성, 무결성 유지 ····· 11
다. 재현의 원칙 ····· 15
라. 신속성의 원칙 ····· 15

제3장 기존의 디지털 포렌식 절차 모델 ····· 16

제1절 디지털 포렌식 절차 모델 ····· 16

제2절 구체적인 디지털 포렌식 절차 모델 ····· 16

1. 1995.~2003.의 디지털 포렌식 절차 모델 ····· 16
가. Computer Forensic Investigative Process (1995) ····· 16
나. DFRWS Investigative Model (2001) ····· 17
다. Abstract Digital Forensics Model (ADFM) (2002) ····· 18
라. Integrated Digital Investigation Process (IDIP) (2003) ····· 19
2. 2004.~2007.의 디지털 포렌식 절차 모델 ····· 21
가. Enhanced Digital Investigation Process Model (EDIP) (2004) ····· 21
나. Hierarchical Objectives based Framework(2004) ····· 21
다. Computer Forensics Field Triage Process Model(2006.) ····· 22
라. Framework for a Digital Forensic Investigation(2006) ····· 23
마. Common Process Model for Incident and Computer Process(2007) ····· 24
3. 2008.~ 현재 디지털 포렌식 절차 모델 ····· 25
가. Digital Forensic Model based on Malaysian Investigation Process(2009) ····· 25
나. Systematic Digital Forensic Investigation Model(2011) ····· 26
다. New Approach of Digital Forensic Model for Digital Forensic Investigation(2011) ····· 27
라. Harmonized Digital Forensic Investigation Process Model(2012) ····· 27
마. Integrated Digital Forensic Process Model (2013) ····· 28

제3절 실무상 디지털 포렌식 절차 ····· 28

제4절 소결 ····· 29

제4장 해외 디지털 포렌식 현실 ····· 30

제1절 외국의 디지털 포렌식 기관 ····· 30

1. NIJ(National Institute of Justice) ····· 30
2. NIST (National Institute of Standard and Technology) ····· 30
3. RCFL (Regional Computer Forensics Laboratory) ····· 31
4. DCFL (Defense Computer Forensics Laboratory) ····· 31
5. 네덜란드의 NFI (Netherlands Forensic Institute) ····· 32

제2절 외국의 디지털 포렌식 관련 현실 ····· 32

1. 미국의 디지털 포렌식 관련 현실 ····· 32
가. 입법례 ····· 32
(1) 디지털 데이터가 압수의 대상인지 여부 ····· 32
(2) 관련 규정 ····· 33
나. 디지털 포렌식 절차 관련 ····· 33
2. 사이버범죄방지조약 ····· 34
가. 사이버범죄방지조약 ····· 34
나. 사이버범죄방지조약의 내용 ····· 34
3. 영국의 디지털 포렌식 현실 ····· 35
가. 입법례 ····· 35
나. 영국의 디지털 포렌식 절차 ····· 37
4. 독일의 디지털 포렌식 현실 ····· 37
가. 입법례 ····· 37
나. 독일의 디지털 포렌식 절차 ····· 37
5. 소결 ····· 38

제5장 우리나라 디지털 포렌식 현실 ····· 39
제1절 디지털 포렌식 관련 기관 ····· 39
1. 대검찰청 디지털수사과 ····· 39
2. 경찰청 사이버 안전국 ····· 40
3. 기타 수사기관 ····· 40
제2절 디지털 포렌식 절차 ····· 40
1. 디지털 포렌식 절차 ····· 40
가. 경찰 ····· 40
나. 검찰 ····· 41
2. 형사소송법 개정 전의 디지털 포렌식에 대한 법원의 태도 ····· 41
가. 전교조 압수·수색 준항고 기각 결정에 대한 재항고 결정(대법원 2011. 5. 26.자 2009모1190결정) ····· 41
나. 압수·수색 영장 별지 ····· 42
3. 형사소송법 개정 ····· 42
4. 검토 ····· 43
제3절 현재 수사기관에서의 디지털 포렌식 절차 ····· 43
제4절 디지털수사망(Digital Investigation Network, D-NET) ···· 44
1. 디지털 포렌식 관련 시스템 구축 필요성 ····· 44
2. 디지털수사망 구축 ····· 45
3. 디지털수사망 개요 ····· 45
4. 각 시스템의 구체적 내용 ····· 47
가. DFIS II ····· 47
나. 디지털증거관리시스템 ····· 48
다. 통합디지털증거분석시스템(IDEAS) ····· 49
(1) 주요인물 등록 ····· 50
(2) 파일 분석 등 동종의 디지털 압수물 분석 ····· 50
(3) 통합상관도 ····· 51

5. NFI의 XIRAF ····· 53
가. 개요 ····· 53
나. XIRAF의 특징 ····· 54
다. 검토 ····· 55

제6장 검찰의 디지털 포렌식 절차 ····· 56

제1절 압수·수색 준비 ····· 57

1. 압수·수색을 위한 정보 수집 ····· 57
2. 영장 청구서 작성 ····· 57
3. 디지털 포렌식 수사지원요청 ····· 57
가. 사전 협의 ····· 58
나. 지원 요청 ····· 58
4. 디지털 데이터가 압수 대상인지 여부에 대한 문제 ····· 58
가. 견해의 대립 ····· 59
(1) 긍정설 ····· 59
(2) 부정설 ····· 60
나. 법원의 태도 ····· 60
다. 검토 ····· 60

제2절 압수·수색 현장에서 정보저장매체 수색 ····· 61

1. 현장 촬영 및 통제 ····· 61
2. 압수·수색 대상 특정 ····· 62
3. 피압수자 등 관련자의 협조 ····· 62
4. 원격지에 저장된 디지털 데이터에 대한 압수·수색의 문제 ····· 62
5. 피압수자 등의 협력 문제 ····· 63
가. 협력의무의 내용 ····· 64
나. 협력의무 명문의 규정 필요성 ····· 64
(1) 보전의무 ····· 64

(2) 제출의무 ····· 65
(3) 협의의 협력의무 ····· 65
다. 검토 ····· 66
제3절 정보저장매체에서 사건과 관련된 디지털 데이터 조사 ····· 66
1. 현장용 디지털 포렌식 도구의 문제 ····· 68
가. 현장용 디지털 포렌식 도구의 요건 ····· 68
(1) 정보저장매체의 확인 ····· 68
(2) 데이터 수색 준비 단계(저장매체 분리) ····· 68
(3) 안티포렌식 탐지·분석 단계 ····· 69
(4) 전체·선별 복사 단계 ····· 70
2. 디지털 증거 수집도구별 기능 비교 ····· 70
3. 검토 ····· 72
제4절 사건관련 파일 복제, 목록 작성 교부, 확인서 ····· 73
1. 구체적인 절차 ····· 73
2. 진정성, 무결성을 인정하기 위한 조치 ····· 73
제5절 복제한 디지털 압수물 업로드 및 색인 ····· 74
1. 시스템에 디지털 압수물을 업로드 하는 행위에 대한 문제 ····· 75
제6절 일선 수사부서에서의 검색, 출력, 복제 ····· 76
제7절 사건 종료 후 디지털 압수물의 처리 ····· 76
제8절 예외적인 경우 디지털 포렌식 절차 ····· 77
1. 예외적인 경우의 세부 절차 ····· 78
가. 압수할 정보저장매체의 분리 및 저장매체·정보시스템 압수 확인서 작성 ····· 78
나. 이미지 파일 생성 및 업로드와 정보저장매체의 환부, 가환부 ····· 79
다. 이미지 파일 분석, 분석한 디지털 데이터 업로드 ····· 79
2. 형사소송법 제106조 제3항 단서의 해석 문제 ····· 79
가. 문제점 ····· 79
나. 견해의 대립 ····· 80

다. 법원의 태도 ····· 80
라. 검토 ····· 81
(1) 압수방법의 문제 ····· 81
(2) 비례의 원칙 적용 ····· 81
(3) 소결 ····· 82
3. 형사소송법 제106조 제3항의 개정필요성 ····· 84
가. 문제점 ····· 84
나. 입법례 ····· 84
(1) 미국 연방형사소송규칙 제41조(e)(2)(B) ····· 84
(2) EU 사이버범죄 방지협약 ····· 84
다. 견해의 대립 ····· 85
(1) 개정 필요설 ····· 85
(2) 개정 불요설 ····· 86
라. 검토 ····· 86
4. 형사소송법 제106조 제3항 단서의 판단기준 ····· 87
가. 문제점 ····· 87
나. 판단기준 ····· 87
다. 검토 ····· 89
5. 형사소송법 제106조 제3항 단서의 판단시기 ····· 89
6. 사건과 관련된 디지털 데이터를 조사하는 행위의 법적 성질 ····· 91
가. 문제점 ····· 91
나. 견해의 대립 ····· 91
(1) 수색론 ····· 91
(2) 2단계 수색론 ····· 91
(3) 정보 확인절차론 ····· 92
다. 검토 ····· 92
7. 분석에 별도의 영장이 필요한지 여부 ····· 92
가. 문제점 ····· 92

나. 견해의 대립 ····· 93
다. 법원의 태도 ····· 94
라. 검토 ····· 94
8. 참여의 문제 ····· 95
가. 문제점 ····· 95
나. 입법례 ····· 95
다. 참여의 일반론 ····· 96
라. 디지털 데이터 압수와 관련된 참여 ····· 97
마. 검토 ····· 97

제7장 디지털 포렌식 모델에 대한 새로운 접근 ····· 99

제1절 현재 우리나라 디지털 포렌식 절차 ····· 99
1. 디지털 포렌식 관련 쟁점 ····· 99
2. 디지털 포렌식 절차 ····· 100
제2절 우리나라 디지털 포렌식 절차의 특징 ····· 100
1. 압수·수색 방법에 따른 특징 ····· 101
2. 각 절차별 확인 ····· 101
3. 디지털 포렌식 절차에 일선 수사팀의 역할 ····· 101
4. 디지털 압수물의 폐기 ····· 102
제3절 우리나라의 현실에 맞는 디지털 포렌식 절차 모델 제시 102
1. 기존의 디지털 포렌식 절차 모델 ····· 102
2. 디지털 포렌식 절차 모델 제시 ····· 103
가. 새로운 디지털 포렌식 절차 모델 제시 ····· 103
나. 디지털 포렌식 절차 모델의 세부 설명 ····· 104
(1) 준비(Preparation) 단계 ····· 104
(2) 수색(Search) 단계 ····· 104
(3) 조사(Examination) 단계 ····· 105

(4) 획득(Acquisition) 단계 ····· 106
(5) 1차 분석(1st Analysis) 단계 ····· 107
(6) 시스템 업로드 및 색인(System Upload & Index) 단계 ····· 107
(7) 2차 분석(2nd Analysis) ····· 107
(8) 제출(Presentation) 단계 ····· 107
(9) 폐기(Disposal) 단계 ····· 107

제8장 결론 ····· 109

참고문헌 ····· 113

Abstract ····· 117

<표 차례>

[표1] 파일 복사와 이미징의 차이점 ····· 12
[표2] Computer Forensic Investigative Process ····· 17
[표3] DFRWS Investigative Model ····· 17
[표4] Abstract Digital Forensics Model ····· 18
[표5] Integrated Digital Investigation Process ····· 20
[표6] Enhanced Digital Investigation Process Model ····· 21
[표7] Hierarchical Objectives based Framework ····· 22
[표8] Computer Forensics Field Triage Process Model ····· 23
[표9] Framework for a Digital Forensic Investigation ····· 24
[표10] Common Process Model for Incident and Computer Process ····· 24
[표11] Digital Forensic Model based on Malaysian Investigation Process ····· 25
[표12] Systematic Digital Forensic Investigation Model ····· 26
[표13] XIRAF framework architecture ····· 54
[표14] 현장 디지털 포렌식 도구 기능 비교 ····· 72
[표15] 새로운 디지털 포렌식 절차 모델 ····· 104
[표16] 조사 단계 세부 절차 ····· 106

<그림 차례>

[그림1] 디지털수사망의 구성 ····· 46
[그림2] 디지털수사망 초기화면 ····· 47
[그림3] 디지털수사통합업무관리시스템 일선 수사팀 화면 ····· 48
[그림4] IDEAS 통합검색 초기화면 ····· 49
[그림5] 주요인물 등록 화면 ····· 50
[그림6] 파일 분석 초기화면 ····· 51
[그림7] 파일 분석 화면 ····· 51
[그림8] 통합상관도 1 ····· 52
[그림9] 통합상관도 2 ····· 52
[그림10] 통합상관도 3 ····· 53

제1장 서설

제1절 연구 배경

현대 사회는 이미 거의 모든 정보가 디지털 형태로 생성, 저장되고, 유통되고 있다. 이미 아침에 스마트폰 알람으로 아침을 시작하고, 스마트 폰으로 뉴스를 검색하며, 내비게이션이 장착된 자동차로 출근하여, CCTV가 설치된 도로를 달려 전자신분증으로 출입이 가능한 직장에 도착하여 컴퓨터로 업무를 보는 것과 같이 우리의 일상 대부분의 생활이 디지털 기기를 이용하게 되었고, 이에 따라 우리가 원하던 원하지 않던 간에 디지털 데이터를 생산하고 사용하고 있다. 2020년에는 사물 인터넷 등으로 인하여 디지털 데이터의 양이 기하급수적으로 늘어나 44조 기가바이트(GB)에 이를 것으로 예측하고 있다.[1)]

이러한 현실에 자연스럽게 범죄를 수사하는 수사기관도 디지털 데이터에 대하여 관심을 가질 수밖에 없게 되었다. 일부 사이버 범죄에 국한되었던 디지털 증거가 거의 모든 범죄에 중요한 증거가 되었기 때문이다. 어떠한 경우는 디지털 증거가 '결정적인' 증거가 되어 수사기관은 디지털 데이터의 확보를 중요하게 생각하게 되었다. 하지만 디지털 데이터는 방대한 양이고, 서로 다른 종류의 기기에서 생산된 것이며, 어떻게 저장되고 유통되는지, 사람이 정확하게 알기는 어렵기 때문에, 기존의 물건에 대한 압수와 달리 여러 가지 문제점이 발생한다.

이에 따라 '디지털 포렌식'이라는 용어로 표현하는 디지털 데이터의 압수·수색 및 분석, 법정 제출에 이르는 전 절차에 대하여 연구하는 분야가 생기게 되었고, 우리나라의 수사기관도 디지털 포렌식 관련 부서를 신설하기에 이르렀다.

그러나 수사기관의 피의자에 대한 광범위한 디지털 데이터를 압수·수색하게 됨으로서 피의자의 프라이버시나 정보의 자기결정권 등 여러 기본권 침해가 심각한 문제가 되었다. 압수·수색의 목적인 실체적 진실 발견과 국민의 기본권 보장을 위한

1) 한국EMC가 2014. 4. 10. 발표한 "Digital Universe of Opportunities" 보고서에 따르면, 2013년 한해 생성된 디지털 데이터는 4.4조 기가바이트이며, 2020년에는 약10배가 증가한 44조 기가바이트가 될 것이라고 예상하였다.

적법절차의 원칙이라는 형사소송법상 두 개의 큰 이념의 조화로운 해석이 필요하다.

제2절 연구 목적

디지털 데이터에 대한 압수·수색은 보통 해당 디지털 데이터가 저장된 디지털 기기(이하 '정보저장매체' 라고 함) 자체를 압수하는 방법으로 이루어졌다. 이는 디지털 데이터의 특징인 대량성, 비가시성 등으로 인하여 기술적으로 어쩔 수 없는 것이라는 인식이 강하여 인정되고 있었다.

하지만 위와 같은 압수 방법은 정보저장매체에 저장된 사건과 관련 없는 광범위한 디지털 데이터를 압수·수색하는 결과가 되어 피의자의 기본권 침해 문제를 야기시켰다. 이에 형사소송법은 제106조 제3항 개정으로 디지털 데이터에 대한 압수방법에 대하여 규정하였으나, 이에 대한 해석이 나뉘고 있고 심지어 개정 논의도 있는 실정이다.

한편, 국민의 기본권을 보장하면서 디지털 데이터를 압수하는 방법에 대한 연구, 특히 현행 형사소송법 하에 일반적인 디지털 데이터의 압수·수색 및 분석에 대한 디지털 포렌식 절차에 대한 연구가 전무하다. 국내외 모두 정보저장매체 자체를 압수하는 방법을 기본으로 하여 디지털 포렌식 절차를 연구하였기 때문이다.

그러므로 본 논문은 기존의 디지털 포렌식 절차 모델에 대하여 살펴보고, 해외 각국의 디지털 포렌식 현실을 고찰한 다음, 수사기관 특히 검찰이 현행 형사소송법 하에서 행하고 있는 디지털 포렌식 절차에 대하여 알아보고자 한다. 그리고 이를 근거로 디지털 포렌식 절차를 확정하고 나아가 국민의 기본권을 보호하면서 수사의 목적을 달성할 수 있는 디지털 포렌식 절차 모델을 제시하고자 한다.

제3절 연구 방법

본 논문은 기존의 디지털 포렌식 절차 모델의 특징 및 장단점에 대하여 알아보고, 해외와 우리나라의 디지털 포렌식 현실을 관련 기관과 절차를 중심으로 살펴보겠다. 그리고 현재 실무상 수사기관, 특히 검찰이 수행하고 있는 디지털 포렌식 절차

에 대하여 구체적인 절차와 각 절차의 쟁점에 대하여 검토함으로서 현행 형사소송법 하에서 적합한 디지털 포렌식 절차를 도출해 보고자 한다.

우선 제2장에서는 디지털 데이터, 디지털 증거의 의미를 명확히 하기 위하여, '디지털 증거' 용어 사용의 부적절함을 지적하고 '디지털 압수물' 이라는 용어로 정의하여 사용하겠다. 디지털 압수물의 특징과 디지털 포렌식의 의의와 기본 원칙에 대하여 알아보도록 하겠다.

제3장에서는 기존에 국내외에서 연구된 디지털 포렌식 절차 모델에 대하여 검토를 하겠다. 각 모델을 1995. ~ 2003., 2004 ~ 2007., 2008.~현재로 나누어 각 모델의 절차, 특징, 장단점을 중심으로 살펴보겠다.

그리고 제4장에서는 국내의 디지털 포렌식 현실의 특징을 명확히 하기 위하여 해외의 디지털 포렌식 현실을 살펴보도록 하겠다. 이는 미국의 NIJ 등 관련기관 현황과 미국, EU의 사이버범죄방지조약, 영국, 독일의 디지털 포렌식 관련 입법례와 디지털 포렌식 절차에 대하여 알아보겠다.

제5장에서는 우리나라의 디지털 포렌식 관련기관 현황과 디지털 포렌식 절차에 대하여 살펴보겠다. 특히 디지털 포렌식 절차는 법원의 전교조 압수·수색 준항고 기각 결정에 대한 재항고 결정과 압수·수색 영장 별지 및 개정 형사소송법을 알아보겠다. 한편 현재 수사기관의 디지털 포렌식 절차 관련하여 검찰이 구축한 디지털 포렌식 시스템인 '디지털수사망'에 대하여 살펴보고, 해외의 이와 유사한 시스템에 대하여 알아보도록 하겠다.

제6장에서는 수사기관 특히 검찰의 디지털 포렌식 절차에 대하여 논하도록 하겠다. 구체적으로 형사소송법 제106조 제3항의 원칙과 예외에 따라 절차를 구분하여 살펴보겠다. 동조 본문의 원칙적인 절차인 ① 압수·수색 준비, ② 압수·수색 현장에서 정보저장매체 수색, ③ 정보저장매체에서 사건과 관련된 디지털 데이터를 찾음, ④ 사건관련 디지털 데이터 복제, 목록, 확인서 작성 및 교부, ⑤ 복제한 디지털 데이터 업로드 ⑥ 색인, 추출 및 일선 수사부서에서의 검색, 출력, 복제 등 세부절차에 대하여 서술하도록 하겠다. 여기에서 디지털 데이터의 압수의 대상 문제, 압수장소 관련 원격지에 저장된 디지털 데이터에 대한 압수·수색, 피압수자 등의 협력문제, 현장용 디지털 포렌식 도구의 문제에 대한 견해의 대립과 법원의 태도도 살

펴보고 어떠한 입장이 타당한지 검토해 보겠다.

그리고 동항 단서의 예외적인 상황에 적합한 세부 절차에 대하여 살펴본다. 특히 예외적인 상황의 경우 절차에 대하여 법원의 독특한 태도가 있는바, 이를 각 문제점 별로 나누어 서술해 보도록 하겠다. 이는 동항의 해석 문제, 동항의 개정 필요성 문제, 동항의 판단기준 문제, 정보저장매체 분석의 법적성질, 피의자와 변호인의 참여 문제, 기타의 문제에 대하여 법원의 태도와 여러 견해를 검토해보고 타당한 결론을 도출하겠다.

재7장에서는 앞서 살펴본 검찰의 디지털 포렌식 절차와 관련 문제점을 중심으로 형사소송법상 실체진실의 발견과 적법절차의 원칙을 조화한 디지털 포렌식 절차를 제시하도록 하겠다. 그리고 이 디지털 포렌식 절차를 일반적으로 적용할 수 있는 디지털 포렌식 절차 모델을 제시한다.

아직까지 현행 형사소송법에 대한 디지털 포렌식 절차 모델에 대한 연구는 없었다. 현행 형사소송법은 최근 해외의 디지털 데이터 압수에 대한 기본권 보호 강화 움직임과 관련하여 시사하는 바가 크다 할 것이다. 그러므로 이에 대한 디지털 포렌식 절차 모델의 연구는 우리나라뿐만 아니라, 전 세계적인 요구에 대한 대안으로서 미약하나마 작용을 하기 바란다.

제2장 디지털 포렌식의 의의

디지털 포렌식이 무엇을 의미하는지 알아보기 전에 디지털 데이터, 디지털 증거가 무엇인지에 대하여 명확히 할 필요가 있다. 현재 우리나라는 디지털 증거, 디지털 데이터, 전자 증거, 전자 문서 등 디지털 포렌식의 대상이 되는 것에 대한 용어를 혼용하여 사용하고 있기 때문에 어떠한 용어가 정확한 것이지 확인 할 필요가 있다. 그리고 디지털 포렌식의 의의와 절차 등에 대하여 알아보겠다.

제1절 디지털 증거의 의의 및 특징

1. 디지털 데이터의 의의

디지털이란 '아날로그에 대응되는 개념으로 자료를 연속적인 실수가 아닌, 특정한 최소 단위를 갖는 이산(離散)적인 수치를 이용하여 처리하는 방법'[2]을 말한다. 보통 0과 1을 이용하여 처리한다. 디지털 데이터란 '디지털 방식으로 생성, 저장, 유통되는 정보'를 의미한다. 디지털 방식으로 인하여, 아날로그 방식에 비하여 정보가 기하급수적으로 늘어나게 되었고, 디지털 데이터가 범죄의 증거가 되는 경우가 비일비재하게 되었다.

2. 디지털 증거의 의의

디지털 증거(Digital Evidence)에 대하여는 아직 하나의 형태로 정의되지 않고 있는 것으로 보인다. 가장 널리 알려진 디지털 증거에 대한 정의는 '디지털 형태로 저장되거나 전송되는 증거가치 있는 정보'[3] 또는 '디지털 형태로 저장되거나 전송되며 법정에서 신뢰할 수 있는 정보'[4]이다. 위 두 정의를 정리하면, 디지털 증거는 '디

2) 위키피디아 "디지털" 인용(http://ko.wikipedia.org/wiki/디지털)

3) 'Information of probative value stored or transmitted in digital form'. 1998년 미국 법무부 마약수사청, 연방수사국, 국세청 범죄수사단, 관세청, 항공우주국 등 연방기관의 증거분석연구소를 중심으로 구성된 디지털 증거에 대한 과학실무그룹(Scientific Working Group on Digital Evidence : SWGDE)에서 정의한 내용. 대검찰청, 과학수사실무매뉴얼(2014), 제150쪽.

4) 'Information stored or transmitted in binary form that may be relied upon in court'. 1995년 세계 수사관들이 컴퓨터 포렌식 및 컴퓨터 수사와 관련된 정보를 교환하기 위해 구성한 국제 포럼(International Organization of Computer Evidence : IOCE). 대검찰청, 과학수사실무매뉴얼(2014), 제150쪽.

지털 형태의 정보'로서 '저장, 전송'되는 것으로 '법정에서 신뢰할 수 있는(증거가치 있는)' 정보라는 것이다.

가. 디지털 형태의 정보

그러므로 디지털 형태가 아닌 정보는 디지털 증거에 해당한다고 볼 수 없다. 전자증거(또는 전자적 증거)라는 용어가 디지털 정보와 혼동하여 많이 사용되나, 전자증거(Electronic Evidence)는 전기와 자기의 신호를 이용하여 저장, 유통되는 증거를 의미하는 것으로 저장 형태가 반드시 0과1로 이루어진 디지털 형태가 아니라, 아날로그 형태로도 가능하다는 점(녹음테이프나 비디오테이프)에서 엄밀한 의미에서는 서로 다른 의미라고 할 수 있다. 미국의 경우 과거 전자 증거라는 용어가 현재 디지털 증거로 바뀌어 사용되고 있지만, 여전히 전자 증거라는 의미는 혼용되고 있다. 하지만, 이날로그 형태의 전자 증거의 형태가 급격히 줄어들고 있는 현실에 비추어 보면, 전자증거를 디지털 증거와 혼용하여 사용하여도 그 의미를 혼동할 수 있을 가능성은 적다고 할 수 있겠다.[5)]

나. 저장 전송되는 정보

디지털 증거는 저장 또는 전송되고 있는 정보이다. 저장에는 그 기간이 문제되지 않는다. 그러므로 일시적 저장에 그치는 RAM(Random Access Memory)상의 저장된 정보도 디지털 증거에 해당한다.[6)]

다. 증거가치 있는 정보

한편, 디지털 증거는 법정에서 신뢰가치 있는 정보이어야 한다. 디지털 증거는 증거로서 의미 있는 정보이어야 한다는 것이다. 형사절차에서 범죄를 입증하거나 무

---

5) 이숙연, "형사소송에서의 디지털증거의 취급과 증거능력", 고려대학교 정보경영공학전문대학원 정보경영공학과 박사학위논문(2010), 제9-10쪽.

6) 이숙연, "형사소송에서의 디지털증거의 취급과 증거능력", 고려대학교 정보경영공학전문대학원 정보경영공학과 박사학위논문(2010), 제8쪽은 이를 ROM이라고 하였으나, RAM의 오기로 보인다. ROM(Read Only Memory)은 기록된 데이터는 빠른 속도로 읽을 수 있지만, 새로운 데이터는 저장할 수 없는 메모리이기 때문이다.

죄를 입증하는 증거를 의미하고, 직접 증거와 간접 증거를 모두 포함한다.[7]

3. '디지털 증거'라는 용어 사용 문제 - 디지털 압수물

그런데 디지털 증거를 압수하는 수사기관의 입장에서는 '디지털 증거'라는 용어의 사용에 주의해야 하는 면이 있다. 디지털 데이터를 압수한다고 하여도 압수한 디지털 데이터 모두가 증거가치 있다고 보기는 어렵기 때문이다.[8] 일반 유체물에 대한 압수의 경우에도 압수한 물건을 모두 '증거'라고 하지 않고, '압수물'이라고 부르는 것도 같은 이유일 것이다. 그러므로 수사기관의 입장에서 압수한 디지털 데이터의 경우 디지털 증거라고 부르는 대신 새로운 용어의 사용이 필요해 보인다. 이는 실제 압수한 디지털 데이터의 관리에 있어서도 중요한 문제이다. 특히, 증거로 제출되지 않은 디지털 데이터의 관리의 문제이다. 현재 디지털 데이터가 압수의 대상이 되는지에 대하여 현행 형사소송법 상 논란의 여지가 있으나, 실무는 압수한 디지털 데이터를 관리 하여야 하기 때문에 별도의 용어가 필요하다. '압수한 디지털 데이터'라고 부를 수도 있으나, 별도의 용어를 사용하는 것이 편리할 것으로 생각된다. 이 논문에서는 디지털 형태의 압수된 정보로서 기존의 유체물인 압수물이라는 용어에 디지털 데이터라는 특징을 알기 쉽게 하기 위하여 '디지털 압수물'이라는 용어로 사용하기로 한다. 물론 무형의 디지털 데이터가 압수의 대상이 되는지에 대하여 논란의 여지가 있으나, 후술 하겠지만, 이미 디지털 데이터가 압수의 대상이라는 전제에서 법원의 결정이 있고,[9] 디지털 데이터가 저장되어 있는 유체물과의 차이를 나타내기 위하여 위 용어가 적절해 보인다.

---

7) 이숙연, "형사소송에서의 디지털증거의 취급과 증거능력", 고려대학교 정보경영공학전문대학원 정보경영공학과 박사학위논문(2010), 제8쪽.

8) 형사소송법의 개정으로 인하여 사건과 관련된 디지털 데이터만 압수하도록 되어 있다(형사소송법 제106조 제3항). 하지만 사건과 관련된 디지털 데이터를 압수하였다 하더라도 이를 모두 증거로서 제출하지는 않기 때문에 압수한 디지털 데이터 모두를 디지털 증거라고 말하기에는 여전히 무리가 있다.

9) 대법원 2011. 5. 26.자 2009모1190결정.

제2절 디지털 압수물의 특징

기존의 연구에서 나타난 디지털 증거의 특징[10]을 종합해보면, 기존의 유체물인 압수물과 다른 점을 중심으로 매체독립성, 비가시성, 취약성, 대량성 등을 들 수 있다.

1. 매체독립성

디지털 압수물은 매체와는 독립하여 존재한다. 정보저장매체에 저장되어 있는 정보의 내용을 압수하는 것이다. 유체물이 아니라 정보 자체이기 때문에 기존의 압수에 관한 절차를 그대로 적용하기 어려운 면이 있다. 디지털 데이터를 압수하는 방법이나 압수·수색 영장 집행 방법에 있어 논란의 여지가 있다.[11]

2. 비가시성

디지털 압수물은 무체물로 정보저장매체에 이진수의 형태로 저장되어 있기 때문에 사람의 지각으로 바로 인지할 수 없어 소프트웨어나 프린터, 모니터 등의 출력장치를 통하여 볼 수밖에 없다. 압수·수색의 대상을 확정하는데 어려움이 있다.[12]

3. 취약성

디지털 압수물은 변경, 훼손이 쉽게 된다. 의도하던 의도하지 않던 디지털 데이터에 접근하는 순간 많은 변화가 일어나게 된다. 따라서 디지털 데이터의 위·변조 및 삭제에 대하여 밝히기도 쉽지 않고, 디지털 데이터를 압수할 때에도 디지털 압수물의 변경이 일어나지 않거나 최소한의 변경을 위한 여러 가지 조치가 요구된다.[13]

---

10) 이숙연, “형사소송에서의 디지털증거의 취급과 증거능력”, 고려대학교 정보경영공학전문대학원 정보경영공학과 박사학위논문(2010), 제16-19쪽에서는 잠재성, 이진성, 취약성, 대량성, 네트워크 관련성을, 양근원, “형사절차상 디지털 증거의 수집과 증거능력에 관한 연구”, 경희대학교 대학원 법학과 박사학위논문(2006), 제22-26쪽에서는 매체독립성, 비가시성, 비가독성, 원본과 사본의 구별의 곤란성, 취약성, 대량성, 전문성, 네트워크 관련성 등을 열거하고 있다.

11) 전승수, “형사절차상 디지털 증거의 압수 수색 및 증거능력에 관한 연구”, 서울대학교 대학원 박사학위논문, (2011), 제13쪽.

12) 전승수, “형사절차상 디지털 증거의 압수 수색 및 증거능력에 관한 연구”, 서울대학교 대학원 박사학위논문, (2011), 제13쪽.

13) 전승수, “형사절차상 디지털 증거의 압수 수색 및 증거능력에 관한 연구”, 서울대학교 대학원 박사학위논문, (2011), 제14쪽.

4. 대량성

정보저장매체에는 방대한 분량의 데이터가 저장되어 있다. 최근에는 저장매체의 발전으로 더욱 많은 정보를 작은 매체에 저장할 수 있게 되었다. 따라서 디지털 데이터의 압수 범위를 확정하는데 사용자의 프라이버시 등의 문제를 야기할 수 있다. 특히, 여러 사람이 공동으로 사용하는 서버와 같은 경우 더욱 문제가 된다. 한편, 대량성으로 인하여 디지털 데이터의 압수와 분석에 과거에 비하여 상당한 시간이 소요되고 있다.[14]

제3절 디지털 포렌식의 의의

1. 포렌식 사이언스(Forensic Science)의 의의

포렌식 사이언스(Forensic Science)는 흔히 법과학이라고 해석되어 통용되고 있는데, 법정에서 사용되는 정보를 수집하고 조사하는 과학적인 방법이다. 포렌식(forensics)이라는 용어는 라틴어의 'forēnsis'에서 유래한 것으로 대중 앞에서(의)(of or before the forum)라는 의미에서 유래되었다. 로마시대에 범죄의 기소는 공공·그룹 앞에서 사건을 설명하는 것을 의미하고, 범죄에 기소된 자와 고소한 자는 서로 자신의 관점에서의 이야기를 발표할 기회를 갖는다. 사건은 최선의 논쟁과 태도를 가진 개인의 기호에 따라 결정된다. 이러한 기원은 현대에 있어 포렌식이라는 단어가 '법적인 증거의 형태'와 '대중 앞에서 발표' 두 가지 현대적 의미를 가진다는 것을 의미한다. 포렌식 사이언스에서의 포렌식이라는 단어는 법적인 또는 법정과 관련된 것 이라는 의미와 동의어로 여겨진다.[15]

현대에는 응용과학 분야의 한 학문으로 '포렌식'이 인식되면서 과학수사를 위한 법의학, 포렌식 화학, 포렌식 인류학, 포렌식 DNA학, 포렌식 문서분석학, 포렌식 천문학 등 다양한 학문으로 발전하고 있다.

---

14) 전승수, "형사절차상 디지털 증거의 압수 수색 및 증거능력에 관한 연구", 서울대학교 대학원 박사학위논문, (2011), 제13-14쪽.

15) http://en.wikipedia.org/w/index.php?title=Forensic_science&redirect=no

2. 디지털 포렌식(Digital Forensics)의 의의

디지털 포렌식은 명확하게 정리된 개념이 아니라, 여전히 발전하고 있는 개념이다. 디지털 포렌식은 디지털 기기나 컴퓨터 범죄에 대하여 발견된 물질에 대한 복구나 조사를 아우르는 포렌식 사이언스에 한 분야이다. 이 용어는 본래 컴퓨터 포렌식과 동의어로 사용되었으나, 디지털 데이터를 저장할 수 있는 모든 기기에 대한 조사로 확장 되었다.

조사의 기술적인 특징은 관련된 디지털 기기의 종류에 따라 컴퓨터 포렌식, 네트워크 포렌식, 포렌식 데이터 분석 및 모바일 포렌식 등 여러 가지 분야로 나누어진다. 전형적인 포렌식 절차는 압수, 포렌식 이미지 취득, 디지털 정보의 분석과 수집된 증거에 대한 보고서 작성을 포함한다.[16]

위키피디아 개념에 의하면, 디지털 포렌식이란 디지털 데이터의 수집과 분석, 그리고 법정에의 제출 등을 아우르는 절차와 기술을 의미한다고 하겠다. 즉, 디지털 포렌식은 "디지털 데이터에서 증거를 보존(Preservation), 수집(Collection), 증명(Validation), 식별(Identification), 분석(Analysis), 해석(Interpretation), 기록(Documentation), 제출(Presentation)하기 위하여 과학적으로 이끌어내고 증명하는 방법"[17]이라고 할 수 있다.

3. 디지털 포렌식의 기본 원칙[18]

16) http://en.wikipedia.org/wiki/Digital_forensics

17) 정교일, "디지털 증거의 압수와 공판정에서의 제출방안", 대검찰청, 형사법의 신동향 통권 제25호(2010. 4.), 제122-123쪽. 위와 같은 절차가 디지털 포렌식 절차 모델인데, 현행 형사소송법에는 적합하지 않는 부분이 있는데, 이에 대하여는 후술하겠다.

18) 대검찰청, "과학수사 실무 매뉴얼", (2014), 제153쪽. 영국의 Association of Chief Police Officer(ACPO)에서는 "good practice guide for computer based electronic evidence"에서 컴퓨터 기반의 전자적 증거의 취급(The Principles of Computer-based electronic evidence)에 있어 다음의 4가지 원칙을 제시하고 있다.

1. 법정에서 신뢰를 얻기 위해서는 수사기관이나 수사관의 작업으로 인해 컴퓨터나 정보저장매체에 저장되어 있는 데이터가 변경되어서는 안 된다.(데이터의 무결성 강조)
2. 컴퓨터나 디지털 정보저장매체에 저장되어 있는 원 데이터에 접근해야 할 필요성이 있는 경우에는 해당 수사관은 반드시 그러한 작업을 수행할 수 있는 충분한 능력을 가지고 있어야 하고, 이후 수행된 각 행위가 디지털 증거를 확보하는 데 있어 밀접한 관련이 있는 행위였고, 그로 인해 어떠한 결과가 초래되었는지에 대하여 충분히 설명할 수 있어야 한다.(수사관의 전문성 강조)
3. 컴퓨터 기반의 전자적 증거에 수행된 모든 과정은 추적 가능할 수 있도록 기록되어 보존되어야 한다. 따라서 객관적인 제3자에 의하여 재현될 경우 동일한 결과 값이 산출되어야 한다.(수행 과정의 기록 및 결과의 재현가능성 강조)
4. 해당 사건의 조사를 담당하고 있는 수사관은 적법절차에 의해 전 과정이 수행되었음을 입증할 포괄적인

디지털 데이터가 증거 능력 있는 '증거'가 되기 위해서 지켜야할 디지털 포렌식의 기본 원칙이 있다.[19] 디지털 증거의 특징으로 인하여 적법절차 원칙을 준수하면서 신속하게 진행되어야 하고, 디지털 포렌식 전 과정에 있어 증거의 내용이 변경되지 않도록 하여야 한다.

가. 적법절차의 원칙

디지털 포렌식의 경우도 형사소송법의 이념인 적법절차의 원칙이 적용되는 것은 당연하다. 하지만 디지털 압수물의 대량성으로 인하여 하나의 디지털 기기[20]에는 범죄관련 이외의 정보가 엄청나게 들어 있고, 어떻게 다루느냐에 따라 다른 사건의 증거를 취득할 수도 있다. 그러므로 디지털 증거의 경우 위법수집증거배제법칙에 문제되는 경우가 많다. 유체물의 압수에서 보다 적법절차의 원칙이 더욱 요구되는 이유가 이 때문이다. 이와 관련하여 압수한 디지털 데이터에서 별건의 사건에 대한 증거가 나왔을 경우 위법수집증거배제법칙의 예외에 대한 논의도 활발하게 진행되고 있다.

나. 동일성, 무결성 유지

디지털 압수물은 변경되지 않아야 한다. 디지털 데이터를 압수, 분석하여 증거로 제출했을 경우, 제출한 디지털 증거가 압수한 디지털 데이터의 원본과 동일함이 증명되어야 한다. 그리고 디지털 증거를 수집 및 분석하는 전 과정에서 내용이 변경되지 않도록 무결성을 유지하여야 한다. 디지털 데이터의 취약성으로 인하여 의도하지 않았더라도 디지털 데이터에 접근하는 순간 쉽게 변경될 수 있다. 그러므로 디지털 압수물이 변경되지 않도록 하기위한 기술적, 절차적 방법이 필요하다.

책임을 진다.(적법절차 준수의 책임 강조)

19) 전승수, "형사절차상 디지털 증거의 압수수색 및 증거능력에 관한 연구" 서울대학교 대학원 법학과 박사학위 논문, 제21-23쪽은 정교일, "디지털 증거의 압수와 공판정에서의 제출방안", 대검찰청, 형사법의 신동향 통권 제25호(2010. 4.), 제125-126쪽의 디지털 포렌식의 기본 원칙으로 정당성의 원칙, 재현의 원칙, 신속성의 원칙, 절차 연속성의 원칙, 무결성의 원칙을 들고 있는데, 이중 정당성의 원칙은 적법절차의 준수와 동일하고, 신속성의 원칙은 일반적인 수사와 달리 디지털 포렌식에 특별하게 인정되기 어렵다고 하면서 적법절차의 준수, 증거의 무결성 유지, 재현의 원칙, 디지털 포렌식 절차의 문서화를 들고 있다. 그리고 대검찰청, "과학수사 실무 매뉴얼", (2014. 12.), 제153-154쪽은 적법절차 준수, 동일성, 무결성 유지, 신뢰성 확보를 들고 있다.

20) 이하에는 용어의 통일성을 위하여 형사소송법에서 사용하는 용어인 '정보저장매체'를 사용하기로 한다.

동일성, 무결성을 유지하는 기술적인 방법으로는 디지털 데이터에 대하여 이미지 파일을 생성하거나, 압수한 디지털 데이터에 대한 해시 함수를 작성하여 원래의 디지털 데이터와 비교하는 방법이 있다. 하지만 형사소송법상 압수 방법의 제한으로 인하여 동일성을 유지하는 기술적 방법은 한계에 이르렀다.[21]

○ 이미지 파일

• 이미징 기법

디지털 데이터를 압수할 때 정보저장매체 자체를 직접 분석 컴퓨터에 연결하여 조사, 분석을 하게 되면, 원래의 정보저장매체의 디지털 데이터가 변경 또는 삭제되어 디지털 데이터를 훼손할 우려가 있다. 이를 방지하게 위하여 정보저장매체 이미징(Storage Imagining) 방법을 이용하여 디지털 데이터를 압수하는 것이 보통이고, 이미징 기법에 의하여 생성된 파일을 디스크 이미지(Disk Image) 또는 이미지 파일[22]이라고 한다. 이미징 기법은 파일 복사와는 다른 기법으로 정보저장매체에 저장되어 있는 디지털 데이터를 비트 스트림(Bit Stream) 단위로 저장하는 방식이다.

구분	파일 복사 방식	이미징 방식
저장방식	Source Read & Destination Write	Bit Stream Clone
저장대상	파일과 디렉터리 단위의 정보	저장매체의 모든 물리적 클러스터
정보손실	Source Read 오류시 정보손실 발생	저장매체의 모든 정보 포함
파일복구	미할당 영역 정보를 수집하지 않음	수집된 미할당 영역에서 파일복구 가능

[표1] 파일 복사와 이미징의 차이점

이미징 방식의 가장 큰 특징은 미할당 영역에서 파일복구 가능이다. 이러한 특징으로 인하여 정보저장매체 자체가 아닌 해당 매체를 이미징한 이미지 파일만으로도 삭제된 디지털 데이터의 복구를 할 수 있다.

이미징 방식은 처음에 이미지 파일을 생성할 때 단 한번만 정보저장매체와의 연결이

21) 형사소송법 개정으로 인하여, 압수·수색 현장에서 정보저장매체의 사건과 관련된 디지털 데이터를 출력, 복제, 복사가 디지털 데이터 압수의 원칙이 되었기 때문에, 압수한 디지털 데이터의 해시 값을 작성했다고 하더라도, 사후에 정보저장매체의 '원본'인 디지털 데이터가 손상된 경우 원래의 디지털 데이터의 해시 값이 달라져 동일성을 인정하기 어렵게 되었다. 그러므로 이를 보완할 수 있는 별도의 장치가 필요하게 되었다.

필요하기 때문에, 원래의 정보저장매체가 훼손될 가능성을 최소화 할 수 있는 방법이다.

또한 이미지 파일은 정보저장매체의 수많은 파일이 '하나의 파일' 형태로 되어 있기 때문에 이를 이용하여 분석을 하더라도 훼손, 변경의 위험이 없다.

다만, 이는 정보저장매체 전체에 대한 이미지 파일을 생성할 경우이다. 정보저장매체에 저장되어 있는 일부 디지털 데이터를 복제하는 것을 보통 '논리적 이미지(Logical images)' 또는 '논리적 이미지파일'이라고 하는데, 파일의 내용뿐만 아니라, 메타데이터[23]까지 동일하게 복사하여 생성한 파일로 단순히 파일의 내용만을 복사하는 파일 복사와는 다르지만, 삭제된 디지털 데이터의 복구는 할 수 없는 점이 이미지 파일과 다르다.[24]

○ 해시함수

• 해시 함수(hash function)는 "임의의 길이의 데이터를 고정된 길이의 데이터로 변환시키는 알고리즘이다. 해시 함수에 의해 얻어지는 값은 해시 값, 해시 코드, 체크섬 또는 해시 등으로 불린다. 해시 함수는 결정론적으로 작동해야 하며, 따라서 두 해시 값이 다르다면 그 해시 값에 대한 원래 데이터도 달라야 한다.(역은 성립하지 않는다) 해시 함수의 안전성은 입력 영역에서의 해시 충돌 확률로 결정되는데, 해시 충돌의 확률이 높을수록 서로 다른 데이터를 구별하기 어려워지고 검색하는 비용이 증가하게 된다."[25]

• 암호 해시 함수(cryptographic hash function)는 해시 함수의 일종으로, 해시 값으로부터 원래의 입력 값과의 관계를 찾기 어려운 성질을 가지는 경우를 의미하는데, 암호 해시 함수의 성질은 다음과 같다[26]

· 역상 저항성(preimage resistance): 주어진 해시 값에 대해, 그 해시 값을 생성하는 입력 값을 찾는 것이 계산상 어렵다. 즉, 제1역상 공격에 대해 안전해야 한다. 이 성질은 일방향함수와 연관되어 있다.

· 제 2 역상 저항성(second preimage resistance): 입력 값에 대해, 그 입력의 해시 값을 바꾸지 않으면서 입력을 변경하는 것이 계산상 어렵다. 즉, 제 2 역상 공격에

대해 안전해야 한다.

· 충돌 저항성(collision resistance): 해시 충돌에 대해 안전해야 한다. 같은 해시 값을 생성하는 두 개의 입력 값을 찾는 것이 계산상 어려워야 한다.

즉, 암호화 해시 함수는 입력 값과 해시 값에 대해서, 해시 값을 망가뜨리지 않으면서 입력 값을 수정하는 공격에 대해 안전해야 한다. 이러한 성질을 가지는 해시 값은 원래 입력 값을 의도적으로 손상시키지 않았는지에 대한 검증 장치로 사용할 수 있다.[27)]

• 암호 해시 함수의 안전성

최근 해시함수의 충돌 쌍을 효과적으로 찾을 수 있는 공격법이 개발되어 표준 해시 함수를 만들기 위한 프로젝트가 미국 NIST에서 진행되고 있다. 또한 디지털 포렌식 도구에서 많이 사용되고 있는 MD5에서 충돌쌍이 발견되어 안성성에 대한 문제가 제기되고 있다.

하지만 무결성 유지를 위해 사용하는 방법에 문제가 있으려면, 제2역상 저항성을 발견할 수 있어야 하는데, 충돌 쌍을 발견하는 것과 제2역상을 발견하는 것은 근본적인 차이가 있으며, 제2역상을 효과적으로 찾는 방법은 아직까지 알려져 있지 않다. 그러므로 무결성 유지를 위한 MD5 함수의 사용은 안전성에 큰 문제가 되지는 않는다고 하겠다.[28)]

절차적인 방법으로는 디지털 데이터를 압수하는 현장에서 피압수자나 변호인에게 디지털 압수물이 원래의 디지털 데이터와 동일하다는 것을 확인하는 절차, 수집 분석 등의 전 과정을 문서화(documentation)하여 보관의 연속성(Chain of Custody)을 준수하는 방법 등이 있다.

---

22) 논리적 이미지 파일과 구분하여 물리적 이미지 파일이라고도 한다.
23) 사용자가 입력한 데이터를 설명하거나, 관리하기 위한 데이터로 응용프로그램에서 자동적으로 생성되기 때문에 메타데이터의 확보가 중요하다.
24) 그러므로 현장에서 사건과 관련된 디지털 데이터만 압수할 경우에는 삭제된 데이터가 있는지 여부에 대한 탐지가 중요하다.
25) http://ko.wikipedia.org/wiki/%ED%95%B4%EC%8B%9C_%ED%95%A8%EC%88%98
26) http://ko.wikipedia.org/wiki/암호화_해시_함수
27) Message Digest5(MD5)의 경우 다른 두 데이터가 동일한 해시 값을 가질 확률은 $1/2^{128}$, SHA1의 경우는 $1/2^{160}$ 등으로 동일한 해시 값을 산출하는 것은 사실상 불가능하다.
28) 이상진, "디지털 포렌식 개론"(2010), 제242-243쪽.

다. 재현의 원칙

디지털 압수물을 가시화나 분석하였을 때, 동일한 조건에서는 동일한 결과가 나와야 한다는 것을 의미한다.

이 원칙은 수사기관의 입장에서 가시화되어 증거로 제출된 디지털 증거가 법정에서도 재현 가능하도록 하여야 하기 때문에 더욱 중요하다. 이는 디지털 압수물의 보관 문제와도 밀접한 관계가 있다. 법원에 제출하는 디지털 증거가 디지털 압수물인 정보저장매체 전체의 이미지 파일에서 나온 경우, 전체 이미지 파일에서 해당 디지털 증거가 나왔다는 것을 증명해야 하므로 재판이 확정될 때까지 사건과 직접적인 관련이 없어도 전체 이미지 파일을 보관해야 한다.

한편, 다양한 디지털 포렌식 도구를 사용한다고 하더라도 동일한 디지털 데이터를 조사하였을 경우 항상 같은 결과를 도출한다는 것을 의미하지는 않는다.[29] 신뢰성 있는 도구를 전문가가 일반적으로 통용되는 기술과 지식을 사용하여 가시화나 분석을 하였을 경우 언제 어디서나 통일한 결과가 나와야 한다는 것을 의미한다.

라. 신속성의 원칙

수사의 전 과정을 신속하게 진행되어야 함은 수사의 일반원칙이다. 그러나 형사소송법의 개정(제106조 제3항)으로 인하여 디지털 데이터의 압수 현장에서 사건과 관련된 디지털 데이터를 압수하는 것이 원칙이기 때문에 압수 현장에서 사건과 관련된 디지털 데이터를 신속하게 찾아내어 압수하는 것이 중요하게 되었다. 또한 전원이 켜진 상태에서만 존재하는 데이터(Live Data)가 사건과 관련된 경우 전원이 꺼지기 전에 신속하게 압수하여야 한다.

29) 정교일, “디지털 증거의 압수와 공판정에서의 제출방안”, 대검찰청, 형사법의 신동향 통권 제25호(2010. 4.), 제125쪽에서는 다양한 증거 분석 도구를 사용한다고 하더라도 동일한 대상 시스템을 조사하였을 경우 같은 결과가 도출되어야 한다고 서술하였는데, 의문이다. 증거 분석 도구, 즉 디지털 포렌식 도구는 각각 특성에 따라 동일한 디지털 데이터에 대하여 다른 결과를 도출할 수도 있기 때문이다. 이것이 신뢰성 있는 도구를 사용해야 하는 이유이기도 하다.

제3장 기존의 디지털 포렌식 절차 모델

제1절 디지털 포렌식 절차 모델

디지털 포렌식 수사에 적용된 절차는 수사의 결과에 직접적인 영향을 끼친다. 부적절한 포렌식 절차의 선택은 증거능력을 상실하게 되어 디지털 증거를 잃어버릴 수 있기 때문이다. 디지털 포렌식 수사관으로 하여금 디지털 포렌식 절차를 수행하는데 적절한 메커니즘을 제공하는 표준을 '디지털 포렌식 절차 모델'이라고 한다. 제대로 구축된 절차 모델 존재는 디지털 포렌식 수사관으로 하여금 적절한 메커니즘을 제공하게 된다.

이러한 디지털 포렌식 절차 모델에 대하여 많은 연구가 이루어진바, 시간적 순서대로 세 개의 분류로 하여 각 모델에 대하여 설명하고, 장단점을 소개하도록 하겠다.[30]. 각각의 연구는 절차 모델에 대하여 model, procedure, process, phase, tasks 등 여러 가지 용어를 사용했으나 혼동을 줄이고자, '절차 모델'로 통일하여 서술하도록 하겠다.

제2절 구체적인 디지털 포렌식 절차 모델

1. 1995.~2003.의 디지털 포렌식 절차 모델

가. Computer Forensic Investigative Process (1995)[31]

Pollitt은 과학적으로 신뢰할 수 있으면서 법으로 수용할 수 있는 결과를 위하여 디지털 증거를 다루는 방법을 제안하였는데, 이는 획득(Acquisition), 식별(Identification), 평가(Evaluation), 제출(Admission)의 4단계의 절차로 구성된다.

---

30) 디지털 포렌식 절차 모델의 내용은 Yunus Yusoff, Roslan Ismail and Zainuddin Hassan, "Common Phases Of Computer Forensics Investigation Model", International Journal of Computer Science & Information Technology (IJCSIT), Vol 3, No 3,(2011.6.)과 Ritu Agarwal, Suvarna Kothari, "Review of Digital Forensic Investigation Frameworks", Information Science and Applications Volume 339(2015)의 내용을 참고하였다.

31) M. M. Pollitt, "Computer Forensics: An Approach to Evidence in Cyberspace", in Proceeding of the National Information Systems Security Conference, Baltimore, MD, Vol. II(1995).

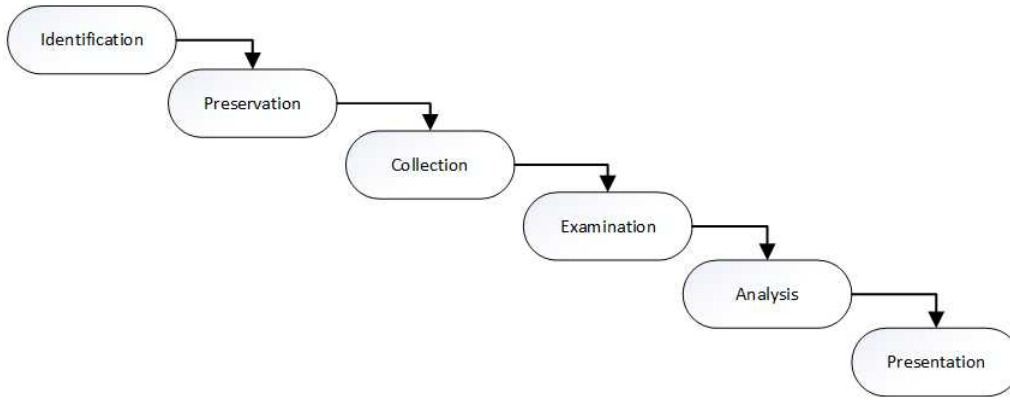
[표2] Computer Forensic Investigative Process

획득 단계는 영장에 승인된 수용할 수 있는 방법으로 증거를 얻는 것이다. 식별 단계는 획득한 디지털 증거에서 디지털 요소들을 식별하고 인간이 인식할 수 있는 형태로 변환하는 단계이다. 평가 단계는 전 단계에서 식별된 내용들이 실제로 사건의 중요한 요소인지, 적법한 증거로서 고려될 수 있는지 결정하는 단계이다. 제출 단계는 획득하고 추출한 증거가 법정에 제출되는 단계이다.

이는 기술에 중점을 둔 가이드라인으로 별도의 절차를 고려하지 않은 단점이 있으나, 디지털 포렌식에 대한 최초의 절차 모델이라는 점에서 의미가 있다.

나. DFRWS Investigative Model (2001)[32)]

공권력 기관이 아닌 학술적인 기관이 모인 최초의 모임인 디지털 포렌식 연구 워크숍(The Digital Forensic Research Workshop, DFRWS) 2001. 제1회에서 일반적인 디지털 수사 절차를 제안하였다.



[표3] DFRWS Investigative Model

이는 식별(Identification), 보존(Preservation), 수집(Collection), 검사(Examination), 분석(Analysis), 제출(Presentation)의 단계로 구성되어 있다.

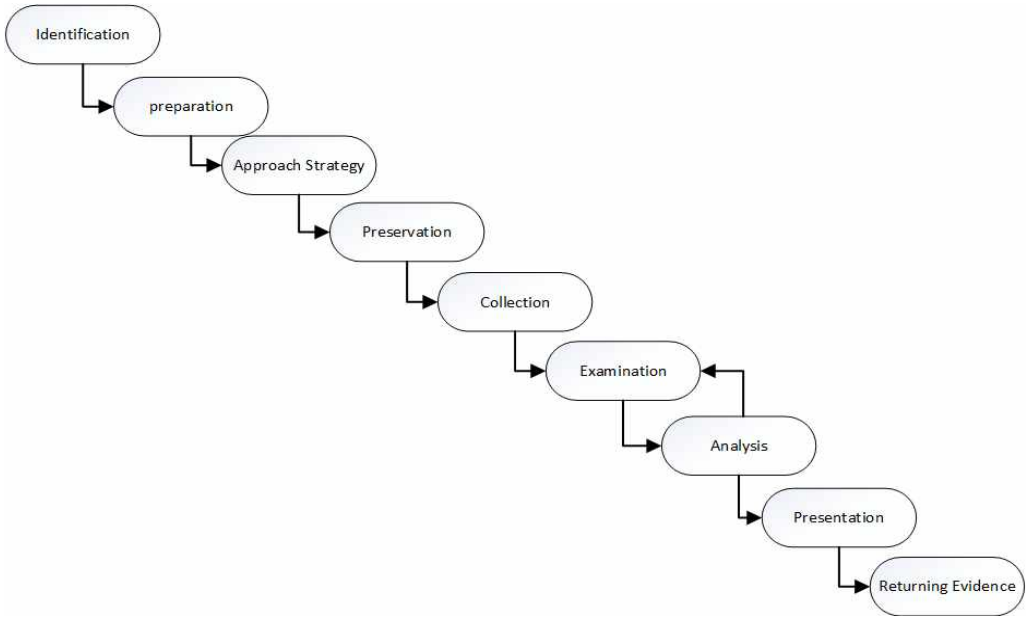
32) G. Palmer, "DTR-T001-01 Technical Report. A Road Map for Digital Forensic Research", Digital Forensics Workshop (DFRWS), Utica, New York(2001).

식별 단계는 프로필을 탐지하고 시스템을 확인하며, 회계 분석 등을 하는 단계이다. 보존 단계는 적절한 사건 관리를 위하여 준비하는 작업과 보관의 연속성(chain of custody)을 보장하는 작업 등을 포함하는데, 오염되지 않게 수집된 데이터라는 것을 보장하는 중요한 단계이다. 그리고 수집 단계는 승인된 여러 가지 복구 기술을 이용하여 중요한 데이터를 수집하는 단계이다. 검사와 분석 단계는 증거를 추적하거나, 증거 확인, 숨겨지거나 암호화된 데이터의 복구, 데이터 수집, 타임라인 분석 등을 하는 단계이다. 제출 단계는 문서화, 전문가 증언 등을 하는 단계이다.

이 절차 모델은 미래의 모델의 기초가 되고, 이를 토대로 많은 미래의 모델이 제안되었는데 큰 의의가 있다.

다. Abstract Digital Forensics Model (ADFM) (2002)[33]

Reith, Carr & Gunsch는 위의 DFRWS Investigative Model에서 강화된 모델을 제안하였다.



[표4] Abstract Digital Forensics Model

33) M. Reith, C. Carr & G. Gunsh, "An Examination of Digital Forensics Models", International Journal of Digital Evidence, Vol. 1, No. 3(2002).

이 절차 모델은 식별(Identification), 준비(Preparation), 접근 전략(Approach Strategy), 보존(Preservation), 수집(Collection), 검사(Examination), 분석(Analysis), 제출(Presentation), 증거반환(Returning Evidence)

위 모델에서 준비, 접근 전략, 증거 반환 단계가 추가되었다. 준비 단계에서는 도구를 준비하고, 기술을 확인하고 지원 방법을 찾는 단계이고, 접근 전략 단계는 오염되지 않은 증거의 획득을 극대화하면서 피해자나 주변 사람들의 부정적인 영향은 최소화 하는 단계이다. 증거 반환 단계는 증거를 정당한 소유자에게 반환하거나 적절하게 파기하는 단계를 말한다.

식별 단계는 사건의 형태를 알아내고 결정하는 단계이다. 준비 단계는 알아낸 사건 형태를 기초로 준비하는 단계이다. 보존 단계에서는 일반 압수물과 디지털 데이터 모두 제대로 격리, 보호되고 보존되어야 하고 보관의 연속성도 지켜져야 한다.

수집 단계에서는 데이터 추출이나 복제가 이루어진다. 체계적인 접근방법을 사용하여 수집된 데이터에서 잠재적인 증거를 식별하거나 찾아내는 단계가 검사 단계이다. 분석 단계는 증거의 중요한 결정 및 발견된 증거에 기초하여 결론을 그리는 작업을 의미한다. 검사와 분석 단계는 재귀적으로 행해질 수 있다. 제출 단계는 확인된 결과물을 요약하고 발표하는 단계이다.

이 절차 모델은 폭넓은 방법은 앞으로 다가올 디지털 기술에 잘 적응할 수 있는 절차 모델을 제안할 수 있는 등 사건의 분류를 잘 할 수 있는 장점이 있으나, 2단계가 3단계와 거의 같은 의미를 가지고 있어 중복이라는 비판이 있다.

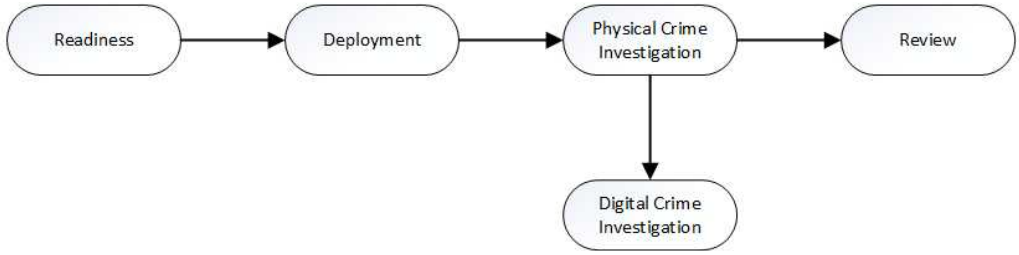
라. Integrated Digital Investigation Process (IDIP) (2003)[34)]

Carrier와 Spafford는 여러 가지 수사 절차를 하나로 통합하기 위한 의도로 이 절차를 제안하였다.

이는 준비(Readiness), 전개(Deployment), 일반 범죄 수사(Physical Crime Investigation), 일반 범죄 수사의 하위로 디지털 범죄 수사(Digital Crime

34) B. Carrier & E. H. Spafford, “Getting Physical with the Digital Investigation Process”, International Journal of Digital Evidence, Vol. 2, No. 2(2003).

Investigation), 검토(Review)의 단계로 되어 있다.



[표5] Integrated Digital Investigation Process

디지털 범죄 현장이라는 개념을 도입하여 디지털 증거에 대하여 소프트웨어나 하드웨어에 의하여 만들어진 가상의 환경을 설정하였다. 이 절차 모델은 미래의 어떠한 수사에도 지원할 수 있는 물질적이면서 운영 인프라의 구축을 위하여 필요한 단계부터 시작하였다. 준비 단계에는 장비를 준비해야 하며, 사람을 효과적으로 사용할 수 있어야 한다. 이는 실제로 조직의 라이프사이클 전반에 적용되는 절차이다.

전개 단계는 사건에 대하여 탐지하고 확인하기 위한 메커니즘을 제공한다. 이는 탐지 및 통보, 확인 및 인증 단계로 구성된다. 일반 증거의 수집 및 분석은 일반 범죄현장 조사 단계에서 행하게 된다. 보존, 조사, 문서화, 검색 및 수집, 재구성 및 발표가 하위 단계이다.

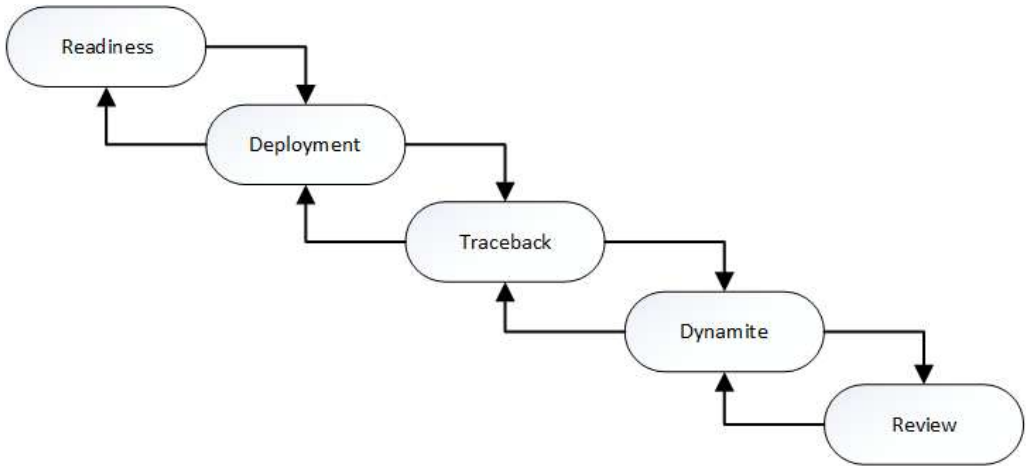
디지털 범죄 현장 수사 단계는 지금 디지털 환경에서의 디지털 증거에 초점을 맞추고 있음을 제외하고 실제 범죄 현장 수사와 유사하다. 마지막 단계는 검토 단계이다. 전체 디지털 범죄 조사 프로세스는 새로운 절차나 교육 요구사항을 도출하는 개선의 영역을 파악하기 위해 검토한다.

이 모델은 모든 사이버 테러 가능성이 있는 경우나 사건을 재구성을 하는 경우에도 적용되는 것이나, 혐의 현장과 피해 현장, 심지어 미리 조사하지 않으면, 디지털 범죄가 일어났는지 여부에 대하여 알아내기 불가능한 경우의 차이를 명확히 설명하지 못하는 단점이 있다.

2. 2004.~2007.의 디지털 포렌식 절차 모델

가. Enhanced Digital Investigation Process Model (EDIP) (2004)[35)]

Barayamueeba와 Tushabe는 기존의 Integrated Digital Investigation Model에 수정작업을 하고 단점을 보완하기 위해 역추적 단계(Trace back phase)와 다이너마이트 단계(Dynamite phase)라는 보강단계를 추가하여 1차 범죄현장과 2차 범죄현장 사이를 명확하게 구분하는 모델을 제안하였다. 이는 두 개의 범죄현장을 동시에 재구성하여 불일치를 최소화하기 위함이다. 이 모델에서는 1차와 2차 범죄현장이 framework에 의해 분리되어 있지만 단계가 선형이 아닌 반복적 패턴으로 묘사되었다.



[표6] Enhanced Digital Investigation Process Model

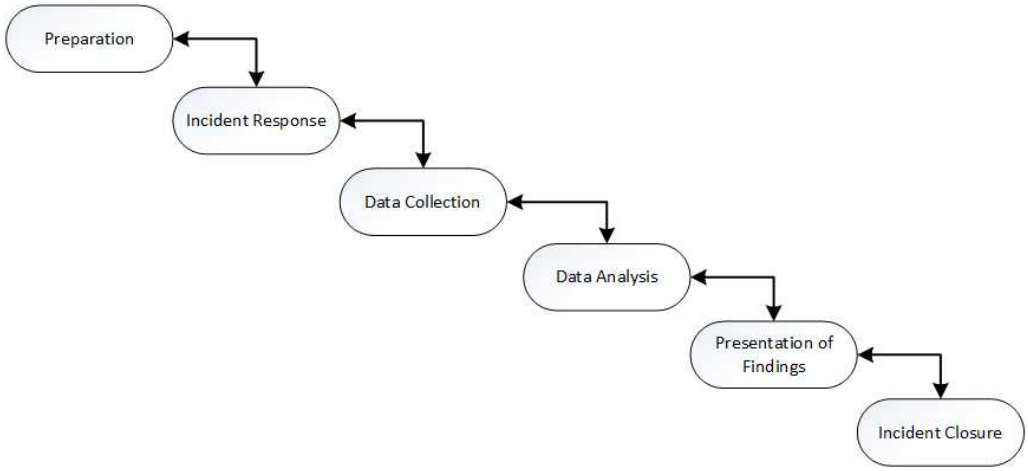
나. Hierarchical Objectives based Framework(2004)[36)]

이는 준비(Preparation), 사건 대응(Incident Response), 정보 수집(Data Collection), 정보 분석(Data Analysis), 증거 발표(Presentation of Findings), 사건 종결(Incident Closure)의 단계로 되어 있고, 각 단계는 반복적으로 수행 가능하다.

35) V. Baryamereeba & F. Tushabe, “The Enhanced Digital Investigation Process Model”, in Proceeding of Digital Forensic Research Workshop, Baltimore, MD(2004).
36) Beebe N., Clark J. "Hierarchical Objectives based Framework for the Digital Investigation Process" DFRWS(2004).

이 절차 모델에서는 지금까지 따르던 단일 단계 접근법과는 대조되게 다단계(multi tire) 접근법이 제시되었다. 이 process는 분석 업무가 수사 목적에 의해 분류되는 객체 중심의 개념(objectives based concept)을 적용하였다.

1차 단계는 위와 같이 이루어져 있고, 2차 단계에서는 data analysis의 하위 절차로 조사 단계(survey phase), 추출 단계(extract phase), 분석 단계(examine phase)로 구성된다. 이 절차 모델은 현실적인 면과 특수성에 있어 독보적인 장점을 가지고 있다.



[표7] Hierarchical Objectives based Framework[37]

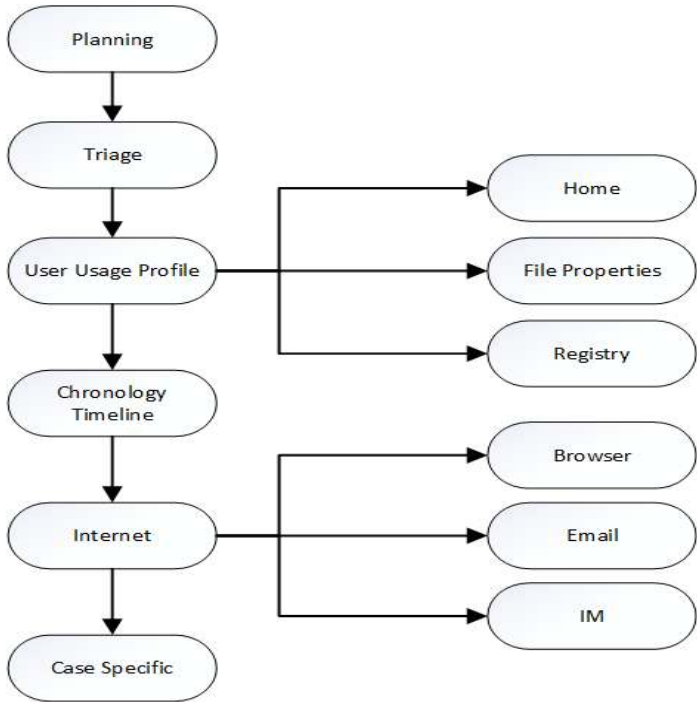
다. Computer Forensics Field Triage Process Model(2006.)[38]

이 절차 모델은 Integrated Digital Investigation Model에서 유래한 것으로 현실의 수사 방법과 매우 밀접한 관계가 있다. 정보저장매체를 제3의 사무실로 가져가서 조사하는 대신 디지털 증거의 확인(identification), 분석(analysis), 해석(interpretation)이 현장에서 이루어진다. 대부분의 디지털 포렌식 절차 모델과 비교했을 때 정반대의 절차로 개발되었다는 점이 특징이다.

37) Ritu Agarwal, Suvarna Kothari, "Review of Digital Forensic Investigation Frameworks", Information Science and Applications Volume 339(2015)
38) M. K. Rogers, J. Goldman, R. Mislan, T. Wedge & S. Debrota, “Computer Forensic Field Triage Process Model”, presented at the Conference on Digital Forensics, Security and Law(2006).

분류 단계에는 증거로서 중요한 단어(term)에 대하여 확인하고 순위화 한다. 사용자 사용 프로필 단계에서는 혐의 관련하여 사용자의 활동과 프로필에 중점을 두고 있고, 연대기적 연대표 단계는 예를 들면, MAC 타임 같은 시간을 알 수 있는 것에 중점을 두고 있으며, 인터넷 단계에는 사용자가 인터넷을 사용한 흔적을 브라우저, 이메일, instant message(IM)를 중점적으로 조사하는 단계이다.

이는 현실성 있고 실용적이라는 장점이 있으나, 특정 사건이나 상황에만 적용되고, 모든 상황에 적용하기 어려운 단점이 있다.



[표8] Computer Forensics Field Triage Process Model

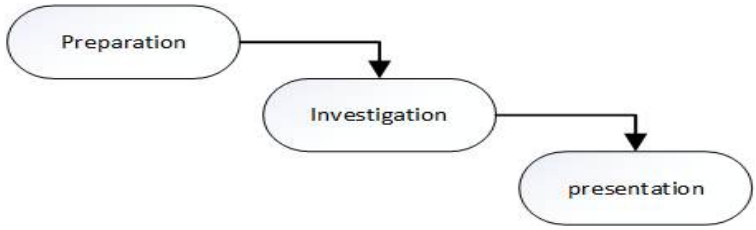
라. Framework for a Digital Forensic Investigation(2006)[39]

Kohn, Eloff, Oliver는 기존의 여러 디지털 포렌식 절차 모델이 복잡한 절차나 단계가 중복되거나 충돌하는 경향이 있으며, 전문용어에 서로 차이가 있다는 점을 발

39) M. Kohn, J. H. P. Eloff, & M. S. Olivier, “Framework for a Digital Forensic Investigation”, in Proceedings of the ISSA 2006 from Insight to Foresight Conference, Sandton, South Africa(2006).

견하고는 이미 제시된 이전 모델들을 합병하고자 하였다.

따라서 비슷한 업무를 그룹화 하여 준비(preparation), 수사(investigation), 보고(presentation)의 세 단계로 구성하면서, 여기서 중요한 점은 디지털 포렌식 절차 모델을 수립하는데 있어 관련 법적 지식이 필수적이라는 것이다.

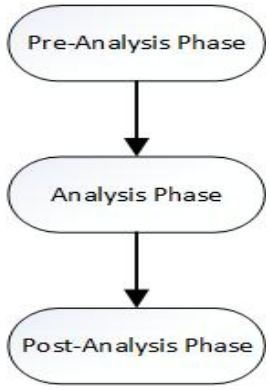


[표9] Framework for a Digital Forensic Investigation

이는 향후 필요할 여러 단계를 추가하여 쉽게 확장이 가능하다는 점이 장점이나, 현실적으로 아무런 절차가 없다는 단점이 있다.

마. Common Process Model for Incident and Computer Process(2007)[40]

Freiling과 Schwittay는 사건 대응과 디지털 포렌식의 두 개념을 합쳐 수사 절차의 전반에 걸쳐 새로운 모델을 제시하였다.



[표10] Common Process Model for Incident and Computer Process

이 모델은 특히 분석에 집중하여 사건 전 준비 단계(Pre-Incident preparation), 분

40) F. C. Freiling & B. Schwittay, "Common Process Model for Incident and Computer Forensics", in Proceedings of Conference on IT Incident Management and IT Forensics, Stuttgard, Germany(2007).

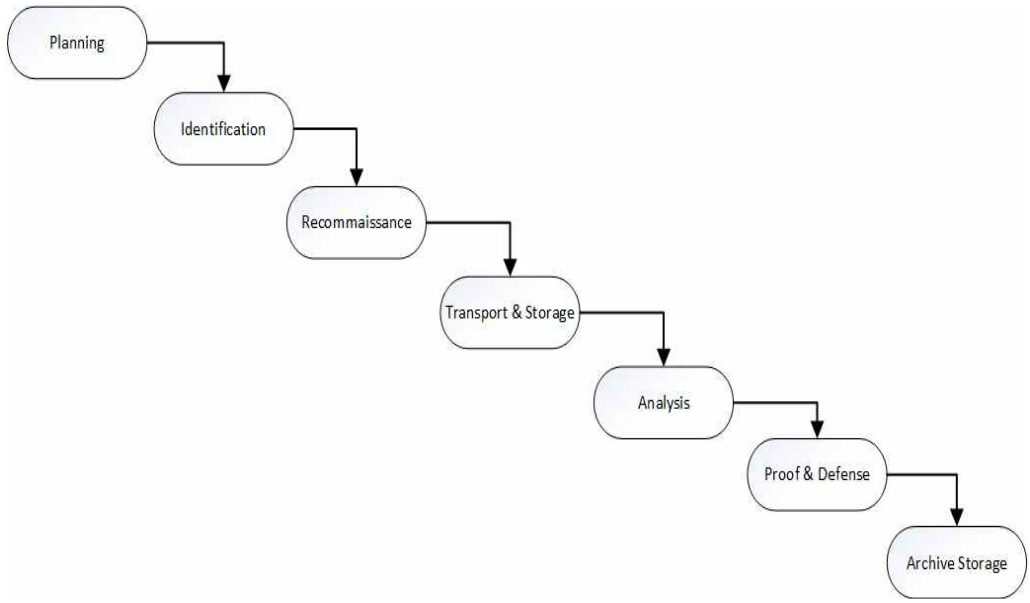
석 전 단계(Pre-analysis), 분석 단계(Analysis), 분석 후 단계(Post-analysis)로 되어 있다. 실제로 분석이 시작되기 전에, 완성된 모든 과정들이 분석 전 단계로 합쳐졌고, 분석 후 단계에서는 수사 과정에서 이루어진 활동에 대한 언급을 다루며, 분석 단계에서는 디지털 포렌식이 적용된다.

따라서 이 모델에 의하면 일반 사건 대응과 디지털 포렌식 분석을 아우르는 사건 대응을 위한 적절한 방법이 제시되었다는 평가가 있다.

3. 2008.~ 현재 디지털 포렌식 절차 모델

가. Digital Forensic Model based on Malaysian Investigation Process(2009)[41]

이 모델은 말레이시아의 수사 절차에 기반을 두어, 특히 취약한 증거에 집중하기 위해 라이브 데이터 획득(live data acquisition)과 정적 데이터 획득(static data acquisition)을 강조한 모델이다.



[표11] Digital Forensic Model based on Malaysian Investigation Process

정찰(Reconnaissance) 단계에서 라이브 포렌식과 같이 여전히 동작 중인 정보저장

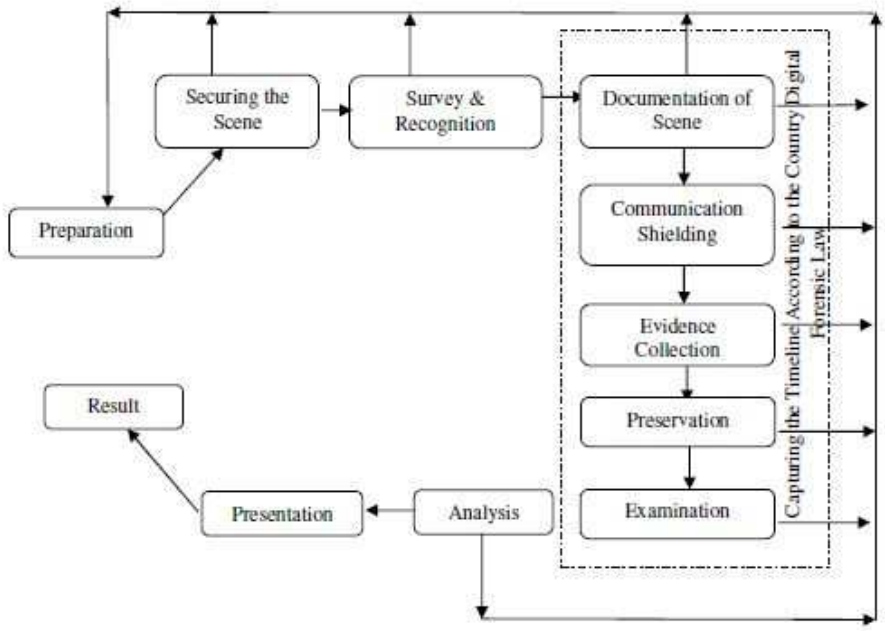
41) P. Sundresan, "Digital Forensic Model based on Malaysian Investigation Process", International Journal of Computer Science and Network Security, Vol. 9, No. 8(2009).

매체에서 라이브 데이터를 획득하는 것을 중점으로 하고 있고, 이동 및 저장 단계는 분석 전의 취약한 데이터를 안전하게 이동하고 저장하는 단계이다.

나. Systematic Digital Forensic Investigation Model(2011)[42]

Agawal은 디지털 포렌식 실무자와 관련 기관들이 적절한 전략이나 절차를 고안하는 데 있어 도움을 줄 수 있는 체계적인 모델을 확립하였다.

11단계로 구성되며 사이버 사기나 사이버 범죄관련 수사방법도 포함하고 있다.



[표12] Systematic Digital Forensic Investigation Model[43]

준비(Preparation), 현장 보존(Securing the scene), 조사 및 인식(Survey and Recognition), 현장 기록(Documenting the scene), 보호자와의 소통(Communication shielding), 증거 수집(Evidence collection), 보존(Preservation), 조사(Examination), 분석(Analysis), 보고(Presentation), 결과 및 검토(Result and Review) 단계로 구성된다. 이 모델은 사이버 범죄나 컴퓨터 사기를 연구하는 데 적합하고, 일반적인 디지

42) Agawal A., Gupta M., Gupta S., Gupta C., "Systematic Digital Forensic Investigation Model", International Journal of Computer Science and Security(2011).
43) Ritu Agarwal, Suvarna Kothari, "Review of Digital Forensic Investigation Frameworks", Information Science and Applications Volume 339(2015)

털 포렌식 모델로 하기에는 무리가 있다.

다. New Approach of Digital Forensic Model for Digital Forensic Investigation(2011)[44]

이 절차 모델은 4단계의 반복적인 접근법으로 이루어지는데, 1단계 준비(preparation), 시작(inception) 단계로 디지털 포렌식 수사를 위한 준비(preparation), 식별(identification), 허가(authorization), 소통(communication)의 4개의 규칙이 있고, 2단계는 상호작용(interaction) 단계로 수집(collection), 보존(preservation), 문서화(documentation)의 규칙이 있고, 3단계는 복원(reconstruction) 단계로 조사(examination), 탐사 시험(exploratory testing), 분석(analysis)의 규칙이 있으며, 4단계는 보고 단계로 결과(result), 검토(review), 보고(report)의 규칙이 있다.

이는 각 단계별 상호작용의 필요성과 실험적 테스트에 대해 확인이 가능한 반면, 모델의 개념이 모호하고 테스트된 적이 없어 현재로는 가설에만 기반하고, 어떻게 디지털 포렌식 수사 절차와 통합이 되는지에 대한 명확한 언급이 없다.

라. Harmonized Digital Forensic Investigation Process Model(2012)[45]

Valjarevic과 Venter는 기존 디지털 포렌식 절차 모델을 조화롭게 융합하고자 하여, 기존에 제안된 모델들과 매우 유사하지만, 각 단계를 다르게 배치하고 몇몇 디지털 포렌식 원리를 실행하는 데 있어 평행 작용(parallel action)이라는 새로운 개념을 이용하여 제시했다는 점에 차별화된다.

이는 사건 탐지(incident detection), 초기 대응(first response), 계획(planning), 준비(preparation), 사건 현장 기록(incident scene documentation), 잠재적 증거의 확인(potential evidence identification), 잠재적 증거의 수집(potential evidence collection), 잠재적 증거의 이동(potential evidence transportation), 잠재적 증거의 저장(potential evidence storage), 잠재적 증거의 분석(potential evidence analysis), 발표(presentation), 결론(conclusion)의 12 단계로 하부 단계 합친 다단계

44) Ademu O., Chris O., David S., "A New Approach of Digital Forensic Model for Digital Forensic Investigation", International Journal of Advanced Computer Science and Application(2011).
45) Valjarevic A., Venter H., "Harmonized Digital Forensic Investigation Process Model", IEEE(2012).

(multi-tiered) 모델을 제시하였다.

하지만, 이 모델도 제시만 되었고 정확도와 효율성에 대한 입증은 되지 않았기 때문에 입증절차가 필요하다는 단점이 있다.

마. Integrated Digital Forensic Process Model (2013)[46)]

이 모델은 준비(preparation) 사건(incident), 사건 대응(incident response), 물리적인 수사(physical investigation), 디지털 포렌식 수사(digital forensic investigation), 보고(presentation) 단계로 구성되어 있으며, 각 단계별로 세부 단계를 두었다.

이는 현재까지 여러 디지털 포렌식 절차 모델들의 문제점은 동일한 절차나 단계인데도 이름을 다르게 명명하거나, 각 단계에 대한 설명이 제각각 이라는 점을 제기하면서, 단지 기존 DFPM들의 단순한 병합이 아닌, 기존 모델들의 통합과 용어의 정제(purification)를 통해 모두를 통합하는 표준화된 디지털 포렌식 절차 모델을 제시하는 것이라고 주장하였다. 이 모델은 각 단계를 자세하게 세분하여 설명하고 있는 것이 장점이나, 동시에 지나치게 복잡하고 세부 단계 이외의 돌발 상황 발생시 적용이 어려운 약점이 있다.

제3절 실무상 디지털 포렌식 절차

미국 법무부에서 발간한 “Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition”[47)]에 의하면 사전준비 단계(Preparation), 현장 보존 단계(Securing and Evaluating the Scene), 현장 문서화 단계(Documenting the Scene), 증거 수집 단계(Evidence Collection), 디지털 증거의 팩킹, 운반, 저장 단계(Packaging, Transportation and Storage of Digital Evidence), 분석 단계(Analysis)로 8개의 과정으로 이루어져 있고, 우리나라의 경찰청 포렌식 프로세스 모델은 사전준비(Preparation), 증거수집(Collection), 조사(Examination), 분석의뢰, 접수, 운반

46) Kohn M., Eloff M., Eloff JHP., "Integrated Digital Forensic Process Model", International Journal of Computer Science and Security(2013.)

47) https://www.ncjrs.gov/pdffiles1/nij/219941.pdf

(Evidence Request, Receipt & Transport), 증거분석(Analysis), 결과보고서(Reporting), 보존 및 증거관리(Preservation & Evidence Management)로 7개의 과정으로 되어 있다. 이들 절차를 보면, 실무는 아직까지 초기의 DFRWS Investigative Model에서 크게 벗어나고 있지 않다는 것이다.

제4절 소결

디지털 포렌식 절차 모델과 관련하여 초기(1995. ~ 2003.)에는 절차를 표현하는 데 그쳤으나, 초기의 모델을 기반으로 몇 가지 절차를 추가하거나 순서를 바꾸는 등 발전된 디지털 포렌식 절차 모델이 연구되었다(2004. ~ 2007.). 그러다 최근에는 모든 사건의 경우를 포함할 수 있는 '통합' 디지털 포렌식 절차 모델의 연구가 활발히 진행되고 있다(2008. ~ 현재).

하지만 각국의 디지털 포렌식 현실에 따라 디지털 포렌식 절차 모델이 달라질 수 밖에 없다. 디지털 포렌식은 기술적인 측면만 있는 것이 아니라, 법률적인 측면도 있기 때문이다.

다음 장에서는 해외 각국의 디지털 포렌식 현실과 우리나라의 디지털 포렌식 현실 및 우리나라 검찰의 디지털 포렌식 절차 실무를 살펴보고, 위의 디지털 포렌식 절차 모델을 비교하여 보겠다.

제4장 해외 디지털 포렌식 현실

디지털 포렌식은 디지털 데이터에 대한 압수 절차와 기술을 의미한다. 기술적인 측면에서는 국제적으로 기술이 통용되므로, 항상 첨단 기술에 대한 동향 파악과 연구가 필요하다. 이에 비하여 제도적인 측면은 각 나라의 형사소송 절차나 디지털 증거를 보는 시각 등의 사정에 따라 차이가 있다. 기술적으로 각국의 연구 기관과 법, 제도적인 측면에서 각국의 디지털 증거 압수 절차에 대하여 알아본다.

제1절 외국의 디지털 포렌식 기관

해외의 경우 디지털 포렌식을 수행하고 있는 기관에 대하여 상세 자료에 대하여 미공개 하고 있다. 미국과 네덜란드의 경우에는 정보가 공개되어 있는바, 미국은 법무부 산하의 NIJ, NIST, RDFL, DCFL 등이 있고, 네덜란드는 NFI가 있다.

1. NIJ(National Institute of Justice)

법무부 산하 기관으로 디지털 포렌식 관련 연구개발(Electronic Crime Program[48])을 총괄하고 있다. 디지털 관련 범죄의 퇴치 및 주와 지방의 법집행기관에 도움을 주기 위한 도구 개발을 지원하고 있다. 또한 디지털 포렌식 관련 가이드[49]를 발간하는 등 산하기관에 디지털 포렌식 관련 표준 확립 및 교육도 힘쓰고 있다.

2. NIST (National Institute of Standard and Technology)

NIST는 미국 상무부 산하의 과학기술 표준을 개발하는 연구소로, 디지털 포렌식

48) http://nij.gov/topics/forensics/evidence/digital/pages/welcome.aspx 이 프로그램은 디지털 증거 조사 도구, 디지털 증거 분석 도구, 디지털 포렌식 표준 및 역량 강화를 중점으로 하고 있다.

49) ① Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors, ② Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition, ③ Forensic Examination of Digital Evidence: A Guide for Law Enforcement, ④ Investigations Involving the Internet and Computer Networks, ⑤ Investigative Uses of Technology: Devices, Tools, and Techniques 등의 가이드가 있다. http://nij.gov/topics/forensics/evidence/digital/pages/welcome.aspx

관련 기술 표준에 대한 연구도 수행하고 있다.[50] 디지털 포렌식 도구 검증을 하는 CFTT(Computer Forensic Tool Testing) 프로젝트를 수행하고 있다. 또한 이미 널리 알려진 파일에 대한 해시 값을 데이터베이스로 구축하여 디지털 포렌식 수사에 활용할 수 있도록 하는 NSRL(National Software Reference Library) 프로젝트를 진행하고 있다.

3. RCFL (Regional Computer Forensics Laboratory)[51]

RCFL는 테러, 아동 포르노, 인터넷 범죄, 사기 등에 대한 디지털 증거 조사를 전적으로 지원하기 위한 연구소 및 훈련 기관이다. 시카고 등 15개의 지역 사무소를 두고 있다.

2002년 FBI는 RCFL의 작업을 감독하고 새로운 시설을 손쉽게 만들기 위하여 NPO(National Program Office)를 설립했다. 이는 각 기관의 RCFL의 설립 및 관리에 관한 정책, 관행 및 법적 절차를 제도화, 각 기관 간의 정보 교환과 정보 교환을 위한 센터로서의 역할을 하여 법집행기관, 민간, 학계 등의 업무 관계를 육성하고, FBI와 다른 정부 기관에 새로운 디지털 포렌식 도구를 개발하고, 디지털 포렌식 수사관에 대한 교육과정 개설 등을 지원한다.

4. DCFL (Defense Computer Forensics Laboratory)[52]

미국 국방부 사이버범죄 센터(Defense Cyber Crime Center)의 디지털 포렌식 전담 부서로서, 국방부 산하기관의 디지털 포렌식을 지원하고 있다.

DCFL는 2005년 9월 the American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB)의 ISO 17025 "Forensic Science Testing"표준을 준수하며, 2012년 한해 1406건, 834.58TB를 분석했다.

---

50) http://www.nist.gov/computer-forensics-portal.cfm
51) http://www.rcfl.gov/about
52) http://www.dc3.mil/digital-forensics/about-dcfl

5. 네덜란드의 NFI (Netherlands Forensic Institute)[53]

법적 의무와 권한이 전혀 없는 순수 연구소로서, 네덜란드의 경찰, 검찰 등 모든 기관뿐만 아니라 UN 등 국제기구에게 디지털 포렌식 도구와 서비스를 제공하고 있다.

NFI는 디지털 포렌식 도구[54]와 서비스[55]를 제공하고 디지털 포렌식 관련 컨설팅과 교육도 수행하고 있다.

디지털 포렌식 관련하여 가장 유명한 연구소로 광범위한 연구개발과 도구를 제작하고 있는 곳으로, 많은 예산과 연구원[56]을 투입하여 디지털 포렌식 기술을 선도하고 있다.

제2절 외국의 디지털 포렌식 관련 현실

1. 미국의 디지털 포렌식 관련 현실

가. 입법례

(1) 디지털 데이터가 압수의 대상인지 여부

무형의 디지털 데이터가 압수의 목적물이 되는지 여부에 대하여, 연방대법원은 United State v. New York Telephone Co. 판결에서 연방 형사소송 규칙 제41조 (a) (2) '정의'의 압수·수색의 대상이 되는 "물건(Property)" 규정이 한정적 열거규정이 아니므로, 유체물에 한정하는 규정 아니라고 판시하면서, 무형의 디지털 데이터가 대한 압수 대상이 된다고 판시하였다. 이 후 위 규정을 압수·수색의 대상이 되는 물건에 "정보(Information)"를 포함하도록 개정하여 디지털 데이터 자체가 압수의 대상이 됨을 명시[57]했다.

---

53) www.forensicinstitute.nl

54) NFI가 개발한 디지털 포렌식 도구는 Bonaparte, Defraser, Faraday Cage, Memory Toolkit, PRNU Compare Professional, XIRAF 등이 있다.

55) NFI가 제공하는 서비스로는 CBRNe, Fingermark Individualization, Forensics in Nuclear Security, Kecida, Mobile Phone Data Recovery, Wildlife Forensics 등이 있다.

56) 2009년 현재 NFI의 예산은 1,120억 원이고, 직원 수는 연구원을 포함 554명이다.

57) Federal Rules of Criminal Procedure - Rule 41. Search and Seizure
(a) Scope and Definitions
(2) Definitions

(2) 관련 규정

연방형사소송규칙 제41조 (e)의 (2)(B)는, "(e)(2)(A)에 의한 영장으로 전자적 저장매체나 전자적으로 저장된 정보를 압수하거나 복사할 수 있다. 영장에 달리 기재되지 않는 한, 영장은 영장에 부합하는 위 매체나 정보에 대하여 추후에 검토할 권한을 부여한다. 위 영장의 집행 시간은 매체나 정보의 압수나 현장 복사에만 적용되고, 이후 집행 현장 이 외에서의 복사, 검토에는 적용되지 아니한다."고 규정하고 있다.[58]

또 디지털 데이터의 압수·수색 방법에 대하여, 연방형사소송규칙 제41조의 (f)(1)(B)는 "전자적 저장매체의 압수 또는 전자적으로 저장된 정보의 압수나 복사의 경우, 압수물 목록은 압수나 복사된 물리적 저장매체의 기재로 한정할 수 있다. 수사기관은 압수 또는 복사된 전자정보의 복사본을 보유할 수 있"도록 규정하고 있다.[59] 위 규정에 의하여 디지털 증거의 압수 방법에 대한 특별한 제한 없이 저장매체 자체의 압수나 해당 정보를 복사하는 방법으로 압수할 수 있음을 알 수 있다.[60]

나. 디지털 포렌식 절차 관련

미국 법무부가 제시한 "Electronic Crime Scene Investigation: A Guide for First Responders[61]"에 의하면, 디지털 포렌식 절차는 사전 준비(Preparation) → 수집(Collection) → 현장 보존 (Securing and Evaluating the Scene) → 현장의 문서화

(A) "Property" includes documents, books, papers, any other tangible objects, and information.

58) Rule 41. Search and Seizure

(e) Issuing the Warrant.

(2) Contents of the Warrant.

(B) Warrant Seeking Electronically Stored Information. A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.

59) (f) Executing and Returning the Warrant.

(1) Warrant to Search for and Seize a Person or Property.

(B) ... In a case involving the seizure of electronic storage media or the seizure or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied. The officer may retain a copy of the electronically stored information that was seized or copied.

60) 이숙연, "디지털증거의 압수수색", 형사법 실무연구(2011), 제641쪽.

61) Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition

(Documenting the Scene) → 증거 수집(Evidence Collection) → 분석(Analysis) → 보고서(Reporting)이다.

여기서 살펴보면, 수집을 하고 나중에 증거 수집을 하는 단계로 구성되어 있는데, 이는 현장에서 디지털 저장매체 자체를 압수하는 후, 디지털 데이터의 압수는 분석실에서 하는 것으로 판단된다.[62]

디지털 데이터를 압수의 대상으로 하면서 디지털 데이터에 대한 압수영장으로 매체자체를 압수하는 것이다. 매체 압수에 대한 과잉압수의 문제는 위법수집증거 배제 법칙과 Plain View 등 여러 예외의 문제로 논의되고 있다.

2. 사이버범죄방지조약

가. 사이버범죄방지조약

유럽평의회(the Council of Europe)는 1997년 4월 전문가회의[63]를 통해 사이버범죄에 관한 최초의 국제조약 제정을 위한 협의 결과 '사이버범죄방지조약 초안(Draft Convention on Cyber Crime)'을 작성하였다. 이 후 2001년 6월 22일 최종안을 작성하여, 2001년 11월 23일 컴퓨터 범죄에 관한 국제회의를 계기로 유럽회의 회원국 26개국과 비회원국 4개국 등 총 30개국이 가입하였다.[64] 2009년 5월 현재 통계에 따르면, 26개국이 비준을 마쳤고, 독일, 미국 등 많은 나라에서 발효되었고[65], 이는 최초의 사이버 범죄 관련 국제 조약이 되었다.

나. 사이버범죄방지조약의 내용

동 조약은 서문과 4장 48개조로 구성되어 있다. 각 장은 제1장 용어의 정의, 제2장 국내에서 취해야 할 조치, 제3장은 국제 협력, 제4장은 최종 규정으로 구성되어

62) "정보"를 압수의 대상인 물건에 정의하였음에도 압수의 방법에 대하여는 특별히 규제하고 있지 않다.
63) 유럽 형사문제위원회(European Committee on Crime Problems)가 1997년 2월 '사이버범죄에 관한 전문가회의(Committee of Experts on Crime in Cyber Space)'를 설치하였다.
64) 2001년 11월 23일에 동 조약에 가입한 국가는 그리스, 노르웨이, 네덜란드, 독일, 루마니아, 마케도니아, 몰도바, 불가리아, 벨기에, 스페인, 스위스, 스웨덴, 아르메니아, 알바니아, 영국, 오스트리아, 우크라이나, 이탈리아, 에스토니아, 크로아티아, 키프로스, 포르투갈, 폴란드, 프랑스, 핀란드, 헝가리 등 유럽의회 회원국 26개국과 캐나다, 일본, 남아프리카공화국, 미국 등 비회원국 4개국이다.
65) 대검찰청, "사이버범죄방지를 위한 국제공조방안 연구 - 유럽사이버범죄방지협약을 중심으로"(2009. 12.)

있는데, 특히 제2장 국내에서 취해야 할 조치의 경우 제1절 실체적 규정, 제2절 절차적 규정, 제3절 관할권에 관한 규정을 두고 있다. 동 장에 절차적 규정의 경우 사이버 범죄 뿐 만아니라, 디지털 포렌식 전반에 적용될 수 있는 절차라고 하겠다.

특히, 제19조 저장된 컴퓨터 자료의 압수·수색에서는 "법집행기관이 자신의 국가의 영토에 있는 컴퓨터 시스템 및 컴퓨터 데이터와 컴퓨터 데이터가 저장되어 있는 저장매체를 수색, 접속할 수 있도록 입법조치를 할"[66]것을 규정하고 있다. 그러면서 압수의 방법으로 컴퓨터 시스템 또는 그 일부 또는 컴퓨터 데이터 저장매체의 압수(혹은 그에 준하는 보전), 컴퓨터 데이터를 복사본을 만들고 보유하는 것, 사건과 관련된 저장된 컴퓨터 데이터의 무결성을 유지하는 것, 접근된 컴퓨터 시스템에서 해당 컴퓨터 데이터를 접근 불가능하게 하거나 삭제하는 권한을 가능하게 하도록 규정하고 있다.

3. 영국의 디지털 포렌식 현실

가. 입법례

영국의 경찰 및 형사증거법(The Police and Criminal Evidence Act 1984, PAC

66) Article 19 – Search and seizure of stored computer data
1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:
a a computer system or part of it and computer data stored therein; and
b a computer-data storage medium in which computer data may be stored in its territory.
2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.
3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:
a seize or similarly secure a computer system or part of it or a computer-data storage medium;
b make and retain a copy of those computer data;
c maintain the integrity of the relevant stored computer data;
d render inaccessible or remove those computer data in the accessed computer system.
4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.
5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

E)[67] 제19조는 제4항에서 '전자정보(information which is stored in any electronic form)'의 수집에 관한 조항을 두고 있다.[68]

제19조 제4항은 "경찰관은 자신이 수사한 범죄나 다른 범죄와 관련된 증거이거나, 범죄 실행의 결과물로 획득된 것이고, 이 정보의 은닉, 멸실, 변조 또는 파기를 방지하기 위하여 압수가 필요하다고 믿을 만한 합리적인 근거가 있는 경우에, 전자적 형태로 저장되고, 압수·수색 장소에 접근하여 가져 갈 수 있는 형태로 만들어질 수 있고, 가시적이거나 읽을 수 있는 형태로 용이하게 만들어질 수 있는 정보를 요구할 수 있다."고 규정하고 있다.

제20조는 "컴퓨터화된 정보에 대한 압수 권한 확대"라는 규정을 두고 있다. "이 섹션에 적용되는 법률에 의하여, 경찰에게 수여된 모든 압수·수색의 권한은 컴퓨터 내에 전자적 형태로 저장되어 있고, 압수 장소로부터 접근하여 가져 갈 수 있는 형태로 만들어질 수 있고, 가시적이거나 읽을 수 있는 형태로 용이하게 만들어질 수 있는 정보를 요구할 수 있다"고 규정하고 있다.[69]

위와 같이 영국은 정보를 압수의 대상으로 하는 명문의 규정이 있고, 디지털 증거의 압수에 대하여 가시화를 할 수 있는 형태로 요구할 수 있다고 규정하여, "해당 정보의 관리자에 대하여 출력, 복제, 저장매체 자체의 제출까지 요구할 수 있는 것"[70]처럼 보인다.

---

67) http://www.legislation.gov.uk/ukpga/1984/60/contents

68) General power of seizure etc.

(4)The constable may require any information which is stored in any electronic form and is accessible from the premises to be produced in a form in which it can be taken away and in which it is visible and legible or from which it can readily be produced in a visible and legible form if he has reasonable grounds for believing—

(a)that—

(i)it is evidence in relation to an offence which he is investigating or any other offence; or

(ii)it has been obtained in consequence of the commission of an offence; and

(b)that it is necessary to do so in order to prevent it being concealed, lost, tampered with or destroyed.

69) 20 Extension of powers of seizure to computerised information.

(1)Every power of seizure which is conferred by an enactment to which this section applies on a constable who has entered premises in the exercise of a power conferred by an enactment shall be construed as including a power to require any information stored in any electronic form contained in a computer and accessible from the premises to be produced in a form in which it can be taken away and in which it is visible and legible or from which it can readily be produced in a visible and legible form.

70) 이숙연, "디지털증거의 압수수색", 형사법 실무연구(2011), 제648쪽.

나. 영국의 디지털 포렌식 절차

영국은 The Association of Chief Police Officers (ACPO)에서 “Good Practice Guide for Computer Based Electronic Evidence”라는 가이드를 제정하여 디지털 증거에 관한 절차에 적용하고 있다.

위 가이드는 디지털 포렌식 절차에 대하여 계획(Plan) → 수집(Capture) → 분석(Analysis) → 제출(Present)의 순으로 이루어진다.

4. 독일의 디지털 포렌식 현실

가. 입법례

독일의 경우 형사소송법 제94조[71]에 압수의 대상을 “물체”(gegenstände)로 규정하고 있고, 디지털 데이터에 대한 별다른 규정은 없다. 그러나 독일 연방헌법재판소는 서버제공자의 메일 서버에 저장된 이메일은 압수의 재상이 될 수 있다고 결정하였다. 독일 형사소송법 제94조의 물건·대상이라고 표현한 것은 원래는 유형적 대상을 전제한 것을 의미하지만, 무형적 대상도 침해의 대상이 된다고 하면서, 동조의 물건·대상은 수사에 의미가 있는 모든 대상을 의미한다는 것을 그 근거로 하였다.

나. 독일의 디지털 포렌식 절차

디지털 정보에 대한 수색에 대한 규정은 있다. 형사소송법 제110조 제3항은 “③수색대상인 자의 전자 저장매체에 대한 수색은 수색대상인 데이터가 상실될 우려가 있다면 저장매체로부터 도달될 수 있는 한, 당해 저장매체와 공간적으로 분리되어 있는 저장매체들에까지 확대될 수 있다. 조사에 중요한 의미가 있을 수 있는 데이터는 이를 압수할 수 있다.”[72]고 규정하였다.

---

71) Strafprozeßordnung (StPO) § 94
(1) Gegenstände, die als Beweismittel für die Untersuchung von Bedeutung sein können, sind in Verwahrung zu nehmen oder in anderer Weise sicherzustellen.
(2) Befinden sich die Gegenstände in dem Gewahrsam einer Person und werden sie nicht freiwillig herausgegeben, so bedarf es der Beschlagnahme.
(3) Die Absätze 1 und 2 gelten auch für Führerscheine, die der Einziehung unterliegen.
72) Strafprozeßordnung (StPO) § 110
(3) Die Durchsicht eines elektronischen Speichermediums bei dem von der Durchsuchung Betroffenen

그리고 형사소송법 제98조a~c는 중대한 범죄에 대한 데이터 검색에 대한 규정을 도입하여, 열거된 중대한 범죄를 범하였다는 충분한 근거가 있을 경우, 데이터에 대한 비교 조사를 하여 혐의자를 추적하는 조사를 할 수 있도록 규정하고 있다.[73]

5. 소결

디지털 포렌식 관련 기관은 직접 디지털 포렌식 업무를 지원하는 기관, 연구 개발을 하는 연구소 및 디지털 포렌식 수사관을 교육하는 교육기관의 형태로 되어 있다. 미국의 경우 여러 개의 조직으로 되어 있고, 네덜란드의 경우는 NFI로 통합되어 디지털 포렌식 지원 및 연구개발, 교육을 하고 있다.

대부분의 국가에서 디지털 데이터를 압수의 대상으로 규정하고 있고, 디지털 포렌식 절차는 정보저장매체 자체를 압수하는 것을 전제로 하고 있고, 피압수자의 기본권 보호를 위한 별다른 조치가 없는 것을 보면, 수사의 목적 달성을 중심으로 규정되어 있음을 볼 수 있다.

---

darf auch auf hiervon räumlich getrennte Speichermedien, soweit auf sie von dem Speichermedium aus zugegriffen werden kann, erstreckt werden, wenn andernfalls der Verlust der gesuchten Daten zu besorgen ist. Daten, die für die Untersuchung von Bedeutung sein können, dürfen gesichert werden; § 98 Abs. 2 gilt entsprechend.

73) 이숙연, "디지털증거의 압수수색", 형사법 실무연구(2011), 제649쪽.

제5장 우리나라 디지털 포렌식 현실

앞에서 각국의 디지털 포렌식 현실에 대하여 살펴보았다. 이에 비해 우리나라의 디지털 포렌식 현실은 어떠한지 디지털 포렌식 관련 기관과 디지털 포렌식 절차에 대하여 알아보겠다.

제1절 디지털 포렌식 관련 기관

우리나라의 디지털 포렌식 관련 기관은 수사기관을 제외하고는 많지 않는 현실이고, 수사기관의 경우에도 각자의 필요에 따라 운영하고 있을 뿐, 서로의 정보 교류도 많지 않다.

1. 대검찰청 디지털수사과

체계적인 디지털수사지원체계의 구축 필요성을 인식하고 매년 폭증하고 있는 압수·수색 및 증거분석 업무를 효율적으로 지원하기 위하여 2005년 대검찰청 기획조정부에서 차장검사 직속으로 직제를 개편하여 '과학수사제2담당관실'을 신설하였다. 이듬 해 담당관실의 정원을 확대, 2007년 '디지털수사담당관실'로 명칭을 변경하고, 그 해 서울중앙지방검찰청에 디지털포렌식수사팀을 신설하였다. 2008년 10월 현재 국가디지털포렌식센터(NDFC)의 전신인 디지털포렌식센터(DFC)를 개소하였으며, 2007년 부산고검, 2009년 대구고검, 2010년 광주고검, 대전고검, 2011년 인천지검, 2012년 수원지검, 2014년 서울고검, 서울남부지검, 창원지검에 이르기까지 전국에 디지털포렌식수사팀을 확대 설치하였다. 2015년 2월에는 체계적인 과학수사 토대를 마련하여 장기적 관점에서 과학수사 정책 수립하고 효율적으로 운용할 조직을 구성하기 위해 종전 3개 담당관(과학수사담당관, 디지털수사담당관, DNA수사담당관) 체제로 운영되던 과학수사기획관실을 1기획관(과학수사기획관), 4개과(과학수사1과, 과학수사2과, 디지털수사과, 사이버수사과)의 '과학수사부'로 승격하였다.

2. 경찰청 사이버 안전국

경찰의 디지털 포렌식팀은 2004년 10월 사이버테러대응센터 기술지원팀에서부터 시작되었다. 2008년 2월 사이버테러대응센터 디지털증거분석센터로 명칭이 변경되었고, 2010년 2월에 사이버테러대응센터 디지털포렌식팀으로 변경되었다.[74] 그 후 사이버안전국이 2014년 6월 신설되면서 사이버안전국 디지털포렌식센터로 되면서 현재의 조직을 갖추게 되었다.[75] 지방경찰의 경우 2011년 7월 사이버수사대내에 디지털증거분석실이 신설되었다. 사이버 수사 인력은 2012년 현재 944명에 이르나, 조직의 대부분이 사이버 범죄 관련 인력이고, 디지털 포렌식을 하는 전담인력은 40명에 불과하여[76], 디지털 포렌식을 전담하고 있는 인력은 매우 부족한 현실이다.

3. 기타 수사기관

국가정보원, 기무사, 관세청, 저작권위원회 등 각 기관의 필요에 따라 디지털 포렌식관련 부서를 두고 있으나, 인력 부족과 예산 부족으로 별도의 연구 개발이나 교육은 어려운 실정이다.

제2절 디지털 포렌식 절차

1. 디지털 포렌식 절차

가. 경찰

경찰은 2006년 12월 "디지털증거처리 표준가이드라인"을 수립하여 절차의 표준을 마련하였다. 이는 사전준비(Preparation), 증거수집(Collection), 조사(Examination), 분석의뢰, 접수, 운반(Evidence Request, Receipt & Transport), 증거분석(Analysis), 결과보고서(Reporting), 보존 및 증거관리(Preservation & Evidence Management) 등 7개의 절차로 이루어졌다.

---

74) 송봉규, 장석헌, "경찰의 디지털 포렌식 실태와 개선방안", 한국경찰연구 제12권 제2호(2013), 제124쪽.

75) http://cyberbureau.police.go.kr/bureau/sub4.jsp?mid=040401, 디지털포렌식센터는 포렌식기획팀, 첨단기법개발팀, 모바일포렌식팀, 컴퓨터포렌식팀으로 구성된다.

76) 송봉규, 장석헌, "경찰의 디지털 포렌식 실태와 개선방안", 한국경찰연구 제12권 제2호(2013),제131쪽. 경찰청 17명, 17개 지방경찰청 23명으로 이들이 전체 분석한 건수는 6,247건으로 1인당 연간 분석 매체 수는 156건에 이른다.

나. 검찰

검찰의 경우 디지털 포렌식에 대한 별도의 가이드라인이나 모델을 제시하지는 않고, "디지털 증거 수집 및 분석 규정"[77]이라는 내부 규정으로 디지털 포렌식 절차를 처리하고 있다. 위 규정은 사전준비, 압수·수색, 정보저장매체 운반, 분석, 분석결과보고서 작성의 절차로 되어 있다.

2. 형사소송법 개정 전의 디지털 포렌식에 대한 법원의 태도

형사소송법에 디지털 데이터에 대한 압수에 대한 규정이 없었던 때에는 법원의 태도에 의하여 디지털 포렌식의 절차와 증거능력이 결정되었다. 특히 위법수집증거배제원칙에 의하여 위법하게 수집된 디지털 증거에 대한 증거능력이 상실됨에 따라, 디지털 데이터 압수에 대한 절차 준수 및 증거능력 인정 여부가 더욱 중요하게 되었다.

가. 전교조 압수·수색 준항고 기각 결정에 대한 재항고 결정(대법원 2011. 5. 26.자 2009모1190결정)

전교조사건 압수·수색 재항고 결정을 통하여 디지털 데이터 압수 절차에 대한 법원의 입장이 정립되었다. 위 결정에서 원칙적으로 혐의사실과 관련된 부분만 출력, 복사하는 방법으로 압수·수색 영장을 집행하여야 하며, 예외적인 사정이 있을 경우에 한하여 저장매체 자체를 이미징하거나, 수사기관의 사무실 등 외부로 반출할 수 있다고 하였다.

그리고 예외적으로 수사기관 사무실 등으로 옮긴 후의 과정도 전체적으로 보아 압수·수색 영장 집행의 일환에 포함된다고 하였고, 그에 따라 전체 과정을 통하여 피압수·수색 당사자나 변호인의 계속적인 참여권 보장 등 압수·수색 대상인 저장매체 내 전자정보의 왜곡이나 훼손과 오·남용 및 임의적인 복제나 복사 등을 막기 위한 적절한 조치가 이루어져야만 집행절차가 적법하게 된다고 하였다.

---

77) 대검 예규 제616호 "디지털 증거 수집 및 분석 규정"

나. 압수·수색 영장 별지

법원은 위 결정이후 압수·수색영장을 발부하면서 "압수방법의 제한"이라는 명칭의 별지[78]를 추가하여 디지털 데이터의 압수 방법을 제한하는 압수·수색영장을 발부하였다. 압수 방법에 대하여 특히 원칙적으로 '혐의사실과 관련된 전자정보만을 문서로 출력하거나 수사기관이 휴대한 저장매체에 복사하는 방법으로 압수할 수 있'고, 예외적으로 '출력·복사에 의한 집행이 불가능하거나, 압수의 목적을 달성하기에 현저히 곤란한 경우에 한하여 저장매체 전부를 복제할 수 있'으며[79], '집행현장에서의 저장매체의 복제가 불가능하거나 현저히 곤란한 때에 한하여 피압수자 등의 참여 하에 저장매체 원본을 봉인하여 저장 매체의 소재지 이외의 장소로 반출할 수 있'다[80]고 하고 있다.

그리고 "압수·수색의 전체 과정을 통하여 피압수자 등의 참여권이 보장되어야 하며, 참여를 거부하는 경우에는 신뢰성과 전문성을 담보할 수 있는 상당한 방법으로 압수·수색이 이루어져야"한다고 하여 피압수자 등의 참여권에 대한 언급이 있다.

3. 형사소송법 개정

디지털 증거에 대한 압수·수색 절차와 증거능력 등 형사소송법상 명확한 규정이 없고 몇몇 사건의 법원의 태도도 학계나 수사기관의 반대 입장이 커 논란이 일어나게 되었다.

이렇듯 디지털 증거 관련 규정의 제정 필요성에 따라 2011. 6. 국회 사법제도개선특별위원회는 디지털 데이터 압수 관련된 형사소송법 개정안을 통과시켰고, 이는 2011. 7. 18. 공포되었고, 2012. 1. 1.부터 시행되고 있다.

개정 형사소송법은 제106조 제1항에 '관련성' 요건[81]을 추가하여 압수·수색의 요

78) 압수·수색영장의 별지는 형사소송법 개정 이후에도 내용이 크게 바뀌지 않은 형태로 영장에 첨부하여 발부하는 경우가 있다. 아래의 별지 내용은 이숙연, "전자정보에 대한 압수수색과 기본권, 그리고 영장주의에 관하여", 헌법학 연구 제18권 제1호(2012), 제32-33쪽의 내용이다.

79) 전부 복제할 수 있는 예외적인 상황으로는 1. 피압수자 등이 협조하지 않거나, 협조를 기대할 수 없는 경우 2. 혐의사실과 관련된 개연성이 있는 전자정보가 삭제, 폐기된 정황이 발견된 경우 3. 출력복사에 의한 집행이 피압수자 등의 영업활동이나 사생활의 평온을 침해하는 경우 4. 기타 이에 준하는 경우를 말한다.

80) 저장매체 소재지 이외의 장소로 반출할 수 있는 예외적인 상황으로는 1. 집행현장에서의 하드카피·이미징이 물리적, 기술적으로 불가능하거나 극히 곤란한 경우 2. 하드카피·이미징에 의한 집행이 피압수자 등의 영업활동이나 사생활의 평온을 현저히 침해하는 경우 3. 기타 이에 준하는 경우를 말한다.

건을 강화하고, 제106조 제3항에 정보저장매체 등이 압수의 목적물인 경우 압수의 방법과 범위를 명시하였고, 동조 제4항에 제3자 보관 디지털 정보의 압수·수색시 정보주체에게 해당 사실을 알리도록 규정을 신설하였다.[82]

4. 검토

개정 형사소송법에 대하여 여전히 논란이 있다. 디지털 데이터가 압수의 대상이 되는지에 대하여 명확한 규정이 없기 때문이다. 그리고 제106조의 사건과의 관련성 요건 추가의 의미에 대하여 많은 논의가 되고 있다.

특히 개정 형사소송법 제106조 제3항[83]은 종래 압수·수색영장의 편철된 별지와 유사하게 입법화한 것으로 보이고, 법원도 개정 형사소송법의 시행 이후에 기존 전교조 압수·수색 준항고 기각결정에 대한 재항고 결정의 입장을 그대로 취하고 있다. 개정된 형사소송법이 법원의 태도와 같다고 판단하여 새로운 입장을 취하지 않은 것으로 보이나, 이에 대하여는 후술하겠다.

제3절 현재 수사기관에서의 디지털 포렌식 절차

앞에서 보았듯이 우리 형사소송법은 디지털 데이터의 압수방법에 대하여 출력, 복제의 원칙, 저장매체 압수의 예외를 규정하고 있는바, 이는 다른 나라의 입법례에는 찾아보기 어려운 규정이다. 이와 같은 형사소송법의 개정으로 기존의 수사기관의 디지털 데이터 압수 절차는 큰 변화를 겪게 되었다.

기존에는 현장에서 정보저장매체 자체를 압수하여 수사기관의 사무실에 가져와 전체에 대하여 이미징을 한 다음, 이 이미지 파일을 분석하고 결과를 보고하는 절

---

81) 제106조(압수) ① 법원은 필요한 때에는 **피고사건과 관계가 있다고 인정할 수 있는 것에 한정**하여 증거물 또는 몰수할 것으로 사료하는 물건을 압수할 수 있다. 단, 법률에 다른 규정이 있는 때에는 예외로 한다.

82) 2011. 7. 18.자 개정으로 디지털 증거 관련 규정은 위의 제106조 제3항, 제4항을 비롯하여, 전자 우편의 압수의 경우를 규정한 제107조, 전기 통신의 경우 압수·수색 영장 기재 사항을 규정한 제114조, 수사기관의 압수·수색검증의 규정인 제215조 등 이다.

83) 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.

차로 이루어 졌으나, 현재는 형사소송법에 따라 압수·수색 현장에서 사건과 관련된 디지털 데이터를 출력, 복제하는 것을 원칙으로 하고 있다. 이는 인적, 물적 여건이 열악할 수밖에 없는 압수·수색 현장에서 디지털 데이터의 압수를 하여야 한다는 것과 더불어 삭제된 파일의 복원을 할 수 없게 되어 압수의 목적을 달성하기 어렵게 되어 국내 디지털 포렌식 수사의 위기를 맞이하게 되었다.

제4절 디지털수사망(Digital Investigation Network, D-NET)

정보저장매체의 대용량화와 가격 하락, 디지털 기기의 사용 급증에 따른 디지털 데이터의 초대용량화도 수사기관의 디지털 데이터 압수에 대하여 큰 영향을 미치게 되었다. 과거 압수한 디지털 데이터의 경우 담당 디지털 포렌식 수사관의 PC에서 간단하게 분석이 가능하였고, 이를 당해 사건을 담당하는 검사나 수사관도 자신의 PC에서 위 분석 결과를 확인할 수 있었다. 그러나 디지털 데이터의 용량의 급증과 여러 안티 포렌식 기법의 등장으로 인하여 기존의 PC상의 분석과 확인이 어려워지는 상황이 발생하면서, 디지털 포렌식 분야에 있어서 분석과 확인을 위한 시스템의 도입이 필요해지게 되었다. 이에 대검찰청은 2009년 디지털 수사망(Digital Investigation Network, DNET)을 계획하여 2012년 서비스를 개시하면서 디지털 포렌식 절차에서 본격적으로 시스템을 사용하기에 이르렀다.

1. 디지털 포렌식 관련 시스템 구축 필요성

디지털 데이터가 범죄의 증거로 사용되는 경우가 폭증하면서, 이와 관련된 업무량은 급증하였고, 업무의 복잡성도 증가하였다. 특히 디지털 압수물의 양이 지나치게 방대해져 PC만으로 분석하고 분석 결과를 확인하는 과정에서 PC가 다운되는 현상이 발생하였다. 이는 디지털 압수물의 훼손 우려가 큰 심각한 문제였다. 그리고 사용하는 디지털 기기와 파일 형식의 다양화로 이를 분석한 결과를 사람이 일일이 확인 대조하는 것은 엄청난 시간이 걸리게 되었고, 정확도도 보장하기 어렵게 되어, 이를 통합적으로 확인, 조사할 수 있는 방법을 모색하기에 이르렀다.

이에 대검찰청은 대용량 디지털 데이터 처리를 위한 인프라와 방대한 디지털 데

이터 분석을 위한 수사도구, 디지털증거의 증거능력 확보를 위하여 증거 데이터의 항목을 유지하고 보관할 수 있도록 관리하고 지원하는 정보시스템의 구축 계획을 세우게 되었다.

2. 디지털수사망 구축

물론 전국디지털수사망(D-NET) 이전에도 디지털포렌식수사정보지원시스템(이하 DFIS[84]), IQS[85], Tracer[86], ACORA[87], 체이서[88]와 같은 업무지원, 증거관리, 분석요청, 증거검색을 지원해주는 시스템과 프로그램은 존재하였다. 그러나 이러한 시스템과 프로그램들은 폭발하는 업무량을 해소하기 위하여 단기적 관점에서 구축, 개발하여 여러 가지 문제점이 있었다.

이에 현장중심의 디지털수사지원체계 구축과 디지털 증거 분석 품질 향상, 디지털 수사 조직 인력의 확대, 디지털 수사 프로세스 개선을 통한 "신속·정확한 디지털수사 지원체계"를 마련하기 위한 계획을 수립하였고, 그 일환으로 2010년부터 본격적으로 시스템 구축에 들어가 2012년 완료하였다.

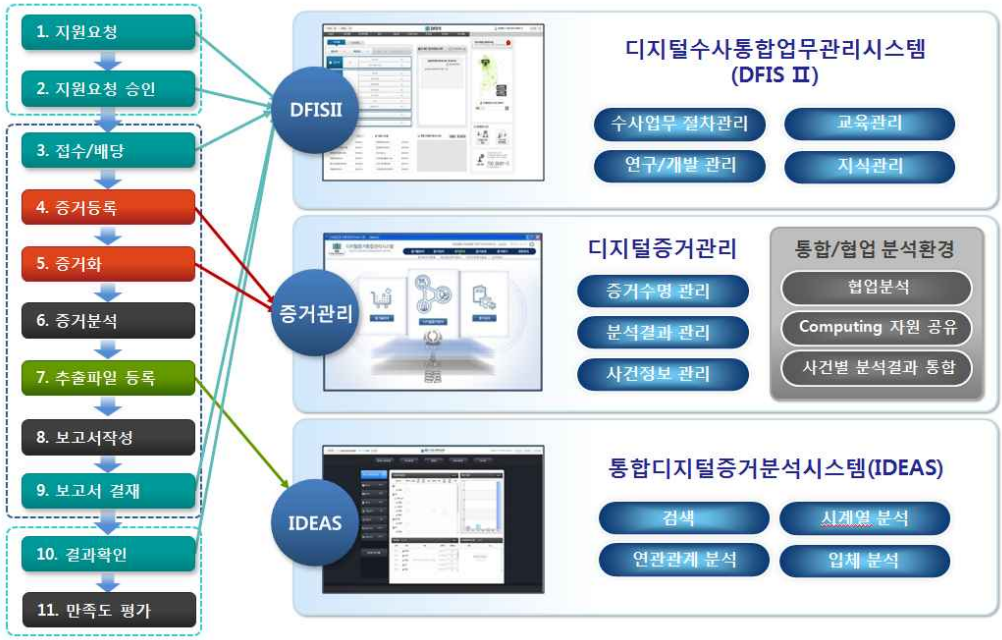
3. 디지털수사망 개요

디지털수사망은 디지털데이터의 압수, 분석, 결과 확인을 할 수 있는 디지털수사통합업무관리시스템(DFIS II), 디지털 증거를 보관하고 관리하는 증거관리시스템, 직접 수사를 하는 검사, 수사관(이하 '수사팀'이라 함)이 디지털 증거에 대하여 직접 분석할 수 있는 통합디지털 증거분석시스템(Integrated Digital Evidence Analysis System, IDEAS)으로 구성되어 있다.

디지털 데이터 압수, 분석에 대하여 사건 관련 정보를 수동으로 입력하는 등 체계적인 관리가 미흡하고, 지원에 있어 여러 번의 공문 수발을 거쳐야 하는 번거로움

84) DFIS(Digital Forensic Information System) : 디지털수사망 구축 이전의 검찰에서 사용하던 디지털 포렌식 관련 행정시스템
85) IQS: Investigation Query System(수사질의어 프로그램)으로 대검찰청이 자체 개발한 소프트웨어
86) 통화내역 분석 프로그램으로 대검찰청이 자체 개발한 소프트웨어
87) 계좌내역 분석 프로그램으로 대검찰청이 자체 개발한 소프트웨어
88) 물리이미징 및 증거보관 시스템

이 있어 업무관리시스템(DFIS II)을 구축하였다.



[그림1] 디지털수사망의 구성

그리고 하나의 사건에 대하여 여러 명의 디지털 포렌식 수사관이 지원한 경우, 각자의 PC에 분석 결과물을 관리하고 있어 수사팀에서 종합적으로 디지털 압수물을 확인하기가 어렵고, 디지털 압수물에 대한 보관 체계가 없어 효율적인 증거 관리가 어렵고, 디지털 압수물에 대한 접근·권한 관리가 되고 있지 않으며, 대용량화된 디지털 압수물의 관리 체계가 미비하여 디지털증거관리시스템을 구축하였다.

한편, 디지털 압수물 분석에 소요되는 시간의 단축이 필요하고, 하나의 사건에 여러 명의 디지털 포렌식 수사관이 디지털 압수물을 분석한 경우 이를 하나로 통합하여 분석하기 어려운 점이 있고, 이종(異種)의 다양한 형태의 디지털 압수물에 대한 통합적 분석이 필요하고, 디지털 압수물의 대용량화로 기존의 어플리케이션으로 하던 색인, 검색 시스템의 한계와 외장하드, DVD 등 수사팀에 오프라인으로 디지털 데이터를 전달하던 실무의 개선이 필요하고, 사건 유형별 검색 키워드 축척이 불가능하고, 분석방식에 있어서도 일차원적인 분석에 그쳐 디지털 압수물의 분석효과도 저조한 문제점의 개선이 필요하고, Stand-alone 방식의 개인 단독 수사가 주로 이루어지면서 수사관 개인 역량에 따른 분석과 보고로 인해 증거분석의 비표준화라는

문제점을 개선할 필요가 있게 되었다. 그래서 사건의 내용을 정확하게 알고 있는 수사팀에서 디지털 압수물을 직접 검색하여 유기적으로 분석함으로서, 수사의 효율성을 높일 필요성이 있어 일선 수사팀에서 디지털 포렌식 수사관이 분석한 디지털 압수물에 대하여 통합적으로 접근할 수 있는 시스템(통합디지털증거분석시스템, IDEAS)을 구축하기에 이르렀다.

4. 각 시스템의 구체적 내용

가. DFIS II

DFIS II는 디지털 포렌식의 프로세스를 정립하고, 각 단계마다 필요한 정보를 관리하며, 디지털 포렌식 수사관이 사용하는 내부 시스템과 일선 수사팀이 사용하는 외부 시스템의 연계를 통해 데이터를 확보한다. '디지털 수사 지원 요청', '현황 조회', '각종 결재', '통계관리', '게시판' 등 디지털 포렌식 관련 모든 업무를 진행할 수 있도록 업무 포털로서 기능을 한다.

디지털 포렌식 수사관과 일선 수사팀의 화면 구성을 달리하여, 각자 역할에 맞게 시스템을 고안하였다.

[그림2] 디지털수사망 초기화면

[그림3] 디지털수사통합업무관리시스템 일선 수사팀 화면

나. 디지털증거관리시스템

디지털증거관리시스템은 디지털 압수물의 생명주기 (Life-cycle) 전체를 관리하고 디지털 압수물과 관련 자료를 사건 별로 관리하고 있다. 메타 데이터를 이용하여 사건 또는 정보저장매체별 디지털 증거의 조회 및 관리의 효율성을 증대시키고, 분석절차정보의 등록으로 Chain of Custody 확보와 사건 단위 관리가 용이해졌다.

별도의 폐쇄망인 초고속 국가망을 이용하여, 각 지역 디지털 포렌식 팀과 대검 디지털수사과를 연결하여 압수된 모든 디지털 압수물을 대검에서 물리적으로 관리할 수 있도록 하여 증거의 안전성과 효율성을 제고하였다.

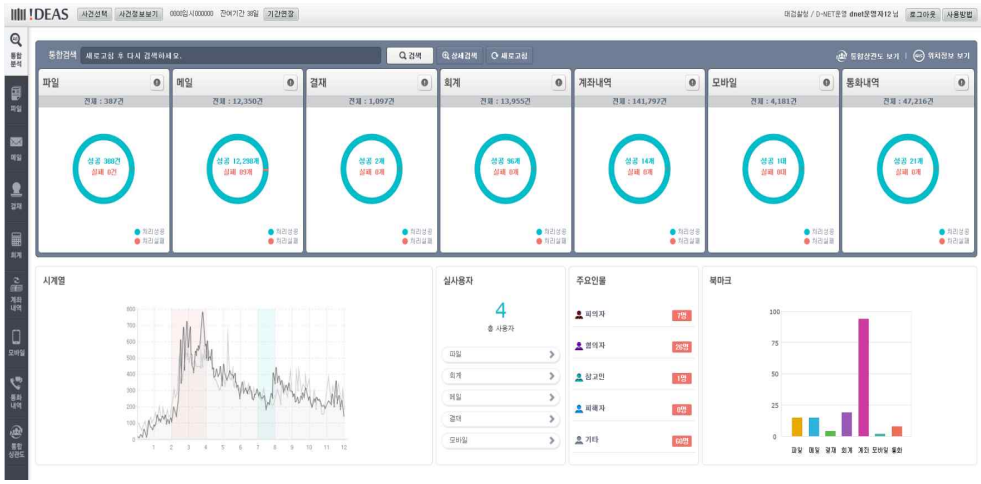
구체적으로 사건단위 통합 정보 저장 기능은 이미지 파일, 채증정보, 분석된 이미지 파일, 분석 결과, 분석 보고서 등을 사건 별로 저장하고, 디지털 압수물을 조회할 수 있도록 한다. 디지털 압수물의 생명주기 관리 기능은 스토리지의 효율적인 구성 및 아카이빙 체계를 구현하고 장기보관 매체에 대한 현황 조회와 제 기록 수행 등 주기적 관리를 통해 디지털증거의 안정적 보관 기능을 수행한다. 그 외에 DFIS 사용자의 권한 정보를 연계, 조회하여 디지털 압수물에 대한 접근 권한을 관리하는 기능을 수행한다. 특히 사건 단위로 디지털 압수물에 대한 디지털 포렌식 수사관 및 수사팀의 접근 권한을 설정하여, 무자격자의 접근 및 변경을 차단을 통해 디지털 압수물의 안정성 및 보안을 강화하고, 디지털 압수물의 접근이력을 관리

하여, 디지털 압수물의 흐름 및 이전, 변경 기록의 추적이 가능하게 되었다.

다. 통합디지털증거분석시스템(IDEAS)

IDEAS는 일선 수사팀이 디지털 포렌식 수사관이 수행한 디지털 압수물 분석 결과를 2단계에 걸쳐 단계별로, SBC(Server Based Computing)와 GPKI 인증을 통해 안전하게 제공한다.

IDEAS는 디지털 압수물의 분석 결과를 사건단위로 통합조회 하거나 분석하는 것을 가능하게 하고, 온라인을 통해 신속하게 분석결과를 전달할 뿐만 아니라, 사건을 잘 알고 있는 일선 수사팀이 디지털 증거를 시계열분석, 인물관계분석, 체인키워드, 특수정보 등 입체적인 추가 분석이 가능하게 한다.



[그림4] IDEAS 통합검색 초기화면

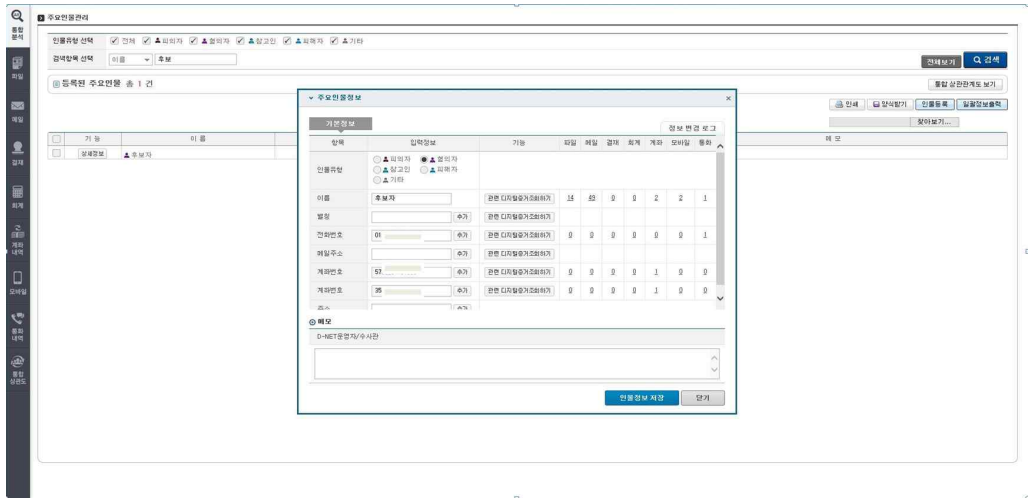
파일, 이메일, 결재, 회계, 모바일, 계좌내역, 통화내역 등 이종의 디지털 증거에 대하여 각각 또는 통합적으로 검색어를 입력하여 검색할 수 있고, 시계열 분석으로 시간에 따라 각 디지털 압수물을 확인할 수 있으며, '체인키워드 및 특수정보 분석'은 사용자가 특정 단어를 연결 검색함으로 결과의 정확성을 높이고, 숫자와 연관된 일정 패턴을 가진 정보를 특수정보로 별도로 관리하여 수사팀이 확인하기에 용이하게 하였으며, '북마크 및 증거분류'는 증거파일, 핵심내용, 메모 등을 북마크 하여 재색인 가능하며, 제공파일을 형태별로 분리하여 파일을 체계적으로 시각화할 수

있다.

또한 기존에 디지털 압수물의 분석 결과를 오프라인으로 DVD 형태로 전달했던 기존의 방식에서 벗어나 사건단위로 정보를 통합하여 온라인으로 다운로드 받을 수 있도록 하여 증거로 제출하기에 용이하게 하였다.

(1) 주요인물 등록

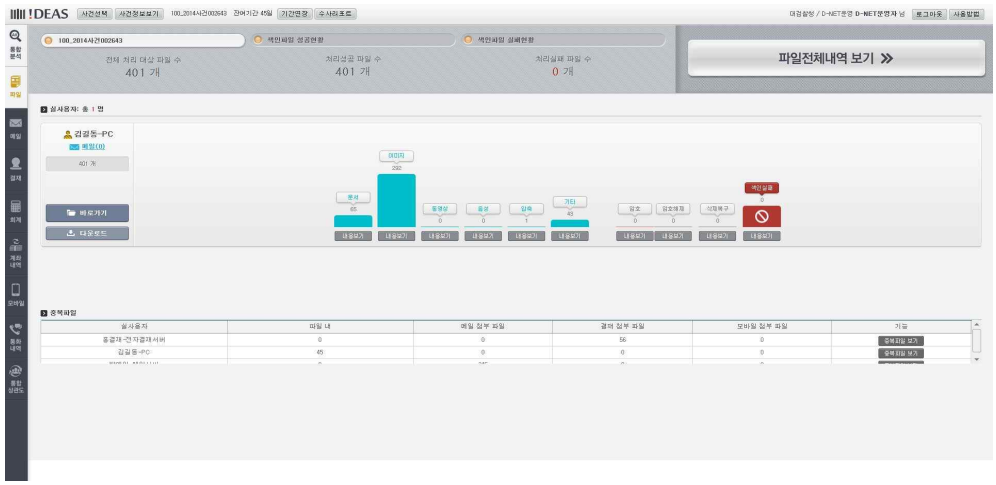
피의자, 참고인 등 사건과 관련된 '주요인물'을 등록하여 인물 중심으로 디지털 압수물을 분석하게 된다.



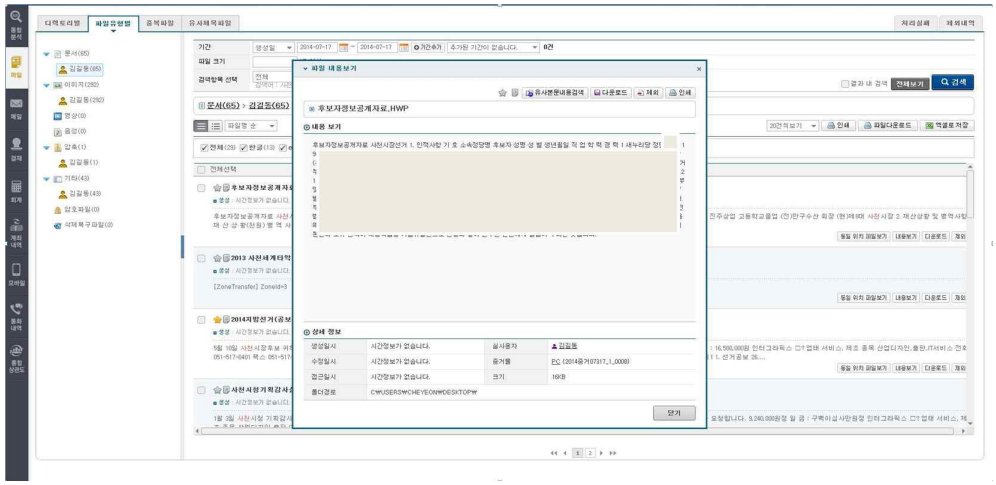
[그림5] 주요인물 등록 화면

(2) 파일 분석 등 동종의 디지털 압수물 분석

파일, 이메일, 결재, 회계, 모바일, 계좌내역, 통화내역 등의 디지털 압수물을 검색하고, 분석할 수 있다. 키워드 검색을 이용하여 원하는 디지털 압수물을 찾을 수 있고, 디지털 압수물을 타임라인 별로 나열하여 보거나, 같은 파일이나 비슷한 파일을 걸러내 분석에 편의성을 더하였다.



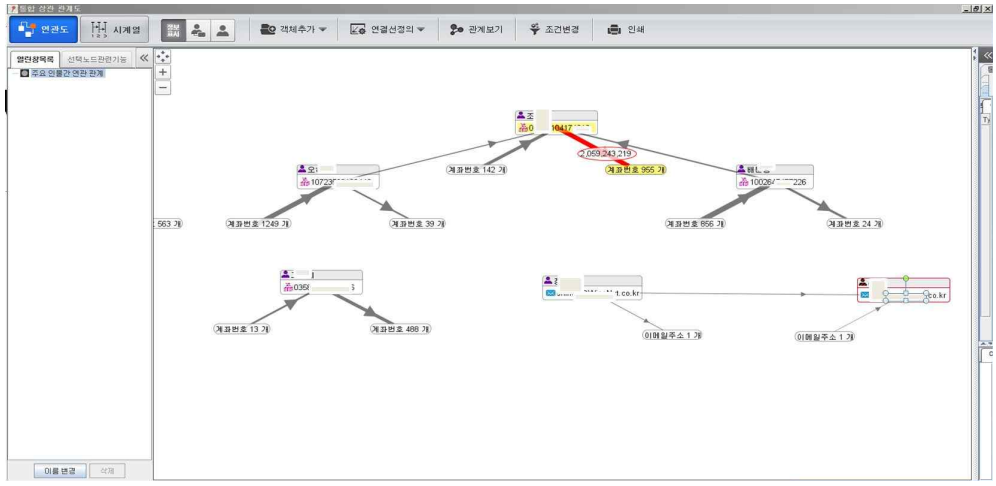
[그림6] 파일 분석 초기화면



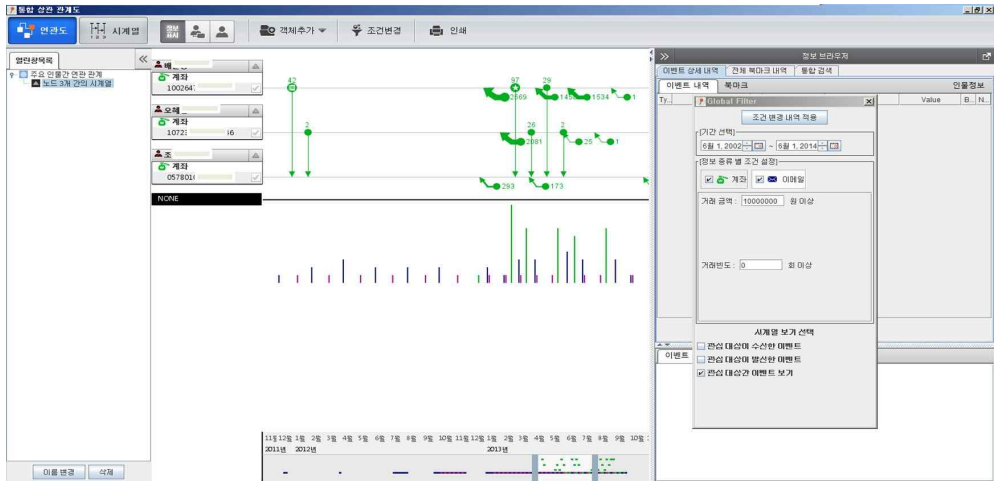
[그림7] 파일 분석 화면

(3) 통합상관도

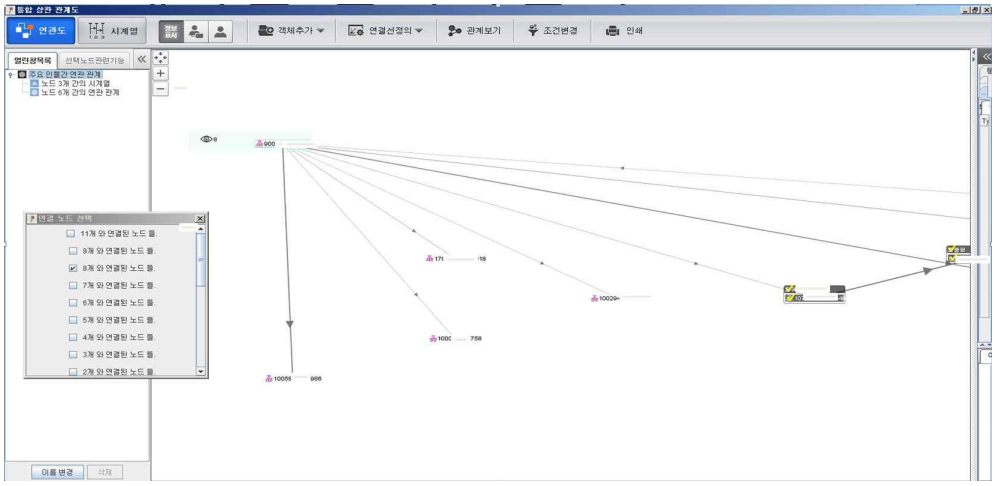
이메일, 통화내역, 계좌내역 등 관계적 속성이 중요한 디지털 압수물은 '통합상관도'로 표현하여 분석이 쉽도록 하였다.



[그림8] 통합상관도 1



[그림9] 통합상관도 2



[그림10] 통합상관도 3

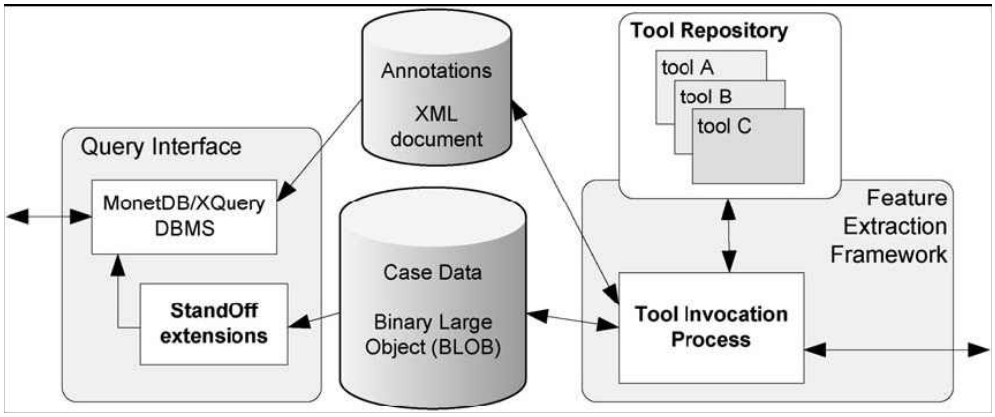
5. NFI의 XIRAF[89]

가. 개요

XIRAF는 네덜란드 NFI에서 개발한 디지털 포렌식 분석 시스템으로 디지털 데이터에서 사건과 관련된 많은 '흔적'을 확인하고, 수사관이 직관적이고 효과적으로 흔적을 검색할 수 있도록 한다. 또한 각 기관이 온라인 포렌식 서비스로 독자적인 시스템을 갖추어 운영할 수 있다.

하드 디스크, 휴대폰, USB 등 많은 디지털 증거가 저장된 디지털 기기에서 파일과 문서, 이메일, 채팅 로그, 브라우저 기록, 통화 기록, 위치 정보 등의 흔적을 자동적으로 수집한다. 이러한 흔적을 찾기 위해서는 방대하고 자세한 기술적인 지식을 습득하고 있어야 하지만, 수사관이 어디에서 어떻게 찾는지 걱정할 필요 없이 사건과 관련된 흔적을 자동으로 수집하고 흔적들을 구성할 수 있도록 하였다.

89) NFI, "XIRAF_Online Advanced Forensic Analysis"(2012)



[표13] XIRAF framework architecture[90]

나. XIRAF의 특징

일단 XIRAF가 수집한 디지털 흔적은 XIRAF에 내장된 검색 엔진으로 검색할 수 있다. 키워드 쿼리를 통해 시간 범위 선택 및 다른 많은 필터로 수사관은 빠르게 관심 있는 흔적을 중점적으로 볼 수 있다. 검색 결과는 타임 라인, 이미지 갤러리나 지도 등 많은 유용한 방법으로 표시된다. 선택한 파일의 복사본의 위치를 찾거나, 이메일에 같은 이름의 파일이 첨부되었는지를 알 수 있어 관련된 흔적의 연계 중에서 각각의 흔적을 표시할 수 있는 브라우저를 제공한다. 다중 사용자 시스템으로 관리자가 사용자가 접속할 수 있는 사건을 결정하고, 다중 사용자는 동시에 XIRAF를 사용하고 쿼리 및 메모를 공유할 수 있으며, 정보는 어디서나 사건 별로 공유될 수 있도록 하였다. 형사, 컴퓨터 포렌식 수사관 및 분석관 등 디지털 추적의 기본적인 지식이 있는 사람이라면 누구나 사용할 수 있다. XIRAF로 수사관에게 디지털 포렌식 서비스를 온라인으로 제공하므로, 웹 브라우저를 이용하고, 서비스 자체는 기관의 망 내에서 실행할 수 있다. 또한 안전한 인터넷 연결을 통하여 어떠한 지역에도 서비스를 제공할 수 있고, 현장 분석용 모바일 솔루션 사용할 수 있다. 그리고 XIRAF는 오픈 시스템으로, XIRAF의 프로그램 인터페이스가 다른 시스템이나 분석 프로그램에 쿼리를 보내고, 결과를 공급하는 방법으로 사용할 수 있다.

90) W. Alink, R.A.F. Bhoedjang, P.A. Boncz, A.P. de Vries, "XIRAF -- XML-based indexing and querying for digital forensics", DFRWS, digital investigation(2006)

다. 검토

XIRAF는 검찰의 IDEAS와 유사한 기능을 가지고 있다. 위에서 소개된 XIRAF의 특징은 IDEAS와 거의 동일하다고 하겠다. 대용량·이종의 디지털 압수물을 단순히 디지털 포렌식 수사관 혼자서 PC로 분석하는 시기를 넘어, 다수의 수사관이 협업과 고성능의 시스템을 이용하여 통합적으로 분석할 수밖에 없는 시대적 요구에 의하여 우리나라 검찰뿐만 아니라, 네덜란드의 NFI도 이러한 시스템을 설계한 것이다.

제6장 검찰의 디지털 포렌식 절차

검찰의 디지털 데이터에 관한 압수·수색은 검찰 예규인 디지털 증거 수집 및 분석 규정과 이를 바탕으로 구축된 디지털수사망을 이용하여, 원칙적으로 ① 압수·수색 준비 → ② 압수·수색 현장에서 정보저장매체 수색 → ③ 정보저장매체에서 사건과 관련된 디지털 데이터 조사 → ④ 사건관련 파일 복제, 목록 작성 교부, 확인서 → ⑤ 디지털 압수물 업로드, (분석), 색인 → ⑥ 일선 수사부서에서의 검색, 출력, 복제 → ⑦ 사건 종료 후 디지털 압수물의 처리의 절차로 진행된다.

한편, 예외적으로 압수·수색 현장에서 사건과 관련된 디지털 데이터를 출력, 복제할 수 없는 경우에는 현장에서 정보저장매체에 저장되어 있는 디지털 데이터 전체를 복제하는 방법과 정보저장매체 자체를 압수하는 방법으로 나누어진다.

전자의 경우 ① 압수·수색 준비 → ② 압수·수색 현장에서 정보저장매체 수색 → ③ 정보저장매체에서 사건과 관련된 디지털 데이터 조사 → ④ 이미지 파일, 복제본 디스크의 생성 → ⑤ 정보저장매체 전부 복제, 이미징 확인서 작성 → ⑥ 디지털 압수물 시스템에 업로드 → ⑦ 업로드한 디지털 압수물 다운로드 받아 분석 → ⑧ 분석한 디지털 압수물 업로드, 색인 → ⑨ 일선 수사부서에서의 검색, 출력, 복제 → ⑩ 사건 종료 후 압수물의 처리의 절차로 진행된다.

후자의 경우는 ① 압수·수색 준비 → ② 압수 수색 현장에서 정보저장매체 수색 → ③ 정보저장매체에서 사건과 관련된 디지털 데이터 조사 → ④ 압수할 정보저장매체의 분리 → ⑤ 정보저장매체 압수 확인서 작성 → ⑥ 이미지 파일 생성 및 이미지 파일 시스템에 업로드 및 정보저장매체의 환부, 가환부 → ⑦ 업로드한 디지털 압수물 다운로드 받아 분석 → ⑧ 분석한 디지털 압수물 업로드, 색인 → ⑨ 일선 수사부서에서의 검색, 출력, 복제 → ⑩ 사건 종료 후 디지털 압수물의 처리의 절차로 진행된다.[91]

91) 예외적으로 압수·수색 현장에서 사건과 관련된 디지털 데이터를 출력, 복제할 수 없는 경우 두 가지 압수 방법은 정보저장매체에 대한 이미지 파일 생성을 현장에서 하는지, 디지털 포렌식 사무실 등 제3의 장소에서 하는지만 다르다.

이 장에서는 각 절차별 세부사항에 대하여 알아보고, 각 절차별 쟁점은 어떠한 것이 있는지에 대하여 알아본다.

제1절 압수·수색 준비

1. 압수·수색을 위한 정보 수집

디지털 데이터의 압수·수색의 경우는 디지털 기기의 종류도 다양하고, 각 디지털 저장매체는 사건과 관련 없는 대량의 데이터가 혼재하고 있기 때문에 일반 유체물에 대한 압수·수색보다 더욱 철저한 정보 수집이 필요하다.

예를 들면, 피압수자의 디지털 기기 사용 수준이나, 서버의 위치, 회사의 전산시스템 관련 정보 등을 미리 확인할 필요가 있다.

2. 영장 청구서 작성

디지털 데이터에 대한 압수·수색 영장을 청구하는 경우에는 압수할 디지털 데이터 및 관련 저장매체를 압수·수색해야할 사유를 소명하여야 한다. 특히 디지털 데이터에 대한 압수·수색 영장 청구의 경우 압수할 컴퓨터, 저장매체나 디지털 데이터의 사건과의 관련성을 소명하여야 하고, 디지털 데이터의 경우 사건과 관련된 디지털 데이터가 저장되어 있을 개연성이 있는 정보저장매체를 기재하고, 위 저장매체에서 압수해야 할 디지털 데이터의 범위를 정하여 기재한다.

3. 디지털 포렌식 수사지원요청

검찰의 경우는 디지털 포렌식 수사관이 별도로 있고[92], 일선 수사팀에서는 디지털 데이터에 대한 압수·수색이나 분석지원을 디지털 포렌식 수사관에게 지원 요청하는 구조이다.

92) 대검찰청은 대검 디지털수사과를 비롯하여, 서울, 부산, 대구, 광주, 대전 5개 고검 및 서울중앙, 인천, 수원, 서울남부, 창원 5개 지검에 디지털 포렌식팀이 설치되어 있다.

가. 사전 협의

디지털 데이터의 압수·수색은 전문지식 및 급변하는 현장에 대응능력이 필요하고 분야별로 전문화된 디지털 포렌식 수사관이 수행하여야 한다.[93] 일선 수사팀은 사건의 개요, 중요 압수 대상 및 압수·수색의 규모 등에 대하여 디지털 포렌식 수사관과 미리 충분히 상의하여야 한다.

나. 지원 요청

사전협의가 이루어진 사건은 일선 수사팀에서 디지털수사통합업무관리시스템에 수사지원을 요청한다. 요청 시 입력해야 할 정보로는 사건번호[94], 죄명, 사건 요지 등의 사건 정보, 접근 권한 설정[95], 그리고 요청할 디지털 포렌식 팀, 압수 장소·일시, 집결 장소· 일시 등의 압수·수색 지원 상세 정보가 있다.

4. 디지털 데이터가 압수 대상인지 여부에 대한 문제

형사소송법은 제106조 제1항에 '증거물 또는 몰수할 것으로 사료되는 물건'이라고 하여 압수의 대상을 '물건'에 한정하고 있다. 그런데 동조 제3항에 "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."고 규정하면서 디지털 데이터에 관한 규정을 입법화하였다. 그런데, 위 규정을 보면 디지털 데이터가 압수의 대상이 되는지에 대하여 명확하게 규정하고 있지 않고 있어, 현행 개정 형사소송법상에 디지털 데이터가 압수의 대상이 되는지

93) 대법원 2007. 12. 13. 선고 2007도7257판결에서 "특히 디지털 저장매체 원본을 대신하여 저장매체에 저장된 자료를 '하드카피' 또는 '이미징'한 매체로부터 출력한 문건의 경우에는 디지털 저장매체 원본과 '하드카피' 또는 '이미징'한 매체 사이에 자료의 동일성도 인정되어야 할 뿐만 아니라, 이를 확인하는 과정에서 이용한 컴퓨터의 기계적 정확성, 프로그램의 신뢰성, 입력·처리·출력의 각 단계에서 조작자의 전문적인 기술능력과 정확성이 담보되어야 한다."

94) 사건번호의 경우 추후 압수한 디지털 데이터의 관리 및 폐기의 측면에서 정확하게 기재하여야 한다.

95) 지원을 요청하는 수사부서에서 당해 지원과 관련된 시스템에 대한 접근 권한을 설정할 수 있다. 사건의 보안 및 압수한 디지털 데이터의 접근 통제를 위하여 엄격하게 접근 권한을 설정하여야 한다.

가 문제된다.

가. 견해의 대립

(1) 긍정설

정보저장매체에 기억된 정보(즉, 디지털 데이터) 자체를 압수의 대상으로 입법화하였다고 보는 견해가 있다.[96]

그리고 개정 형사소송법 제106조 제3항과 제4항의 규정이 문리적으로 컴퓨터용디스크나 그와 비슷한 정보저장매체이지만, 이에 기억된 정보의 범위를 정하여 출력, 복제하여 제출받도록 규정되어 있기 때문에, 압수대상은 디지털 데이터이고, 디지털 데이터에 대한 기본권은 그 저장매체가 아니라 정보의 내용이 대상이 된다는 점을 근거로 위 규정의 신설로 압수의 대상이 디지털 데이터로 보는 견해가 있다.[97]

또한, 제106조 제3항은 마치 '정보저장매체'가 압수·수색의 대상임을 명시한 것처럼 보이나, 동조 제4항에서는 '제3항에 따라 정보를 제공받은 경우'의 통지의무를 규정하고 있고, 압수·수색 방법은 원칙적으로 출력, 복제에 의하도록 정하고 있으므로, 제106조 제3항 전단에도 불구하고 압수·수색의 대상은 '전자정보'라는 견해가 있다.[98]

한편, 증거가치가 있고 압수의 필요성이 있는 무형의 '디지털 정보'는 압수·수색의 대상이 될 수 있다고 보는 견해도 있다.[99] 유체물인 저장매체는 디지털 정보를 압수하기 위한 수단일 뿐이고, 피압수자의 기본권 보장에 유리하며, 디지털 정보의 네트워크 관련성을 감안하여 디지털 증거 자체의 압수가 가능한 점 등을 근거로 하고 있다.

---

96) 손동권, "새로이 입법화된 디지털 증거의 압수수색제도에 관한 연구", 형사정책(제23권 제2호)(2011), 제328쪽; 정웅석, 백승민, 형사소송법(전정 제4판)(2011), 제227쪽.
97) 오기두, "전자정보의 검증 수색 압수에 관한 개정 형사소송법의 함의"(2012. 2. 17.) 한국형사소송법학회 발표문, 제5쪽.
98) 이숙연, "디지털증거의 압수수색", 형사법 실무연구(2011), 제660-661쪽.
99) 이주원, "디지털 증거에 대한 압수수색제도의 개선", 안암법학(37권) (2012), 제160쪽.

(2) 부정설

컴퓨터에 입력된 정보 자체는 그 자체로 압수의 대상물이 아니고, 유체물인 형사소송법 제106조 제3항의 '명문상 컴퓨터용디스크, 그밖에 이와 비슷한 정보저장매체'가 압수의 대상이 될 뿐이라고 본다.[100]

나. 법원의 태도

법원은 전교조 준항고 기각결정에 대한 재항고 사건[101]에서 "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."고 판시함으로써 압수의 대상을 저장매체가 아닌 디지털 데이터라고 하는 긍정설의 입장으로 보인다.

다. 검토

형사소송법 제106조 제3항의 문언상 압수의 목적물은 "컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체"로 디지털 데이터가 아니라, 유체물인 디스크 등 정보저장매체임이 분명하고, 동항은 정보저장매체등에 대한 압수의 집행방법을 규정한 것에 불과하다고 할 수 있다.

또한 동조 제1항에서는 압수의 대상을 "증거물 또는 몰수할 것으로 사료하는 물건"으로 유체물에 한정하고 있고, 법원도 디지털 데이터의 물건성을 부정하고 있다.[102]

그리고 디지털 데이터의 특성에 따라 기존의 유체물에 대한 압수 규정이 그대로 적용되기 어려운데, 이에 대한 별도의 규정을 두고 있지 않기 때문에 압수의 대상

100) 신동운, 신형사소송법(제4판), 법문사(2012), 제343쪽.
101) 대법원 2011. 5. 26.자 2009모1190결정.
102) 대법원 2002. 7. 12. 선고 2002도745 판결은 "컴퓨터에 저장되어 있는 '정보' 그 자체는 유체물이라고 볼 수도 없고, 물질성을 가진 동력도 아니므로 재물이 될 수 없다 할 것이며, 또 이를 복사하거나 출력하였다 할지라도 그 정보 자체가 감소하거나 피해자의 점유 및 이용가능성을 감소시키는 것이 아니므로 그 복사나 출력행위를 가지고 절도죄를 구성한다고 볼 수도 없다."고 판시하여 컴퓨터에 저장되어 있는 정보의 물건성을 부정하였다.

에 디지털 데이터가 포함된다고 보기 어렵다고 할 수 있다.

그러나 위와 같은 이유에도 불구하고 정보저장매체는 디지털 데이터를 저장하는 매체일 뿐이고, 디지털 데이터의 매체독립성으로 인해 저장매체 자체와 디지털 데이터는 명백히 구별되므로, 정보저장매체는 이에 저장된 디지털 데이터를 압수하기 위한 수단일 뿐 그 자체가 압수의 대상이 될 수는 없다고 볼 것이다.[103] 이렇게 보는 것이 디지털 데이터가 압수의 대상이 된다고 보고 있는 실무의 태도에도 부합하고, 피압수자의 기본권도 충실하게 보장할 수 있다.[104]

그러므로 형사소송법 제106조 제3항 본문에도 불구하고, 디지털 데이터는 압수의 대상이 된다고 하겠다. 다만, 명문으로 디지털 데이터가 압수의 대상이라고 형사소송법에 규정하여, 이와 같은 논란을 없애야 할 것이고, 디지털 데이터가 압수의 대상이 된다고 했을 경우 디지털 데이터의 특성으로 인하여 기존의 압수 절차를 그대로 적용하기 어려운 부분에 대하여 별도의 입법이 필요하다 할 것이다.

제2절 압수·수색 현장에서 정보저장매체 수색

1. 현장 촬영 및 통제

압수·수색 현장은 어떻게 변할지 모르기 때문에 현장 입구, 전체 구조, 피압수자의 정보저장매체가 있는 위치, 정보저장매체[105] 등을 사진 촬영을 해두는 것이 바람직하다. 디지털 데이터는 훼손, 변경이 용이하므로, 압수·수색 현장을 신속히 통제하여야 한다. 특히 회사와 같이 피압수자가 여러 명인 경우 피압수자에 대한 통제를 신속히 하여야 한다. 그리고 피압수자가 소지하고 있는 USB나 스마트폰 등의 정보저장매체도 압수한다.

한편 압수·수색 영장 집행 과정에서 사건과 관련된 디지털 데이터를 원격에서 삭제, 은닉하는 경우를 대비하여 네트워크 케이블을 차단하여 이에 대비한다.[106]

---

103) 원혜욱, “정보저장매체의 압수수색”, 형사판례연구 22, 제315쪽.

104) 정보저장매체가 압수의 대상이라고 하면, 정보저장매체에 사건과 관련 없는 디지털 데이터도 당연히 압수의 대상으로 보아 피압수자의 프라이버시 등의 권리를 침해할 가능성이 커진다.

105) 컴퓨터 등이 작동 중일 경우 컴퓨터 등의 시간이 실제 시간과 차이가 나는 경우도 있으므로, 시간 정보를 확인할 수 있도록 하여 사진을 촬영한다.

106) 대검예규 제616호 디지털 증거 수집 및 분석 규정 제15조 제2항 후단. “압수·수색·검증 대상 정보저장매체가 정보통신망에 연결되어 있고, 압수·수색 대상자가 정보통신망으로 접속하여 기억된 정보를 임의로 삭제할

2. 압수·수색 대상 특정

압수·수색 대상을 특정하여 압수·수색 영장의 집행을 하여야 한다. 이를 위하여 직원 배치표 등을 이용하여 피압수자를 결정[107]하고, 실 근무 위치, 담당 업무 등을 파악하여 수색할 정보저장매체를 특정한다.

또한 최근 컴퓨터 등 정보저장매체의 교체 및 OS 재설치 현황 등을 확인하여, 교체 전 사용하던 저장매체를 확보하고 교체나 재설치 경위 등을 파악하여 증거 인멸 여부를 확인한다.

3. 피압수자 등 관련자의 협조

디지털 데이터를 압수·수색하는 경우에는 피압수자나 기업의 전산담당자의 협조가 중요하다. 예를 들면, 컴퓨터 등이 암호화 되어 있는 경우 암호의 해제를 요청하여 디지털 데이터를 수색할 수 있고, 특히 기업 압수·수색의 경우 다양한 서버, 스토리지 등의 정보저장매체로 구성되어 있기 때문에 전산담당자의 협조가 필수적이다.

전산담당자에게 시스템 및 주변기기의 운영 방법, 관리 및 백업 정책, 백업 데이터의 보관 위치 등의 정보를 확인해야 한다.

4. 원격지에 저장된 디지털 데이터에 대한 압수·수색의 문제

디지털 데이터의 압수·수색의 경우 압수·수색 장소는 통상 해당 디지털 데이터가 저장된 정보저장매체가 있는 장소라고 하여 영장 청구서에 특정한다. 하지만, 최근 기업의 경우 IDC(Internet Data Center)를 별도로 운영하는 곳이 늘어나고, 제3자 소유의 서버를 임차하여 사용하거나 '클라우드' 컴퓨터가 보편화 되면서, 집이나 사무실에 정보저장매체를 두지 않고 다른 곳에 있는 서버나 저장매체에 디지털 데이

우려가 있을 경우에는 정보통신망 연결 케이블을 차단할 수 있다." 다만, 서버의 경우 사건과 관련 없는 대량의 디지털 데이터를 서비스 하고 있는 경우가 있으므로 네트워크 케이블 차단에 신중해야 한다.

107) 보통의 경우 피압수자는 압수·수색 영장의 피의자로 특정되지만, 경우에 따라 담당 업무로 피압수자를 특정하는 경우도 있다. 특히 회사 관련 압수·수색을 하는 경우 주요 피압수자는 피의자를 비롯하여 회사의 회계업무를 담당하고 있는 직원이 될 수 있다.

터를 저장하는 경우가 증가하고 있다. 이 경우 압수·수색 영장에 기재되어 있는 압수·수색 장소와는 다른 장소에 있는 저장매체의 디지털 데이터를 압수할 수 있는지 문제된다.

이 경우 영장에 기재된 압수·수색 장소가 아닌 원격지에 있는 서버 등 정보저장매체에 '접속'하여 범죄와 관련된 디지털 데이터를 '출력, 복제'하게 되면 디지털 데이터가 압수·수색 현장에 있는 것이 되어 압수·수색 영장에 허용된 범위를 넘는 것은 아니다. 압수의 대상은 압수·수색을 개시할 때부터 압수·수색 장소에 있을 것을 요구하지 않고, 압수·수색이 종료하기 전까지 확보됨으로 족하기 때문이다.[108]

현재 이와 관련하여 실무는 수사기관이 '압수·수색 장소에 존재하는 컴퓨터로 해당 웹사이트에 접속하여 디지털 정보를 다운로드한 후 이를 출력 또는 복사하거나 화면을 촬영하는 방법으로 압수한다.'고 영장청구서에 기재하여 압수·수색 영장을 발부받는 등의 방법으로 원격지 압수·수색에 관한 적법성을 확보하고 있는 실정이다.[109]

하지만, 이러한 수색행위를 위 압수·수색영장 실무나 형사소송법 제120조의 필요한 처분의 해석론으로 '강제처분법정주의'에 비추어 보면 부담이 따른다는 점에서 이에 대한 입법적 조치가 필요하다고 본다.[110]

5. 피압수자 등의 협력 문제

디지털 기술의 발전에 따라 수사기관이 범죄자에 비하여 증거 수집에 있어서 우월한 지위에 있다고 보기 어렵게 되었고, 오히려 법원에 의하여 발부된 압수·수색 영장의 집행을 따라야할 소극적 의무만을 부담하는 피압수자 등 관련자의 협조가

108) 이숙연, "디지털증거의 압수수색 ", 형사법 실무연구 제123집(2011), 제663쪽. 다만, 압수·수색 영장에 '특정 장소에 저장중인 디지털 데이터'로 특정되어 있는 경우에는 위와 같은 방법의 압수가 적법하다고 보기는 어렵다. 이와 관련하여, 일반 유체물인 서류와 관련된 '제주도지사 공직선거법위반 사건'에서 압수·수색 영장에 압수대상물을 압수장소에 '보관중인 물건'으로 기재한 경우, 이를 '현존하는 물건'으로 해석할 수 없다고 판시하였다(대법원 2009. 3. 12. 선고 2007도763판결).

109) 이숙연, "디지털증거의 압수수색 ", 형사법 실무연구 제123집(2011), 제664쪽.

110) 이와 관련하여 일본 형사소송법은 개정으로 통하여 명문의 규정을 두어 입법적으로 해결하였다. 일본 형사소송법 제99조 제2항 및 제218조 "압류(압수)할 것이 전자계산기인 때에는 당해 전자계산기에 전기통신회선으로 접속하고 있는 기록매체로서, 당해 전자계산기로 작성 또는 변경을 한 전자적 기록이나 당해 전자계산기로 변경 또는 삭제할 수 있는 전자적 기록을 저장하는데 사용되고 있다고 인정할 만한 상황에 있는 때에는 그 전자적 기록을 당해 전자계산기나 다른 기록 매체에 복사한 후, 해당 전자계산기나 다른 기록 매체를 압류(압수)할 수 있다."

필요하게 되어, 피압수자 등 관련자의 협조를 구할 수 있는 규정의 필요성이 대두되었다.

가. 협력의무의 내용

피압수자 등 관련자가 압수·수색 영장의 목적달성에 필요한 조치를 집행기관에 적극적으로 제공하여야 하는 의무를 '협력의무'라고 할 수 있다. 구체적으로 압수·수색 영장 집행 전에 디지털 데이터가 삭제되지 않도록 보전조치를 하여야 하는 '보전의무', 압수·수색 영장 집행 단계에서 디지털 데이터를 제출하는 '제출의무', 암호화된 정보저장매체에 대한 패스워드의 제공, 암호화된 파일의 복호화, 네트워크로 연결된 다른 컴퓨터의 접속에 필요한 조치의 제공 등 수사기관의 영장 집행행위에 협력하는 '협의의 협력의무'가 있을 수 있다.[111]

나. 협력의무 명문의 규정 필요성

(1) 보전의무

피압수자나 관련자가 보전의무를 위반 하였을 경우 제재 수단이 마땅치 않고, 피압수자가 제3자일 경우 민사적인 개인정보 보호책임 내지 그 정보보호 의무와 충돌하고, 헌법상의 적법절차 원리 구현 규정을 사문화할 우려가 있기 때문에 협력의무를 규정하는 것에 부정적인 견해도 있다.[112]

그러나 보전의무의 경우 디지털 데이터의 취약성에 직접적으로 기초한 것으로 위의 다른 협력의무보다 남용의 위험성도 적고, 피압수자 등 관련자에 권리의 침해 정도도 적기 때문에 수사기관의 긴급처분으로서 도입되는 것이 타당하다.

111) 이윤재, "디지털증거의 압수수색영장의 집행에 있어서의 협력의무" 한국형사법학회, 형사법연구 제24권 제2호(2012), 제304-305쪽.
112) 오기두, "디지털증거 압수수색에 관한 법률의 문제점과 개선방안"의 토론문, 2012년 디지털증거 압수수색에 관한 개정법률(안) 공청회 자료. 제53-55쪽.

(2) 제출의무

제출의무의 경우 형사소송법 제106조의 개정으로 법원과 더불어 수사기관도 디지털 증거에 대하여 제출명령을 할 수 있게 되었다는 견해가 있다.[113] 이 견해는 개정법의 입법과정에서 입법자들이 디지털 증거의 특성에 초점을 두고 제출명령을 논의한 뒤 유형력의 행사에 의한 압수를 추가함으로써 제출명령과 유형력에 의한 압수를 병렬적 형태로 규정하고자 하였다고 하면서, 개정법에서 제출명령이 도입된 것은 명백하다고 한다. 그러나 동조는 압수에 관한 규정으로 동조 제3항은 디지털 데이터에 관한 압수·수색 방법에 관한 규정이지, 동항 본문이 제출명령을 도입한 것이라고 단정할 수 없기 때문에 위의 의견에 동조하기 어렵다.

제출의무는 디지털 데이터에 대한 압수·수색 영장이 발부되었을 경우 수사기관이 강제력을 이용하여 압수하는 대신 피압수자 등 관련자의 협조에 의하여 사건과 관련된 디지털 데이터를 취할 수 있다는 점에서 영장 집행보다 피압수자 등의 권리를 덜 침해하는 방법이므로, 이에 대한 입법적 조치가 필요하다.[114]

(3) 협의의 협력의무

협의의 협력의무는 제출의무 이행에 대한 정보저장매체의 작동이나 복호화, 시스템을 이용하여 디지털 데이터를 검색 및 출력과 같은 협의의 협력의무까지 포함하고 있으므로, 협의의 협력의무가 의미 있는 경우는 피압수자 등 관련자가 디지털 데이터를 찾아 줄 의사나 능력은 없지만 디지털 데이터를 저장하고 있는 시스템을 이해하고 그 관리권을 갖고 있을 때와 같이 피처분자에게 제출명령을 하는 것이 의미가 없을 때이다.

구체적으로 모든 경우를 특정하여 규정하기는 어려울 것이므로, '수사기관의 협력요청이나 요구' 정도로 규정하는 것이 바람직할 것이다. 이에 따라 협력의무를 이행을 하면 일정한 경우에 제3자에 대한 법적 책임을 면하거나 그 협력에 대한 보상규정을 도입할 수 있는 근거가 생기기 때문에 의미가 있다 하겠다.[115]

---

113) 이윤재, "디지털증거의 압수수색영장의 집행에 있어서의 협력의무" 한국형사법학회, 형사법연구 제24권 제2호(2012), 제319-320쪽.

114) 한편, 제출을 명하였을 때 불응했을 경우 비록 경미한 정도라도 일정한 제재를 가할 수 있도록 입법이 필요하다.

115) 이윤재, "디지털증거의 압수수색영장의 집행에 있어서의 협력의무" 한국형사법학회, 형사법연구 제24권 제2호(2012), 제327쪽.

다. 검토

생각건대, 국민의 기본권 존중이 근간인 우리 헌법 하에서 수사권을 약화시켜야 한다는 이유로 국민의 의무를 확장하는 것은 바람직하지 않다고 할 수 있으나, 형사소송법상 증언의무와 같은 국민의 협력의무와 이에 대한 강제수단이 도입되어 있는 점, 유체물에 대한 제출명령이 이미 기존 형사소송법에 도입되어 있었던 점에 비추어 디지털 데이터의 압수·수색과 관련한 협력의무가 헌법에 위배된다고 보기는 어렵다.

그리고 최근 세계적인 추세는 디지털 증거에 관한 제출의무, 보전의무, 협의의 협력의무를 인정하는 방향으로 가고 있다.[116]

그러므로 피압수자 등 관련자에게 협력의무를 부과하여 수사기관이 디지털 데이터에 대하여 접근할 수 있는 가능성은 열어 두는 것이 시대 현실에 부합한다고 하겠다. 물론, 이러한 협력의무가 진술거부권, 증언거부권과 같은 기본권을 침해해서는 안 될 것이다.[117]

제3절 정보저장매체에서 사건과 관련된 디지털 데이터 조사

현장에서 디지털 포렌식 수사관은 수색한 정보저장매체에서 범죄와 관련된 디지털 데이터를 검색한다. 개정 형사소송법과 법원의 태도에 의해 원칙적으로 디지털 포렌식 수사관은 정보저장매체에서 사건과 관련된 디지털 데이터를 찾는다. 찾는 방법은 키워드를 이용하여 해당 정보저장매체를 검색하거나, 범죄와 관련된 시간을 정하여 해당 시간에 생성하거나 접근한 파일을 검색하거나, 일 등 파일의 종류 별로 검색 또는 파일 시그니처[118]를 검색하는 방법이 있다.[119]

---

116) 이윤재, “디지털증거의 압수수색영장의 집행에 있어서의 협력의무” 한국형사법학회, 형사법연구 제24권 제2호(2012), 제320-323쪽.

117) 이윤재, “디지털증거의 압수수색영장의 집행에 있어서의 협력의무” 한국형사법학회, 형사법연구 제24권 제2호(2012), 제325쪽.

118) 파일 시그니처(File Signature)는 파일 헤더에 저장되어 있는 파일의 종류를 식별하는 고유한 정보이다. 같은 종류의 파일은 같은 값의 파일 시그니처를 가지고 있다. 이에 비하여 파일의 확장자는 Window와 같은 OS 시스템이나 응용프로그램이 파일의 종류를 식별하기 위하여 사용하는 정보로 파일 이름 뒤에 3byte 크기로 저장된다. 파일의 확장자는 사용자가 쉽게 변경할 수 있으나, 파일 시그니처는 그 변경이 매우 어렵다.

119) 대검찰청, 과학수사 실무 매뉴얼(2014), 제170-170쪽.

○ 현장에서 사건과 관련성 있는 디지털 데이터를 확인할 수 있는 기술적 방법

현장에서 디지털 데이터를 하나씩 열어 그 관련성 여부를 판단하고 압수하는 것이 가장 이상적이지만, 제한된 시

정보저장매체에서 사건과 관련된 디지털 데이터의 조사를 압수·수색 현장에서 행하는 것은 실제로 상당히 어려운 일이다. 이는 정보저장매체 자체를 압수하여 수사기관의 사무실에서 전체에 대하여 이미지 파일을 생성하여 이에 대하여 행하던 것을 시간과 인력, 장비가 한정된 현장에서 해야 하기 때문이다. 압수·수색 현장의 경우 해당 정보저장매체의 성능에 많이 의존하게 된다. 성능이 낮을 경우 사건과 관련된 디지털 데이터를 조사하는 과정에서 다운되어 디지털 데이터를 상실할 우려도 있다. 그리고 수사기관의 사무실에서 분석하는 경우와 달리 디지털 데이터를 다양한 방법으로 조사할 수 없게 되어 효과적인 압수·수색을 할 수 없을 수도 있다.[120]

간, 공간, 인원, 기술, 도구 등에 비추어 현실적으로 불가능하므로, 디지털 데이터에 대한 관련성 여부를 판단함에 있어 다음과 같은 기술적 방법을 활용할 수 있다.

1. 파일명 검색
혐의사실과 관련 있는 '검색어'로 파일 이름을 검색하여 사건과의 관련성 여부를 확인할 수 있다.
그러나 혐의자가 파일명을 '1.hwp, 20150302.ppt', '아무개.hwp, 잡동사니.doc, ㅎㅎ.xls' 등 습관적으로 또는 은폐의 목적으로 무작위로 만든 것이 확인될 경우에는 다른 방법으로 추가 검색을 해야 한다.
2. 파일 시간별 검색
혐의사실과 관련된 기간에 생성, 수정, 또는 접근한 파일을 검색하여 사건과의 관련성 여부를 확인할 수 있다.
예를 들면, 혐의자가 2014. 3. 2.경 회사 사무실에서 업무용 컴퓨터에 저장된 주요 고객정보를 담고 있는 엑셀 파일을 자신의 USB에 복사하여 유출하였다는 혐의를 받고 있다면, 해당 USB를 검색하여 2014. 3. 2.경에 생성된 엑셀 파일을 1차적으로 선별할 수 있다.
3. 파일 종류별 검색(확장자 검색)
혐의사실과 관련 가능성이 있는 파일의 종류를 검색하여 사건과의 관련성 여부를 확인할 수 있다.
예를 들면 혐의자가 헤어진 여자 친구의 나체를 찍은 동영상을 인터넷에 유포하였다는 혐의를 받고 있는 경우에는 동영상파일(avi, wmv, mp4), 사진파일(jpg, bmp), 압축파일(zip, alz) 등 동영상과 그래픽 관련 파일 위주로 검색하는 방법이 있다.
4. 파일내용 검색
혐의사실과 관련 있는 '검색어'로 문서파일의 내용을 검색하여 사건과의 관련성 여부를 확인할 수 있다.
하지만 이 방법은 파일을 열어보지 않고 사건과 관련성이 있는 내용을 포함한 문서파일을 확보할 수 있어 매우 유용한 방법이지만, 검색할 디지털 데이터가 문서파일이어야 하고, 그 데이터의 용량이 적어야 하며 압수 대상 컴퓨터가 고성능일 경우에 한해서 사용하는 방법이다.
왜냐하면 문서파일의 양이 방대하면 검색하는데 장시간이 소요되고, 압수 대상 컴퓨터가 저사양이면 검색 중 대상 컴퓨터가 다운되어 디지털 데이터가 훼손될 수 있기 때문이다. 또한 문서파일을 스캔하여 저장해둔 경우에는 그림파일로 변환되기 때문에 검색어를 입력하여 파일의 내용을 검색할 수 없으므로 다른 방법으로 추가 검색을 하여야 한다.
5. 파일 시그너처 검색
혐의자가 "유치권약정서.hwp" 라는 파일을 숨기기 위해 파일의 확장자인 'hwp'를 'jpg'로 변경하여 "유치권약정서.jpg" 파일로 저장하는 등 의도적으로 파일의 확장자를 변경하여 파일을 은닉하였을 경우에는 현장에서 파일의 시그너처로 검색하는 방법이 있다.

120) 여러 가지 디지털 포렌식 도구를 사용하여 다양한 방법으로 디지털 데이터를 찾는 것이 분석 과정에 일환인데, 이 과정을 현장에서 해결해야 하는 문제가 생겼다.

1. 현장용 디지털 포렌식 도구의 문제

위와 같은 문제점으로 인하여 현장에서 디지털 포렌식 수사관이 사건과 관련된 디지털 데이터를 조사하고 복제하는데 사용하는 도구의 중요성이 강조되고 있으나, 이에 대한 연구는 미미한 현실이다. 검찰의 경우 디지털 포렌식 수사관은 현장에서 Encase portable, CFT[121]등을 많이 사용하나, 위와 같은 도구는 실질적으로 압수·수색 현장에서 디지털 데이터에 대한 '분석'을 해야 하는 우리나라의 현실에 맞게 개발된 것이 아니라 문제의 소지가 있다.

가. 현장용 디지털 포렌식 도구의 요건

(1) 정보저장매체의 확인

디지털 정보저장매체의 다양화, 대용량화 등을 고려하여 피압수자가 소지하고 있는 모든 디지털 정보저장매체를 압수·수색할 수 있도록 현장용 디지털 포렌식 도구는 다양한 정보저장매체를 확인할 수 있어야 한다.[122]

(2) 데이터 수색 준비 단계(저장매체 분리)

압수·수색 현장은 여러 가지 변수가 존재한다. 전원 연결 장치가 없는 등 해당 정보저장매체를 그 자체만으로는 확인할 수 없는 경우, 정보저장매체를 분리, 현장용 디지털 포렌식 도구에 연결하여 확인할 수밖에 없다.

한편, 현장용 디지털 포렌식 도구는 해당 정보저장매체가 켜져 있는 경우 현재 실행중인 프로그램이나 프로세스 정보 등 휘발성 데이터[123]를 수집할 수 있는 기능이 제공되어야 한다.[124]

---

121) Computer Forensics Tools의 약자로 대검찰청이 직접 개발한 현장용 디지털 포렌식 도구로 형사소송법 개정이전에 개발된 도구이다.

122) 임한희, "개정된 형사소송법에 적합한 현장 디지털 증거 추출도구 필요요건에 관한 연구", 고려대학교 정보보호대학원 석사학위논문(2012), 제33쪽.

123) 휘발성 데이터의 종류로는 시간 정보 기록, 현재 네트워크 연결 상태, 현재 오픈된 TCP, UDP 포트 정보 기록, TCP, UCP 포트를 오픈하고 있는 실행 파일 기록, NETBIOS 캐시 정보 기록, 현재 접속 사용자 정보 기록, 인터넷 라우팅 테이블 기록, 실행중인 프로세스 내역 기록, 실행중인 서비스 내역 기록, 예약된 작업 내역 기록, 현재 사용중인 파일 내역 기록 등이 있다.

124) 임한희, "개정된 형사소송법에 적합한 현장 디지털 증거 추출도구 필요요건에 관한 연구", 고려대학교 정보보호대학원 석사학위논문(2012), 제33-34쪽.

(3) 안티포렌식 탐지·분석 단계

Window나 리눅스, 유닉스 등 다양한 운영체제와 여러 가지 복합적인 정보저장매체의 사용 환경 변화에도 대처할 수 있는 다양한 파일시스템 분석을 지원해야 한다. 그리고 최근 사용이 늘어나고 있는 클라우드 시스템의 경우 디지털 데이터가 현장의 정보저장매체가 아닌 클라우드 서버에 저장되어 있을 가능성이 크므로, 클라우드 시스템 사용여부도 현장에서 반드시 확인해야 한다.[125]

한편, 최근의 안티 포렌식 기술은 완전 삭제, 은닉, 암호화 등 여러 가지 형태로 디지털 포렌식을 위협하고 있다. 그러므로 안티 포렌식에 의해 디지털 데이터가 은닉, 훼손되었는지 확인할 수 있는 기능이 있어야 한다. 또한 디지털 데이터를 압수함에 있어 증거분석을 위해 반드시 필요한 정보인 메모리 정보, 레지스트리, 웹브라우저, 메타데이터 등 행위관련 데이터를 신속하게 수집할 수 있는 기능이 필수적이다.[126]

파일 검색 및 키워드 검색기능의 중요성은 말할 필요가 없다. 디지털 데이터를 수색할 때 파일 및 키워드 검색은 빠른 시간에 사건과 관련된 데이터를 찾을 수 있어 현장 압수·수색의 기본이 되는 압수·수색 방법이기 때문이다. 파일 검색의 경우 문서, 동영상, 그림 파일 등 종류별로 검색이 가능하여야 하고, 키워드 검색은 사건과 관련된 특정 문자열을 파일, 할당 영역, 비할당 영역, 슬랙 영역, 메모리에서 검색할 수 있어야 한다.[127]

끝으로 최근 디지털 기기를 능숙하게 다루는 사람이 아니더라도 인터넷에서 찾거나, 프로그램을 이용하여 손쉽게 디지털 데이터를 삭제할 수 있게 되었다. 이에 대한 대비로 삭제된 파일의 복원 기능이 필요하다. 복원 기능은 삭제된 파일, 유실 파일에 대한 복구와 비할당영역, 슬랙 영역에 대한 복구 가능, 파일 유형에 따른 복구 기능도 지원되어야 한다.[128]

---

125) 임한희, “개정된 형사소송법에 적합한 현장 디지털 증거 추출도구 필요요건에 관한 연구”, 고려대학교 정보보호대학원 석사학위논문(2012), 제35쪽.
126) 임한희, “개정된 형사소송법에 적합한 현장 디지털 증거 추출도구 필요요건에 관한 연구”, 고려대학교 정보보호대학원 석사학위논문(2012), 제35쪽.
127) 임한희, “개정된 형사소송법에 적합한 현장 디지털 증거 추출도구 필요요건에 관한 연구”, 고려대학교 정보보호대학원 석사학위논문(2012), 제36쪽.

(4) 전체·선별 복사 단계

디지털 데이터에 대한 복제, 복사 기능이 지원되어야 한다. 사건과 관련된 파일을 수색하여 찾은 경우 이를 진정성, 무결성[129]을 보장하면서 복제, 복사 하여야 하는 기능은 디지털 증거의 증거능력 인정을 위하여 필수적인 기능이다. 또한 예외적인 경우 현장에서 해당 정보저장매체 전체의 이미지 파일을 생성하여야 할 경우도 있으므로, 물리적 이미지 파일 생성 기능도 지원해야 한다.[130]

2. 디지털 증거 수집도구별 기능 비교

현재 국내에서 가장 많이 사용되고 있는 현장용 디지털 포렌식 도구의 성능에 대하여 비교하였다. CFT는 검찰에서 주로 사용하는 현장용 디지털 포렌식 도구이고, HERA는 경찰청 수사관이 컴퓨터에 대한 전문지식이 없어도 디지털 포렌식 관련 업무를 수행할 수 있도록 경찰이 자체 개발한 도구이다. Encase Portable의 경우는 미국의 Guidance사가 만든 현장용 디지털 포렌식 도구이다. 아래에서 비교한 버전은 CFT의 경우 2010. 개발된 CFT10, HERA의 경우는 2011. 개발된 프로그램, Encase Portable의 경우는 2012. 버전을 기준으로 비교하였다.[131]

분류	지원항목	CFT	Encase Portable	HERA
파일시스템	NTFS	O	O	O
	FAT	O	O	O
	NFS	X	X	X
	EXT2	X	X	X
	EXT3	X	X	X
	EXT4	X	X	X
	HFSX	X	X	X
	UFS	X	X	X

128) 임한희, “개정된 형사소송법에 적합한 현장 디지털 증거 추출도구 필요요건에 관한 연구”, 고려대학교 정보보호대학원 석사학위논문(2012), 제36쪽.
129) 진정성, 무결성을 보장을 위하여 복제, 복사된 파일에 대한 해시 값 생성 등의 기능을 지원하여야 한다.
130) 임한희, “개정된 형사소송법에 적합한 현장 디지털 증거 추출도구 필요요건에 관한 연구”, 고려대학교 정보보호대학원 석사학위논문(2012), 제36쪽.
131) 임한희, “개정된 형사소송법에 적합한 현장 디지털 증거 추출도구 필요요건에 관한 연구”, 고려대학교 정보보호대학원 석사학위논문(2012), 제37쪽.

분류	지원항목	CFT	Encase Portable	HERA
이미지 읽기	E01	O	X	X
	DD	O	X	X
	DFI	X	X	X
이미지 쓰기	E01	O	O	O
	DD	O	O	O
	DFI	O	O	X
논리이미지	LFI	O	O	X
	TAR	X	X	O
물리 드라이브	HDD	O	O	O
	USB / Memory CARD	X	X	X
	논리 드라이브	O	O	O
정보수집	휘발성 정보 수집	O	O	O
	하드 디스크 분석	O	O	O
	메모리 정보 수집	O	O	O
	레지스트리 정보 수집	O	O	O
	인터넷 히스토리	O	O	O
	클라우드 정보수집	X	X	X
	SNS 정보수집	X	X	X
복구	삭제된 파일	O	O	O
	유실 파일	O	O	O
	비할당 영역 복구	O	X	X
	슬랙 영역 복구	O	X	X
안티포렌식 탐지	완전삭제도구 탐지	X	X	X
	파일 은닉 도구 탐지	O	X	X
	가상 드라이브, 암호화 도구 탐지	X	X	X
검색	키워드 검색, 정규식 검색	O	X	O
	비할당 영역 검색	X	X	X
	슬랙 영역 검색	O	X	X
	HWP/DOC 등 오피스 파일 키워드 검색	O	O	O
	파일 이름 검색	O	X	O
	파일 타입 검색	O	O	O
	개인 정보 검색	O	X	O
시각화	이미지 갤러리 지원	O	X	X
	문서 미리 보기	O	O	X
	헥사뷰	X	X	X

분류	지원항목	CFT	Encase Portable	HERA
	텍스트 뷰	O	X	X
	데이터 전환	X	X	X
프로젝트	프로젝트 파일 지원	X	X	X
	북마크	O	X	X
기타	운영체제 정보	O	X	O
	사용자 정보	O	X	O
	이메일 분석	O	O	O
	웹검색	O	X	O
	메신저	X	X	O
	USB 히스토리	O	X	O
	이벤트 로그	O	X	O
	원격 사용 정보	O	X	O
	프로세스 분석	O	O	O
	해시데이터 생성 기능	O	O	O
	증거데이터 목록 출력	O	X	O

[표14] 현장 디지털 포렌식 도구 기능 비교[132)]

위 비교에 따르면, 분석 가능한 파일시스템의 경우 NTFS와 FAT만 지원하고 있고, 안티포렌식 도구 탐지 기능은 CFT가 지원하고 있으나, 완전 삭제 프로그램, 가상 드라이브, 암호화 프로그램, 파일 은닉 프로그램 등 다양한 안티포렌식에 대한 탐지 기능은 부족하다.

그리고 가장 중요한 기능이라고 볼 수 있는 디지털 데이터에 대한 복구 기능, 검색 기능, 유용한 정보 분석 기능이 상호간에 차이가 있고, 그 지원 정도도 다양한 현장 상황에 대응하기에는 부족하여 문제된다.

3. 검토

위에서 보았듯이 압수·수색 현장에서 하나의 도구만을 가지고 조사하는 것은 불가능하다고 할 것이다. 그렇다고 하나의 정보저장매체에 여러 가지 디지털 포렌식 도구를 사용해 보는 것은 시간적 제약에 의해 곤란하다고 할 것이다. 그러므로 우

132) 임한희. 개정된 형사소송법에 적합한 현장 디지털 증거 추출도구 필요요건에 관한 연구. 석사학위논문. 2012. 제38-39쪽.

리나라의 현실에 적합한 현장용 디지털 포렌식 도구 개발이 절실하게 요구된다고 하겠다.

제4절 사건관련 파일 복제, 목록 작성 교부, 확인서

1. 구체적인 절차

압수하고자 하는 데이터의 변경이 발생하지 않도록 선별한 디지털 데이터를 현장용 디지털 포렌식 도구를 사용하여 논리적 이미지 파일을 생성한 후, 해시 값을 계산하는 등 무결성을 담보하기 위한 적절한 조치를 취하여야 한다.

‘현장조사보고서’에 생성한 이미지 파일에 대한 해시 값 등을 기재하고 피압수자 또는 참여인에게 확인, 서명을 받아 2부를 사본한다. 그 중 사본 1부는 피압수자에게 교부하고, 다른 사본 1부는 디지털 포렌식 수사관이 보관하며, 원본은 수사팀에 인계한다. 수사팀은 인계받은 ‘현장조사보고서’의 내용을 참고하여 압수목록을 작성해 피압수자에게 교부한다.

2. 진정성, 무결성을 인정하기 위한 조치

과거 주로 정보저장매체 자체를 압수하던 때에는 저장매체를 봉인하여 수사기관의 사무실로 옮긴 다음, 봉인 해제한 저장매체에 대한 전체 이미지 파일을 생성하고 이를 분석하였기 때문에 상대적으로 무결성에 대한 시비는 크게 없었다. 무결성과 관련된 문제가 제기되었을 경우 전체 이미지 파일에서 재현을 하면 되었기 때문이다. 하지만, 디지털 데이터에 대하여 현장에서의 압수가 원칙이 된 지금은 기술적으로 압수한 디지털 데이터의 무결성(특히 원본성)을 인정하는 것이 어렵게 되었고, 진정성, 무결성에 대한 시비가 생길 수 있게 되었다.

이를 대비하여 검찰은 디지털 데이터를 현장 압수하는 경우 압수한 디지털 데이터의 파일명과 이에 대한 해시 값을 기재한 현장조서보고서를 작성하여 피압수자나 참여인에게 확인, 서명을 받아 압수한 디지털 데이터에 대한 최소한의 무결성 보장 장치를 마련하였다.

하지만 현장조사보고서는 실무상 활용되고 있는 문서일 뿐이다. 현장조사보고서나 이를 근거로 작성한 증거목록을 법정에서 피고인이 부동의 한다면, 압수한 디지털 데이터에 대한 무결성을 입증하기는 어렵게 된다. 그러므로 이에 대한 절차적인 보완이 필요하다.

한편, 압수목록에 기재하는 방법도 문제이다. 형사소송법은 제129조, 제219조에서 수사기관이 압수한 경우 목록을 작성하여 소유자, 소지자, 보관자 기타 이에 준하는 자에게 교부하여야 한다고 규정하고 있다. 이는 압수물의 존재 여부, 압수물의 멸실, 훼손 등의 변경에 대한 시비를 사전에 방지하고, 피압수자에게 환부, 가환부 청구 등의 권리행사를 보장하기 위함이다. 그런데 압수한 디지털 데이터의 경우 이를 특정하여 기재하는 것이 쉽지 않다. 파일명이 있는 경우 파일명을 특정하여 기재하는 것이 가능하나 이 경우도 수색한 정보저장매체가 함께 기재되어야 특정될 것이다. 또한 '압수목록은 피압수자의 권리 행사에 지장이 없도록 압수 직후 현장에서 바로 작성하여 교부해야 하는 것이 원칙'[133]이나, 압수한 파일의 수가 많을 경우 현장에서 일일이 압수목록이 기재하는 것이 만만치 않은 경우도 있다. 생각건대, 디지털 압수물에 대한 압수목록 기재 방법 등에 대한 입법적 보완이 필요하다 하겠다.

제5절 복제한 디지털 압수물 업로드 및 색인

디지털 포렌식 수사관은 디지털 압수물을 대검찰청 디지털수사통합업무관리시스템(DFIS II)에 업로드 한다.[134] 검찰은 디지털 압수물을 안전하게 보관하고 접근을 제어하고자 기존의 디지털 포렌식 수사관 각자의 PC에 보관하는 방식을 개선하여 별도로 디지털 증거 관리 시스템을 운영하고 있다.

디지털 압수물의 메타 데이터를 분석해야 하는 등 정밀 분석이 필요한 경우를 제외하고는 통상적으로 현장에서 사건과 관련된 디지털 데이터만 선별한 경우에는 특별히 분석할 것이 없이 디지털 압수물을 그대로 DFISII에 업로드 한다.

업로드 후 디지털 포렌식 수사관은 압수 및 분석결과보고서를 작성하고, 디지털

133) 대법원 2009. 3. 12. 선고 2008도763 판결.
134) 검찰 예규 제616호 디지털 증거 수집 및 분석 규정 제18조.

포렌식 수사관의 디지털 포렌식 지원 절차는 종료한다. 디지털 포렌식 수사관은 자신의 노트북이나 외장하드에 저장하고 있는 압수한 디지털 데이터는 업로드 후 즉시 삭제한다.[135]

업로드된 디지털 압수물은 각 지역 거점청 스토리지에서 대검찰청 디지털수사과의 메인 스토리지에 전송, 보관되고 거점청 스토리지의 디지털 압수물은 전송완료 후 삭제된다. 대검찰청 디지털수사과에서는 백업을 하는 등 디지털 압수물을 안전하게 보관하기 위한 조치를 취한다.[136]

업로드된 디지털 압수물은 통합디지털증거분석시스템에서 자동으로 색인을 한다. 색인이란 디지털 압수물의 내용을 형태소별로 정리하여 보관하는 과정으로, 색인이 완료된 디지털 압수물은 키워드로 검색하는 시간이 짧게 걸려 최근 대용량화 하고 있는 디지털 압수물을 수사에 활용하는데 반드시 필요한 절차이다.

1. 시스템에 디지털 압수물을 업로드 하는 행위에 대한 문제

디지털 압수물을 시스템에 업로드 하는 행위가 법적 성질이 무엇인지 문제된다. 시스템에 업로드 하는 행위는 디지털 압수물에 대한 '복제'라고 할 수 있는데, 이것이 영장주의에 위배되는지 문제가 되기 때문이다.

압수의 대상이 디지털 데이터라고 하는 견해나 정보저장매체라고 하는 견해 모두 압수의 방법으로 현장에서 사건과 관련된 디지털 데이터를 선별하여 압수한 경우 현장에서의 압수로 압수는 종료되었다고 볼 것이다. "전자정보에 대한 압수·수색영장을 집행할 때에는 원칙적으로 영장 발부의 사유인 혐의사실과 관련된 부분만을 문서 출력물로 수집하거나 수사기관이 휴대한 저장매체에 해당 파일을 복사하는 방식으로 이루어져야"한다는 법원의 견해도 현장에서의 디지털 데이터의 압수로 압수는 종료되었다고 할 것이다.

---

135) 대검찰청, 수사 등의 과정에서 취득한 디지털 자료 관리 지침 제8조 제1항 "검찰공무원은 사건 처분시 업무용 PC에 저장된 디지털 자료를 삭제하여야 한다."

136) 디지털 압수물은 분석 및 색인이 종료되면 보관용 저장서버에 보존되고, 항소·상고 등의 사유로 법원, 피고인 등에 의해서 확인이 필요한 경우 이외에는 접근이 차단되어 사건 종결 시까지 봉인된다. 이미지 파일이 보존되는 동안 그에 대한 접근 로그를 생성, 관리함으로써 권한 없이 접근하였을 경우 이를 추적할 수 있도록 하여 이미지파일 보존 절차를 강화하였다. 대검찰청, 과학수사 실무 매뉴얼(2014), 제194쪽.

그러므로 디지털 데이터가 압수의 대상이 되는지 여부와 관계없이, 사건과 관련된 디지털 데이터를 출력, 복사, 복제했을 때 압수·수색 영장의 집행이 종료되었으므로, 그 이후 시스템에 디지털 압수물을 업로드 하는 행위는 집행 종료 후 취약한 디지털 데이터에 대한 원형보존조치[137]나 디지털 압수물을 수사에 활용하는 임의수사[138]에 해당한다고 하겠다.

제6절 일선 수사부서에서의 검색, 출력, 복제

디지털 압수물의 색인이 완료되면 일선 수사팀은 통합디지털증거분석시스템(IDEAS)을 통하여 법정에 증거로 사용할 수 있는 디지털 압수물을 검색한다. IDEAS는 일반 문서 파일 뿐 아니라, 메일, 결재 시스템, 회계 시스템, 계좌내역, 모바일, 통화내역[139] 등 이종의 형태의 디지털 데이터를 통합적으로 분석할 수 있도록 구현한 시스템이다. 수사팀은 IDEAS를 통하여 증거로 제출할 만한 디지털 데이터를 선별하여 출력하거나, 복제하여 증거로 제출한다. IDEAS의 색인된 디지털 압수물은 일정 시간이 경과하면, 자동으로 삭제된다.[140]

제7절 사건 종료 후 디지털 압수물의 처리

기소하여 판결의 확정, 불기소하는 등 사건에 대하여 종결되거나 공소제기전이더라도 압수를 계속할 필요가 없다고 인정되는 압수물의 경우 소유자 등의 청구가 있는 때에는 환부 또는 가환부 하여야 한다.[141] 그리고 위험 발생의 우려가 있거나 법령상 생산·제조·소지·소유 또는 유통이 금지된 압수물로서 부패의 염려가 있거나 보관하기 어려운 압수물에 대한 폐기하여야 한다.[142] 그러므로 디지털 압수물도 실제

137) 이후 단계에서의 시스템이 백업을 하는 등 디지털 압수물을 복제하는 행위는 원형보조조치에 해당한다.
138) 수사팀에서 디지털 압수물을 증거로 제출하기 위하여 검색, 출력, 복제하는 행위도 디지털 압수물을 수사에 활용하는 임의수사라고 할 것이다.
139) 계좌내역과 통화내역의 경우 엄밀히 보면, 압수·수색 영장을 금융회사나 통신사에 직접 집행하여 전달받기 때문에 디지털 포렌식이라 보기 어려운 측면이 있으나, 디지털 데이터 형태로 되어 있고, 다른 디지털 압수물과 관련된 부분이 많아 통합적으로 검색, 분석한다면 수사의 효율성을 증대시킬 수 있어 포함하였다.
140) 현재 기본적으로 보관하는 기간을 50일이고, 일선 수사부서에서 기간을 연장할 수 있다.
141) 형사소송법 제218조 제1항 “검사는 사본을 확보한 경우 등 압수를 계속할 필요가 없다고 인정되는 압수물 및 증거에 사용할 압수물에 대하여 공소제기 전이라도 소유자, 소지자, 보관자 또는 제출인의 청구가 있는 때에는 환부 또는 가환부하여야 한다.”

로 증거로 사용하지 않는 등 압수를 계속할 필요가 없을 경우 환부 또는 가환부를 하여야 한다. 하지만, 디지털 데이터의 경우 환부 또는 가환부가 의미가 있는지 의문이다. 현장에서 사건과 관련된 디지털 데이터를 출력, 복제하였기 때문에 이에 대한 원래의 디지털 데이터는 피압수자가 소유 및 점유하고 있기 때문이다. 그러므로 불필요한 디지털 압수물은 수사기관에서 삭제, 폐기함이 타당하다고 생각된다.

그러나 현재 압수물에 대한 형사소송법 규정은 위에서 본 바와 같이 유체물을 전제로 한 규정으로 폐기 사유가 무형의 디지털 데이터에 대하여 바로 적용하기 어렵다.

한편, 증거 제출은 대부분 출력하여 수사보고서와 함께 기록에 편철하거나 CD/DVD로 복제하여 기록에 편철하는 방법으로 이루어진다. 이 경우 판결문에 디지털 압수물에 대한 별도의 처분이 없고, 검사도 이에 대하여 별도의 처분이 없는 경우가 대부분이어서 검찰은 사건 기록물에 준하는 기간으로 압수한 디지털 데이터를 보관, 관리하고 있다.

그러나 디지털 압수물은 사건 기록물과는 너무나 다른 형태와 특성이 있어 위와 같이 관리하는 것은 문제가 있다고 할 것이다. 그러므로 압수한 디지털 데이터에 대한 관리 및 폐기에 대한 구체적인 규정이 절실히 필요하다.

제8절 예외적인 경우 디지털 포렌식 절차

압수·수색 현장에서 사건과 관련된 디지털 데이터를 출력, 복제하는 것이 불가능하거나 곤란한 경우에는 압수·수색 준비, 압수·수색 현장에서 정보저장매체 수색, 정보저장매체에서 사건과 관련된 디지털 데이터 조사, 이미지 파일, 복제본 디스크의 생성, 정보저장매체 전부 복제, 이미징 확인서 작성, 디지털 압수물 시스템에 업로드, 업로드한 디지털 압수물 다운로드 받아 분석, 분석한 디지털 압수물 업로드,

142) 형사소송법 제130조(압수물의 보관과 폐기) ① 운반 또는 보관에 불편한 압수물에 관하여는 간수자를 두거나 소유자 또는 적당한 자의 승낙을 얻어 보관하게 할 수 있다.

② 위험발생의 염려가 있는 압수물은 폐기할 수 있다.

③ 법령상 생산·제조·소지·소유 또는 유통이 금지된 압수물로서 부패의 염려가 있거나 보관하기 어려운 압수물은 소유자 등 권한 있는 자의 동의를 받아 폐기할 수 있다.

색인, 일선 수사부서에서의 검색, 출력, 복제, 사건 종료 후 압수물의 처리의 절차로 진행된다.

이 경우에도 압수·수색 준비, 압수·수색 현장에서 정보저장매체 수색, 정보저장매체에서 사건과 관련된 디지털 데이터 조사, 색인, 일선 수사팀에서의 검색, 출력, 복제, 사건 종료 후 디지털 압수물의 처리의 절차는 앞서 본 원칙적인 디지털 포렌식 절차와 동일하다.

아래에서는 예외적인 경우 고유한 절차의 세부 내용과 관련 쟁점을 정보저장매체 자체를 압수하는 절차를 중심으로 논의해 보겠다.[143]

1. 예외적인 경우의 세부 절차[144]

가. 압수할 정보저장매체의 분리 및 저장매체·정보시스템 압수 확인서 작성

대상 정보저장매체의 시간 정보를 확인하고, 전원을 차단한 다음, 정보저장매체를 분리한다. 정보저장매체 이름 등을 기재한 '저장매체·정보시스템 압수 확인서'를 작성하여 피압수자 등에게 확인 및 서명을 받은 후 추후 이미지 파일 생성 과정에 참여할지 여부를 확인한다.[145]

그리고 분리한 정보저장매체를 봉인하여 디지털 포렌식 사무실 등 제3의 장소로 안전하게 이동한다.

---

143) 예외적인 경우에는 현장에서 이미지 파일을 생성하는 방법과 정보저장매체 자체를 압수하는 방법이 있는데, 정보저장매체 자체를 압수하는 경우에도 해당 유체물인 정보저장매체를 분석하는 것이 아니라, 정보저장매체 전체에 대한 아미지 파일을 생성하여 분석하기 때문에 이미지 파일을 압수·수색 현장이 아닌 제3의 장소에서 생성하는지만 차이가 있지 실질적으로 차이가 없다.

144) 현장에서 정보저장매체 전부의 이미지 파일을 생성하는 경우는 '이미지 파일·복제본 디스크의 생성 및 저장매체 전부 복제·이미징 확인서 작성' 절차가 고유한 절차로 구체적으로 보면, 해당 정보저장매체의 시스템에 설정된 시간정보를 확인하고, 저장매체를 분리한 다음, 쓰기방지장치를 연결하여 디지털 포렌식 수사관의 현장용 디지털 포렌식 도구로 이미지 파일을 생성하거나 복제본 디스크를 생성한다. 이미지 파일이 생성되면, 이미지 파일명, 원래의 정보저장매체 이름, 이미지 파일에 대한 해시 값 등을 기재한 '저장매체 전부 복제·이미징 확인서'를 작성하여 피압수자 등에게 확인 및 서명을 받은 후 추후 디지털 데이터 추출 과정에 참여할지 여부를 확인한다.

145) 위 확인서를 2부를 사본하여 1부는 피압수자에게 교부하고, 다른 사본 1부는 디지털 포렌식 수사관이 보관하며, 원본은 수사팀 수사관에게 인계하고, 수사팀 수사관은 인계받은 확인서의 내용을 참고하여 압수목록을 작성해 피압수자에게 교부하는 것은 원칙적인 절차와 동일하다.

나. 이미지 파일 생성 및 업로드와 정보저장매체의 환부, 가환부

압수한 정보저장매체는 디지털 포렌식 사무실로 운반하여 봉인을 해제한다. 봉인 해제 후 전 과정을 촬영하여 보관의 연속성 및 무결성을 유지하고, GPS 시계로 봉인해제와 이미지 파일 생성 과정 사이의 시간을 확인한다.[146]

봉인을 해제하면, 정보저장매체의 제조사, 모델명, 시리얼번호 등 정보를 확인하여, 디지털수사통합업무관리시스템(DFISII)에 입력한다.

해당 정보저장매체를 쓰기방지장치를 하여 이미지 파일을 생성하고, 이를 위 시스템에 업로드한 다음, 해당 정보저장매체를 재봉인하여 수사부서에 인계하면,[147] 수사팀은 이를 피압수자에게 환부 또는 가환부를 한다.

다. 이미지 파일 분석, 분석한 디지털 데이터 업로드

디지털 포렌식 수사관은 업로드한 이미지 파일을 다운로드 받아, 삭제 파일 복원, 사건과 관련된 파일 조사, 관련 로그 기록 확인 등의 분석 과정을 거쳐 사건과 관련된 디지털 데이터를 선별하면, 이를 시스템에 업로드한다.

2. 형사소송법 제106조 제3항 단서의 해석 문제

가. 문제점

형사소송법 제106조 제3항은 "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."고 규정하고 있고, 동법 제219조에서 수사기관의 압수에도 준용하고 있다. 비록 형사소송법은 디지털 데이터에 대하여 압수의 대상이라는 명문의 규정은 없지만, 압수의 대상이 된다는

146) 대검 예규 제616호 디지털 증거 수집 및 분석 규정 제20조. 정보저장매체등의 봉인 해제, 이미지파일로 복제, 디지털수사통합업무관리시스템에 등록하는 과정은 사진을 촬영하는 등 디지털 증거의 진정성, 무결성, 신뢰성 유지를 위하여 필요한 조치를 취하여야 한다.

147) 대검찰청, 과학수사 실무 매뉴얼(2014) 제179-180쪽.

점은 앞에서 살펴보았다. 문제는 동조 제3항 단서에서 “정보저장매체등을 압수할 수 있다.”라고 규정하고 있는데, 이에 대하여 예외적 상황에서 정보저장매체를 압수하면 압수가 종료되는지 여부다. 동조 해석론에 따라 압수 이후의 단계에서 영장주의가 적용되는지 여부가 결정되는 것으로 특히 수사기관의 입장에서는 매우 중요한 문제가 된다.

나. 견해의 대립

이에 대하여 정보저장매체 자체의 압수로 압수가 종료된 것이 아니라는 견해와 종료되었다는 견해가 대립한다.

먼저 압수·수색의 대상은 디지털 데이터이며, 압수·수색 현장에서 정보저장매체를 압수하는 행위는 제3의 장소에서 압수의 대상인 디지털 데이터를 출력, 복제하기 위한 압수·수색 영장 집행 과정의 일환이라는 견해가 있다.[148] 이 견해는 정보저장매체에서 관련 디지털 데이터를 최종적으로 복사 또는 출력하였을 때 압수·수색 영장의 집행이 종료된다고 본다.

한편, 압수·수색의 대상은 정보저장매체 등의 유체물이므로, 피압수자의 점유를 배제하고 수사기관이 점유를 하게 됨으로서 압수·수색 영장의 집행이 종료되었다고 보는 견해가 있다.[149]

다. 법원의 태도

법원은 전교조 압수·수색 준항고기각 결정에 대한 재항고 결정[150]에서 “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 문서 출력 또는 파일복사 대상 역시 혐의사실과 관련된 부분으로 한정되어야 하는 것은 헌법 제12조 제1항, 제3항, 형사소송법 제114조, 제215조의 적법절차 및 영장주의

148) 이숙연, “디지털증거의 압수수색”, 법원도서관, 형사법 실무연구(2011), 제687쪽.
149) 전승수, “디지털 정보에 대한 압수수색영장의 집행”, 법조(2012. 7.), 제262쪽.
150) 대법원 2011. 5. 26.자 2009모1190결정.

원칙상 당연하다.”고 판시하여 정보저장매체 자체의 압수는 압수·수색 영장 집행의 일환으로 디지털 데이터에 대한 압수는 종료된 것으로 보지 않고 있는 입장이다.

라. 검토

(1) 압수방법의 문제

생각건대 위 견해의 대립은 디지털 데이터를 압수의 대상으로 보는지 여부가 정보저장매체의 압수를 어떻게 보는지 논리적인 연관성이 있는 것으로 논거를 제시하고 있다. 하지만 디지털 데이터를 압수의 대상으로 보는가에 따라 논리 필연적으로 견해가 나뉘는 것은 아니라고 본다.

법원과 압수·수색 영장 집행의 일환이라는 견해는 디지털 데이터가 압수의 대상이므로, 디지털 데이터를 저장하고 있는 유체물인 정보저장매체 자체는 압수물이 아니라는 전제에서 판단하고 있음에도 불구하고, 그러면서도 경우에 따라 정보저장매체 자체의 압수를 인정하고 있고[151], 압수·수색 영장의 집행이 종료되었다는 견해도 결국 정보저장매체가 아니라 정보저장매체에 저장된 디지털 데이터를 분석하여 출력이나 복제하여 증거로 제출한다고 하고 있다.

그러므로 디지털 데이터의 압수의 대상 여부와 동항은 관련이 없다고 하겠다. 동항의 문제는 디지털 데이터에 대한 압수방법을 어떻게 할 것인지에 대한 논의이다.

(2) 비례의 원칙 적용

디지털 데이터의 압수도 가장 덜 침익적인 방법으로 집행하여야 하는 것은 비례의 원칙상 당연하다. 따라서 디지털 데이터를 압수하는 방법은 비례의 원칙에 의하여 원칙적으로 ① 압수·수색 현장에서 사건과 관련 있는 디지털 데이터 출력, 복제하고, 압수·수색 현장에서 출력, 복제하는 방법이 불가능하거나 압수의 목적을 달성

151) 이숙연, “전자정보에 대한 압수수색과 기본권, 그리고 영장주의에 관하여” 헌법학연구 제18권 제1호(2012. 3.), 제24쪽. 위 논문에서 디지털 데이터에 대한 압수·수색의 방법으로 법익침해가 적은 것부터 수색·검증, 출력·복사, 복제(이미징), 저장매체 자체의 압수를 소개하고 있고, “피압수자 등의 방해나 비협조로 현장에서 출력이나 복제본의 작성에 의한 압수·수색이 불가능하거나, 전자증거의 인멸이나 폐기의 정황이 있어 출력이나 복사의 방법으로는 압수·수색의 목적을 달성할 수 없는 경우 저장매체 자체의 압수라는 방법에 의하여 압수·수색 할 수 있을 것이다.”라고 하여 정보저장매체 자체의 압수가 압수·수색 영장 집행의 일환이라는 자신의 견해와 모순된다.

할 수 없을 경우에는 ② 현장에서의 이미징하거나 ③ 정보저장매체 자체의 압수[152] 해야 한다. 동항은 디지털 데이터의 압수 방법에 대하여 비례의 원칙을 규정한 것이라고 할 것이다. 동항은 과거 정보저장매체 자체를 압수하여 범죄와 관련이 없는 디지털 데이터까지 수사기관이 압수하여 별개 사건의 증거로 사용하거나 프라이버시 침해 등 피압수자의 권리를 침해할 우려가 있음에 대한 반성적인 규정이라고 할 것이다.

(3) 소결

동항을 디지털 데이터의 압수의 방법에 관한 비례의 원칙을 천명한 규정으로 본다면, 예외적으로 정보저장매체 자체를 압수할 수도 있다는 것이고, 이 경우에는 정보저장매체 자체의 압수로 디지털 데이터에 대한 압수는 종료하는 것이다.

물론 동항 단서의 경우 법원의 입장과 압수·수색 영장 집행의 일환이라는 견해는 피압수자의 권리를 보호하기 위한 해석으로 볼 수 있다. 그러나 동조 단서는 수사기관의 압수에 대한 과도한 제약을 가하고, "다만, 범위를 정하여 출력 또는 복제하는 방법이 불가능 하거나 압수의 목적을 달성하기 현저히 곤란하다고 인정되는 때에는 정보저장매체 등을 압수할 수 있다."고 하여 정보저장매체의 압수를 디지털 데이터의 압수 방법 중 하나로 명확하게 보고 있는 점[153], 압수·수색의 종료시점에 관하여 디지털 데이터의 압수·수색이라고 하여 통상적인 압수·수색의 종료시기와 달리 해석할 이유나 형사소송법상의 근거도 없고, 디지털 데이터도 불가시성으로 인하여 보이지 않을 뿐, 정보저장매체에 저장되어 있고 이를 수사시관이 점유가 확보하면, 압수·수색은 종료한 것으로 보면 되고, 이는 디지털 데이터 압수 방법의 원칙인 출력 또는 복제의 경우도 출력물, 복제물이 수사기관에게 점유가 이전되면 압수·수색은 종료한 것으로 보면 되므로, 유체물의 압수와 달리 취급할 이유가 없다는 점[154], 압수·수색 영장 집행이 종료되지 않았다고 해석한다면, 동일한 장소를 재차

152) ②와 ③의 차이는 정보저장매체 자체를 현장에서 이동하는지 여부이다. 한편 ②의 경우 현장에서의 이미지 파일 생성이 상당한 시간이 소요될 것으로 예상되어 현장에서 하는 것이 오히려 피압수자의 권리를 침해하는 경우에는 ③의 경우보다 더 침익적인 경우도 있을 수 있다.

153) 이에 대하여 압수·수색 영장 집행의 일환으로 보고 있는 법원의 견해는 형사소송법 개정 이전의 것으로 향후 입장의 변경이 필요하다.

154) 조광훈, "형사소송법 제106조의 쟁점과 개정안 검토", 법조 제694호(2014. 7), 제218쪽. 박혁수 "디지털 정보에 대한 압수수색 실무 상 문제점" 제12회 대법원 형사실무연구회 특별 심포지엄 자유토론문(2012. 12. 17.), 제13쪽.

집행하더라도 유효한 영장의 집행이 되고[155][156], 압수·수색 장소가 영장에 기재되지 않은 수사기관의 사무실 등으로 확장될 수 있고[157], 분석 기간도 영장 집행기간에 포함된다면, 영장의 유효기간이 무의미해지는 문제 등 영장주의의 전반에 모순되는 문제가 발생할 수 있다는 점, 수사기관에 의하여 압수·수색 영장의 집행이 계속되어 광범위한 압수·수색을 허용하게 되고, 이는 결국 수사기관에 의하여 압수의 집행이 확대되어 포괄적이고 광범위한 기본권의 침해를 발생시킬 우려가 있다는 점[158] 등을 고려하면, 현장에서 범위를 정하여 출력 복제가 불가능 하거나, 압수의 목적을 달성하기에 현저히 곤란하다고 인정되는 예외적인 경우에는 정보저장매체 자체를 압수하는 방법으로 디지털 데이터를 압수하는 것이 허용된다고 볼 것이다.

따라서 이렇게 해석할 경우 수사기관 사무실에서 정보저장매체 전체에 대한 이미지 파일 생성행위, 이를 서버에 업로드 하는 행위, 이미지 파일 분석하는 행위 등은 압수·수색 영장 집행 종료 이후의 문제이므로 영장주의의 적용을 받는 것은 아닌 임의수사라고 할 것이다.[159]

한편, 법원의 전교조 압수·수색 준항고 기각 결정에 대한 재항고 결정[160]은 형사소송법 개정 이전의 결정이나, 개정 이후에도 법원은 위 결정과 같은 입장을 여전히 고수하고 있다. 아마도 위 결정의 태도가 개정 형사소송법에 그대로 반영되었다는 판단에서 입장을 변경하지 않고 있는 것으로 보인다. 하지만, 형사소송법 제106

---

155) 대법원1999. 12. 1, 99모161 결정. 압수·수색 영장을 집행하면, 영장의 유효기간이 남아 있다 하더라도 다시 동일한 장소에서 동일한 영장으로 압수·수색을 할 수는 없다. 이는 디지털 데이터의 압수의 경우도 달리 볼 수 없는 영장주의의 원칙이다.

156) 조광훈, "형사소송법 제106조의 쟁점과 개정안 검토", 법조 제694호(2014. 7), 제219쪽. 수사기관이 정보저장매체를 수사기관의 사무실로 압수한 다음, 분석하였으나 사건과 관련된 디지털 데이터가 없는 경우 다시 집행하더라도 유효한 영장 집행으로 볼 수도 있기 때문에 동일한 압수·수색 영장을 무한정으로 같은 장소에서 계속 집행할 수 있다는 해석도 가능하게 만든다.

157) 조광훈, "형사소송법 제106조의 쟁점과 개정안 검토", 법조 제694호(2014. 7), 제219쪽.

158) 정보저장매체의 대용량화, 기술의 발달로 정보저장매체에 저장되어 있는 디지털 데이터에 사건과 관련된 데이터를 조사, 분석하는데, 단시간에 끝내지 못하는 경우가 많아, 피압수자는 장기간으로 계속하여 수사기관의 압수·수색을 받아야 할 경우가 있을 수 있다.

159) 박혁수 "디지털 정보에 대한 압수·수색 실무 상 문제점" 제12회 대법원 형사실무연구회 특별 심포지엄 자유토론문(2012. 12. 17.), 제26쪽. 위 법원 결정의 내용을 문언 그대로 기계적으로 적용하면, 디지털 포렌식 수사관이 시스템에 업로드 하는 행위는 영장주의에 위배되는 위법한 압수 처분이 된다. 그러나 이러한 기계적 해석은 우선 기존의 법원의 영장 실무와 수사기관의 압수·수색 실무에 정면으로 반한다는 문제가 있다. 위와 같이 해석하면, 정보저장매체 자체를 수사기관의 사무실로 가져온 이후에는 **오로지** 그 원본만을 가지고 분석, 추출, 검색 등 일련의 증거분석을 모두 마쳐야 하는 결론에 이르는데, 이는 최근 디지털 데이터의 대량화에 정면으로 반하는 것이며, 최종적으로 혐의사실과 관련된 데이터를 출력 또는 복사하는 행위를 제외한 나머지 일체의 복사 또는 출력 행위는 모두 영장주의에 위배되는 위법한 처분이 되는바, 디지털 데이터의 취약성 따른 조치와 증거능력을 인정받기 위한 무결성을 위한 조치도 위법한 처분이 되어 문제된다.

160) 대법원 2011. 5. 26.자 2009모1190결정.

조 제3항 단서에서 명문으로 정보저장매체의 압수를 인정하고 있는바, 이에 대한 판례의 변경이 필요하다.

3. 형사소송법 제106조 제3항의 개정필요성

가. 문제점

한편, 동항은 디지털 데이터에 대한 압수방법에 대하여 원칙과 예외로 규정하고 있는바, 압수·수색 현장에서 수사기관이 방대한 양의 디지털 데이터 중에서 사건과 관련된 데이터를 범위를 정하여 출력, 복제하는 것은 이미 사건의 내용을 완전히 파악하지 못하면 불가능하므로 이 규정이 압수·수색의 목적 달성이라는 의미에서 현실적으로 준수될 수 있는지에 대하여 의문을 제기하면서, 원칙과 예외의 규정 형식 자체가 문제가 있어 다시 개정할 필요가 있다는 의견의 목소리가 커지고 있다.

나. 입법례

(1) 미국 연방형사소송규칙 제41조(e)(2)(B)

'전자적 저장정보(Electronically Stored Information)'의 압수·수색은 "전자적 저장정보가 있는 전자적 저장매체(electronic storage media)를 압수"하거나 "전자적 저장정보를 압수"하거나 "전자적 저장정보의 복제본(copying of electronically stored information)을 압수" 할 수 있도록 규정[161]하고 있지만, 압수방법에 대하여 우선순위가 있는 것은 아니다.

(2) EU 사이버범죄 방지협약

동 협약 제19조는 저장된 컴퓨터 자료에 대한 압수·수색과 관련하여 컴퓨터 자료를 법집행기관이 압수하거나 확보할 수 있도록 그 권한을 부여하는데 필요한 입법

161) Rule 41. Search and Seizure
(e) Issuing the Warrant.
(2) Contents of the Warrant.
(B) Warrant Seeking Electronically Stored Information. A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.

및 부수조치를 취하도록 규정[162]하고 있다. 이 경우 동 조치에는 컴퓨터 시스템과 컴퓨터 저장매체를 압수·확보할 권한, 컴퓨터 자료에 대한 사본(a copy)을 작성·보유할 권한, 저장된 컴퓨터 자료에 대한 무결성을 유지할 권한 등이 해당한다고 하고, 압수 방법에 있어 원칙과 예외로 나누지는 않고 있다.

다. 견해의 대립

(1) 개정 필요설[163]

동항의 개정이 필요하다는 견해는 "우리 형사소송법과 같은 원칙, 예외 형식의 입법례가 없다는 점, 어차피 압수·수색은 피압수자에게 침익적이지만, 헌법과 법률이 정한 절차에 따라 비례의 원칙을 준수하면서 집행하는 압수·수색은 합법적인 법집행이라는 점, 디지털 데이터의 압수는 현실적으로 현장에서 종료하기 어렵고, 현장 상황이 수시로 변하므로 이에 대한 탄력적 대응이 어렵다는 점, 동조의 적용을 따를 경우 디지털 데이터에 대한 증거능력을 인정하기 위하여 필요한 요건인 동일성을 충족시키기 어렵다는 점 등의 근거를 제시"하면서, 디지털 데이터의 압수 방법을 '병렬식'으로 나열하는 입법이 상당하다고 주장한다.

---

162) Article 19 – Search and seizure of stored computer data
1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:
a a computer system or part of it and computer data stored therein; and
b a computer-data storage medium in which computer data may be stored in its territory.
2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.
3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:
a seize or similarly secure a computer system or part of it or a computer-data storage medium;
b make and retain a copy of those computer data;
c maintain the integrity of the relevant stored computer data;
d render inaccessible or remove those computer data in the accessed computer system.
4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.
5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

163) 노명선, "디지털증거 압수수색에 관한 법률의 문제점과 개선방안"의 토론문, 2012년 디지털증거 압수수색에 관한 개정법률(안) 공청회, 제16-17쪽.

(2) 개정 불요설[164]

현행 형사소송법 제106조 제3항의 규정의 개정이 필요 없다는 견해는 “오늘날 디지털 데이터의 압수는 국민의 삶을 파괴하는 정도에 이르는 중대한 기본권 침해 영역에 해당하므로, 정보저장매체가 있는 현장에서 주관적, 객관적, 시간적으로 관련된 디지털 데이터만을 압수하는 것을 원칙으로 하고, 그것이 불가능한 경우에 한해 예외적으로 정보저장매체 자체를 압수할 수 있다고 해야 한다”고 주장하면서, 압수의 목적을 달성하기에 현저히 곤란한 경우를 아주 제한적으로 허용해야 한다고 한다.

라. 검토

생각건대 최근에는 디지털 데이터가 증거로서 중요한 사례가 많아 동항의 규정형식으로 인하여 수사기관의 입장에서는 수사에 어려움을 겪게 될 수 있다. 하지만 수사기관의 수사도 국민의 기본권을 지나치게 침해하면서 행하여 질 수 없음은 헌법상 자명하다. 미국, 유럽 등 경제적 선진국의 입법례가 없다고 하여 이를 개정해야 할 이유도 없다 할 것이다.

동항은 수사기관의 디지털 데이터의 압수·수색에 대하여 국민의 기본권을 보장하기 위한 규정으로 볼 수 있다. 그리고 동항과 같은 규정이 디지털 증거의 압수·수색 방법을 병렬적으로 하는 규정보다 국민의 기본권을 더욱 보장하는 방법이기 때문이다. 또한 원칙적으로 압수·수색 현장에서 출력, 복제하는 방법으로 디지털 데이터를 압수하고, 이러한 방법이 불가능하거나 수사의 목적을 달성하기 곤란한 경우라는 사정이 있을 경우 예외적으로 정보저장매체 자체를 압수하는 것은 수사의 목적 달성에 국민의 기본권 침해 여부에 대하여 비례의 원칙을 적용한 것으로, 동항에 대한 개정 논의 보다는 해석론의 연구가 더욱 절실하다.

164) 오기두, “디지털증거 압수수색에 관한 법률의 문제점과 개선방안”의 토론문, 2012년 디지털증거 압수수색에 관한 개정법률(안) 공청회, 제49-50쪽.

4. 형사소송법 제106조 제3항 단서의 판단기준

가. 문제점

동항이 기본권을 보장하는데, 더 적합한 규정이라는 것은 앞에서 살펴보았다. 하지만, 출력, 복제의 원칙, 예외적 정보저장매체의 압수라는 동항을 정보저장매체의 압수 원칙과 출력, 복제의 예외적 압수로 변칙적으로 적용할 수 있는 문제가 생긴다. 이는 누가, 언제, 어떠한 판단 기준으로 예외적인 상황이라고 판단하느냐하는 동항의 해석이다.

나. 판단기준

디지털 데이터 압수·수색 영장의 별지의 내용과 판례에서 몇 가지 판단 기준을 알아볼 수 있다.

영장 별지의 압수방법의 제한[165]에는 집행 현장에서 복제할 수 있는 경우는 출력·복사에 의한 집행이 불가능하거나, 압수의 목적을 달성하기에 현저히 곤란한 경우로 구체적으로 1. 피압수자 등이 협조하지 않거나, 협조를 기대할 수 없는 경우, 2. 혐의사실과 관련될 개연성이 있는 전자정보가 삭제, 폐기된 정황이 발견되는 경우, 3. 출력·복사에 의한 집행이 피압수자 등의 영업활동이나 사생활의 평온을 침해하는 경우, 4. 기타 이에 준하는 경우

집행현장에서의 저장매체의 복제가 불가능하거나 현저히 곤란하여 저장매체의 원본 반출이 허용되는 경우로 1. 집행현장에서의 하드카피·이미징이 물리적, 기술적으로 불가능하거나 극히 곤란한 경우, 2. 하드카피·이미징에 의한 집행이 피압수자 등의 영업활동이나 사생활의 평온을 현저히 침해하는 경우, 3. 기타 이에 준하는 경우를 들고 있다.[166][167]

---

165) 이숙연, "전자정보에 대한 압수수색과 기본권, 그리고 영장주의에 관하여", 헌법학연구 제18권 제1호(2012. 3.), 제32-33쪽.

166) 대법원 2011. 5. 26. 선고, 2009모1190 결정은 ① 압수·수색 장소에 증거인멸의 정황이 있었던 점, ② 피압수자의 수가 70,000여 명에 달하고 피의사실과 관련된 인원이 17,000여명에 달했던 점, ③ 영장 집행에 현장에 다수 피압수자가 있었던 점, ④ 피압수자가 영장 집행에 적대시하고 다른 조합원이 현장에 몰려온 점, ⑤ 영장집행 당시 서버에 전원 공급이 되지 않았다고 하다가 서버와 컴퓨터의 본체를 압수하려고 할 경우에 비로소 전원 공급이 가능하다고 말한 점, ⑥ 사법경찰관이 하드카피에 필요한 장비 등을 소지하고 있었던 점 등을 들고 있는데, 이는 결국 위의 영장 별지의 압수방법의 제한이 구체적 상황에 적용된 것이라 할 수 있다.

167) 영장 별지에서 압수·수색 형장에서의 복제와 정보저장매체의 반출이 허용되는 경우를 분리한 것은 압수·수색 현장에서의 복제가 정보저장매체의 반출보다 피압수자의 권리가 덜 침익적이라는 판단에서 나눈 것으로

한편 정보저장매체의 압수에 대한 예외적 집행의 허용사정으로 1. 영장에 예외적 집행방법이 기재되어있는지 여부 2. 영장에 압수할 대상이 기재되어 있는지 여부 3. 증거인멸의 정황 4. 압수·수색 대상물의 수량 5. 압수·수색 대상자의 수 6. 압수·수색할 내용의 수량 7. 피압수자의 비협조 정도 8. 압수·수색 장소의 전산시스템의 사정 9. 수사관의 현장 포렌식 장비 구비 정도 10. 현장 포렌식 수사관의 인원 11. 암호화의 여부 12. 전자정보의 삭제 정도 13. 현장에서 전자정보를 분리할 경우, 전자정보와 저장매체의 손상을 초래하는지 여부 14. 현장에서 전자정보를 분리할 경우 그 분리로 인해 압수의 목적이 되는 증거로서의 가치에 손상을 가하는지 여부 등을 제시하는 견해[168]도 있다.

이에 대하여 대검찰청은 1. 몰수의 대상물인 경우 2. 인멸, 은닉, 삭제, 폐기된 정황이 있는 경우, 3. 당사자가 협조를 거부하는 경우, 4. 피압수자의 이익을 위한 경우, 5. 기타 압수 목적을 달성하기 어려운 경우 등을 들고 있다.[169]

보인다. 그러나 앞서 살펴보았듯이 반드시 그런 것이 아니고, 양자의 차이는 복제하는 장소가 현장인지 디지털 포렌식 사무실 등 제3의 장소인지 일 뿐이고, 정보저장매체를 압수하는 경우에도 복제 후 바로 반환 조치하므로 양자의 차이는 크지 않다고 하겠다.

168) 독고지은, “디지털 증거 압수수색에 대한 개정 형사소송법의 규제와 집행에 관한 연구 -영장 집행시 제기되는 쟁점을 중심으로-”, 법조(통권680호), 법조협회(2013. 5), 제293-294쪽.

169) 대검찰청, 과학수사 실무 매뉴얼(2014. 12.) 제177쪽.

(1) 몰수 대상물인 경우는 컴퓨터 또는 정보처리시스템이 금제품이거나 컴퓨터 또는 정보저장매체 등 물건 자체가 범행의 수단으로 사용된 경우로 예를 들면 게임 업소나 도박 사이트 등에서 불법으로 사용되는 컴퓨터나 서버가 이에 해당한다.

(2) 인멸·은닉·삭제·폐기된 정황이 있는 경우는 사건과 관련된 디지털 데이터가 인멸·은닉되었거나 삭제·폐기된 정황이 발견되었으나 현장에서 복원이 불가능한 경우로 예를 들면 ① 하드디스크가 손괴된 정황이 확인되어 저장매체를 수리하여 데이터를 복원할 필요가 있는 경우, ② 컴퓨터에서 디지털 데이터를 삭제하는 프로그램을 발견하였거나 구동한 흔적이 발견되는 등 의도적으로 디지털 데이터를 삭제한 정황이 확인되어 디지털 데이터를 복구하거나 증거를 인멸한 정황 등을 확인하기 위한 경우, ③ 압수·수색 이전에 하드디스크 포맷, OS 재설치, 드라이브 삭제 등을 이유로 협의사실과 관련된 기간에 생성되었던 디지털 데이터가 삭제된 것을 확인하였으나 현장에서 현장용 포렌식 도구로는 삭제된 파일을 복원할 수 없는 경우, ④ 의도적으로 컴퓨터에 대용량 파일을 다운받아 디지털 데이터를 삭제한 정황 등이 발견되어 이를 복구하기 위한 경우, ⑤ 하드디스크 또는 USB 등에 암호가 걸려 있어 현장 포렌식 도구로는 저장매체의 내용을 확인할 수 없는 경우 등이다.

(3) 협조 거부의 경우는 피압수자 등의 협조를 요청하였으나 협조하지 않거나 협조를 기대할 수 없는 경우로 예를 들면 ① 기업 등에서 사용하는 컴퓨터 시스템의 경우에는 기업의 보안정책에 의하여 대부분 ‘DRM’, USB 등 매체 접근 차단 등과 같은 기술적 보안 조치가 되어 있어 시스템을 관리하는 담당자의 협조를 얻어 보안 조치를 해제한 후 압수·수색을 수행하여야 하는데, 전산담당자 등이 협조하지 않거나, 협조를 기대할 수 없는 경우 ② 현장에서 피압수자 등이 압수·수색할 수 없을 정도의 소란을 일으켜 사실상 관련 디지털 데이터 선별 등의 방식으로 집행이 불가능한 경우 등이다.

(4) 피압수자의 이익을 위한 경우는 압수·수색 현장에서 사건과 관련된 디지털 데이터에 대하여 압수·수색하는 것이 피압수자 등의 영업활동이나 사생활의 평온을 침해하는 경우로 피압수자 등의 동의를 받아 압수하는 것이 바람직한데, 예를 들면 ① 압수·수색할 정보저장매체가 지나치게 많거나, 확인해야 할 협의사실이 많고 현장에서 협의사실과 관련된 디지털 데이터를 선별하는 것이 장시간이 소요되어 피압수자 등의 영업 활동이나 사생활의 평온을 침해할 수 있는 경우, ② 압수·수색 현장에 절대적 안정이 필요한 환자, 어린이, 노인 등이 있어 다수의 디지털 포렌식 수사관이 현장에서 협의사실과 관련된 파일을 선별하는 것이 적절하지 않는 경우 등이다.

(5) 기타 압수목적을 달성하기 어려운 경우는 압수·수색 현장에서 사건과 관련된 데이터를 압수하는 것으로는 압

다. 검토

위 견해들을 종합해 보면, 예외적인 상황에 대한 구체적인 판단기준으로는 1. 피압수자 등이 협조하지 않거나, 협조를 기대할 수 없는 경우, 2. 사건과 관련된 디지털 데이터가 삭제, 은닉, 폐기된 등 안티포렌식 정황이 발견되는 경우 3. 출력·복사, 현장에서의 이미징에 의한 집행이 피압수자 등의 영업활동이나 사생활의 평온을 침해하는 경우, 4. 집행현장에서의 하드카피·이미징이 물리적, 기술적으로 불가능하거나 극히 곤란한 경우 5. 기타 이에 준하는 경우를 기준으로 예외적인 상황을 판단함이 타당하다고 생각된다.[170]

5. 형사소송법 제106조 제3항 단서의 판단시기

앞서 형사소송법 제106조 제3항 단서의 판단기준을 검토하였다. 법원이 제시한 판단기준과 크게 차이가 없다 하겠다. 다만, 법원의 압수·수색 영장 발부시 첨부하는 별지를 보면 정보저장매체 자체를 압수해야 할 예외사항에 대하여 법원이 미리 알아야 한다는 입장인 듯하다. 즉 수사기관이 디지털 데이터에 대한 압수·수색 영장 청구시 미리 법원에 소명해야 한다는 것이다.

하지만, 제시한 판단기준은 대략적인 기준을 제시한 것에 불과하다. 이보다 더욱 구체적인 각각의 상황은 압수 현장에서 직접 확인하지 않으면, 알아내기 어려운 것으로 사전 조사를 통하여 알기에는 한계가 있다.[171] 그러므로 이에 대하여 수사기관이 소명하라고 하는 것은 불가능하다고 할 것이다.

위와 같이 예외적인 상황에 대한 기준은 '미리' '법원'이 '제시'하지만, 결국 압수·수색 '현장'에서의 예외적 사정의 '판단'은 '수사기관'이 인식하였거나, 신중한 중의를 기울였다면 알 수 있었던 사정을 종합적으로 고려하여 할 수 밖에 없다고 하겠다.[172] 이에 대하여 기본권 보장의 최후의 보루인 법원이 예외적 상황인지 여부를

수목적을 달성하기 어려운 경우로 예를 들면, 기술유출, 특허법 위반 등 사건의 경우 기술 도면 파일 등을 열어보기 위해서는 전문적인 지식과 별도의 뷰어 프로그램이 필요하기 때문에 현장용 포렌식 도구로는 파일의 내용을 확인하기 어려운 경우이다.

170) 한편, 예외적 상황의 판단기준으로 수사관의 현장 포렌식 장비 구비 정도, 현장 포렌식 수사관의 인원 등 수사기관의 주관적 사정을 포함하는 것은 국민의 기본권 보장의 측면에서 옳지 않다고 하겠다.

171) 증거인멸의 정황 등 안티 포렌식 여부, 피압수자의 인원과 피압수자의 비협조 여부, 저장매체의 암호화 여부 등은 압수·수색 현장에서 판단할 수 있을 뿐, 미리 알아내는 것은 사실상 불가능하다.

172) 전승수, "디지털 정보에 대한 압수수색영장의 집행", 법조 제670호(2012. 7.), 제267-268쪽.

사전에 판단하여야 한다고 한다[173]는 견해가 있으나, 예상할 수 있는 모든 예외적인 상황을 '미리' 영장 청구시 수사기관이 법원에 소명하여 법원이 예외적인 상황 여부를 판단, 이를 압수·수색 영장에 반영한다는 것은 사실상 불가능에 가깝다는 점, 사전에 법원이 판단한 예외적인 상황에 해당하지 않는데, 수사기관이 이를 넘어서 예외적인 상황으로 판단하여 정보저장매체 자체를 압수한 경우 수사기관에 대한 제재 수단이 마땅히 없다는 점에서 현실성이 없다고 하겠다.

또 위와 같은 판단 기준은 형사소송법 제106조 제3항의 해석상 충분히 예상할 수 있는 상황이라고 할 수 있고, 압수·수색 영장 별지에서 알 수 있듯이 예외적인 상황의 대강의 기준 정도를 미리 예상하거나 수사기관이 소명한 것을 법원이 압수·수색 영장에 기재하여 반영한 것으로 법원도 위 예외적인 상황에 대하여 제시하였을 뿐, 상황에 대한 판단은 수사기관에 부여한 것으로 해석할 수 있다.

다만, 수사기관이 예외적인 상황을 판단함에 있어 국민의 기본권 보호와 수사기관의 압수·수색 필요성의 소명책임에 부합할 수 있도록 신중을 기해야 함은 물론이다. 법원의 수사기관의 영장주의를 넘어선 수사기관의 압수·수색은 헌법상 영장주의와 적법절차의 원칙에 반하는 행위로서, 이로 인하여 확보된 증거는 위법수집증거배제법칙(형사소송법 제308조의2)에 의하여 증거능력이 부정될 것이다.

수사기관이 예외적인 상황을 자의적으로 해석하여 압수한 위법한 압수·수색에 대한 통제 절차는 압수에 대한 준항고 및 증거능력 판단[174]이 될 것이나, 법원은 판단 당시에 알려진 모든 객관적 사정을 종합적으로 고려하는 것이 아니라, 영장을 집행 당시 수사기관이 인식하였거나 신중한 주의를 기울였다면 인식할 수 있었던 사정을 종합적으로 고려하여 예외적 사정의 발생 여부를 판단함이 상당하다.[175]

---

173) 오기두, "디지털증거 압수수색에 관한 법률의 문제점과 개선방안"의 토론문, 2012년 디지털증거 압수수색에 관한 개정법률(안) 공청회, 제49쪽.

174) 이는 압수·수색의 목적 달성을 이루지 못하게 하는 가장 강력한 통제수단이라고 할 것이다.

175) 전승수, "디지털 정보에 대한 압수수색영장의 집행", 법조 제670호(2012. 7.), 제267-268쪽. 예를 들면, 수사기관이 현장에서 삭제 정황 발견 등으로 예외적 사정에 해당한다고 판단하여 정보저장매체 자체를 압수하였으나, 분석하여 복원 결과 사건과 관련된 디지털 데이터가 전혀 없는 경우, 사후적으로 객관적인 사정으로 종합하여 사건과 관련 없는 디지털 데이터의 압수로 압수·수색 영장 범위를 넘은 위법한 집행이라고 판단하는 것은 부당하기 때문이다.

6. 사건과 관련된 디지털 데이터를 조사하는 행위의 법적 성질

가. 문제점

정보저장매체에서 사건과 관련된 디지털 데이터를 조사하는 행위에 대하여 그 법적 성질이 무엇인지 논의가 있다. 디지털 데이터의 대량성과 비가독성으로 인하여, 정보저장매체를 찾아 압수하는 단계와 해당 정보저장매체에서 사건과 관련된 디지털 데이터를 인식하기 위한 행위의 단계를 절차적으로 구분하고 디지털 데이터를 인식하는 행위에 대하여 새로운 취급을 하려는 움직임이 있다. 이는 주로 정보저장매체 자체를 압수한 다음, 수사기관의 사무실 등으로 이전하여 관련 디지털 데이터를 찾는 실무와 관련하여 특히 문제되었다.[176] 주로 미국에서 발달한 이론으로 프라이버시 등 기본권 보호와 관련하여 수시기관의 정보저장매체에서 디지털 데이터를 찾는 행위에 제한을 두려고 한다.

나. 견해의 대립

(1) 수색론

디지털 증거도 프라이버시 관련 정보가 포함될 수 있는데, 이를 가시화 하려면 특별한 장비가 필요하기 때문에 일반 서류보다 더 큰 프라이버시 기대를 인정할 수 있고, 이 기대를 침범하는 것은 미국 수정헌법 제4조의 수색에 해당한다고 한다.[177] 이는 위 조항이 요구하는 합리성의 기준이나 특정성 기준으로 정보저장매체에서 사건과 관련된 디지털 데이터를 찾는 것을 제한하고자 한다.

(2) 2단계 수색론

IT 기술의 발달로 정보저장매체의 급격한 대용량화로 인하여 저장매체를 압수하여 수사기관 사무실에서 분석(forensic review)하는 경우가 많아지게 되었는데, 이 분석과정도 수색으로 파악하여 수색의 개념을 연장하였다.[178] 이는 다수의 법원에서

---

176) 예외적으로 정보저장매체 자체를 압수한 경우 압수·수색 영장의 집행은 정보저장매체 자체의 압수로 종료되었고, 그 이후 사건과 관련된 디지털 데이터를 조사하는 과정은 압수 종료 후 임의수사라 하겠다. 이에 대하여는 후술한다.

177) 이완규, “디지털 증거 압수수색과 관련성 개념의 해석”, 법조(2013.11.), 제30쪽. C. Ryan Reetz, “Warrant Requirement for Searches of Computerizes Information", 67 B.U.L.Rev 179, 197(1987), United States v. Marbury, 732 F. 2d, 390, 399-400(5th Cir. 1984), United States v. David, 756 F. Supp. 1385, 1390(D.D.N.1991), United States v. Chan, 830 F. Supp. 531, 534-535(D.N.D. Cal. 1993).

178) 이완규, “디지털 증거 압수수색과 관련성 개념의 해석”, 법조(2013.11.), 제31쪽. Orin S. Kerr, “Search Warrants in an Era of Digital Evidence”, 75 MISS. L. J. 85(2005).

도 받아들여 디지털 데이터의 수색을 2단계 수색(two-stage search)으로 파악하는 실무가 형성되었다.

(3) 정보 확인절차론

종래의 유체물에 대한 압수·수색 이론을 디지털 데이터의 압수·수색의 경우에도 그대로 적용하여 정보저장매체 자체를 압수하면, 압수 절차는 종료하고, 그 후 정보저장매체에 대하여 조사하는 과정은 압수물에서 정보를 확인하는 절차에 불과하므로 별도의 수색으로 파악할 필요가 없다는 견해이다.[179]

다. 검토

생각건대, 유체물도 정보를 포함하고 있다는 점에서 디지털 데이터 압수와 다르지 않고, 차이가 있다면 정보의 양 일 뿐이므로 정보저장매체도 그 자체로 하나의 물건이라고 하여야 한다. 정보저장매체에 저장된 디지털 데이터도 종이로 인쇄된 자료와 다르게 볼 이유가 없다고 할 수 있다.[180]

그리고 이렇게 해석하는 것이 현행 형사소송법 제106조 제3항의 문언에 충실한 해석[181]이라고 하겠다.[182]

7. 분석에 별도의 영장이 필요한지 여부

가. 문제점

정보저장매체 자체를 압수하면, 이에 대하여 이미지 파일을 생성한 다음, 이를 디지털수사통합업무관리시스템에 업로드하고, 업로드한 디지털 압수물을 디지털 포렌식 수사관이 자신의 PC로 다운로드하여 분석하고, 사건과 관련 있는 디지털 데이터가 있는지 조사한 다음, 압수할 디지털 데이터를 선별[183]한다. 분석은 파일 검색, 삭

179) 이완규, “디지털 증거 압수수색과 관련성 개념의 해석”, 법조(2013.11.), 제32쪽. Josh Goldfoot, "The Physical Computer and the Fourth Amendment", 16 Berkley J. Crim. L. 112, 157(2011).

180) 이완규, “디지털 증거 압수수색과 관련성 개념의 해석”, 법조(2013.11.), 제32-33쪽.

181) 위 견해에 의하면, 압수·수색 현장에서 정보저장매체에 저장된 데이터 중 사건과 관련된 디지털 데이터를 조사, 선별하여 출력, 복제하는 원칙적인 경우에는 출력, 복제할 때 압수가 종료된다고 한다. 위 디지털 압수물을 사후에 검색하는 것은 수색이 아니고 정보를 확인하는 과정이고, 디지털 데이터의 출력이나 복제는 피압수자의 소유자적 이해에 중요한 침해를 했기 때문에 이를 압수로 본다고 한다.

182) 위 검색의 법적성질은 정보저장매체 성질에 대한 논의와 연결되는데, 자세한 논의는 이완규, “디지털 증거 압수수색과 관련성 개념의 해석”, 법조(2013.11.), 제33-41쪽 참조.

제 파일 복원, 각 파일의 헥사 값 비교 등 신뢰성 있는 도구를 통하여 다양한 방법으로 한다. 이는 압수·수색 영장 집행 현장에서 정보저장매체를 조사하여 사건과 관련된 디지털 데이터를 출력, 복사하는 경우와 달리 압수·수색 영장 집행 이후의 임의수사라는 점에서 구별된다.

그런데 압수한 정보저장매체에 대한 이미지 파일을 생성하여 업로드하고, 이를 다운로드 받아 분석하여 사건과 관련된 파일을 선별하는 행위가 별도의 압수·수색 영장이 필요로 하는지 문제된다.

나. 견해의 대립

디지털 데이터에 대한 분석은 압수·수색 영장 집행 종료 이후에 행해지는 임의수사에 해당한다고 보는 견해가 있다. 이는 정보저장매체 자체의 압수로 압수·수색 영장의 집행은 종료되었음을 전제로 하여, "영장의 집행 이후에 새로이 물리적 강제력을 행사하거나 상대방의 의사를 제압하는 것이 아니라는 점, 압수물에 대하여 행하여지는 처분으로 새로운 법익이나 인권을 침해하지 아니하며, 상대방에게 법적 의무를 부과하지도 아니하는 점, 압수·수색영장의 청구 및 발부시에 미리 예정되어 있어 그 요건 등에 대하여 법원의 사전 심사를 받은 영역에 포함되는 점 등을 근거"[184]로 하고 있다.

반면, '정보저장매체 자체를 압수하는 단계는 아직 압수가 완료된 것이 아니며 그 저장매체를 검색하면서 사건과 관련성이 있는 것을 확인해 나가는 과정은 수색이라고 파악'하는 견해가 있다.[185]

한편, '디지털 데이터가 스크린에 현출되는 것과 같이 수사기관의 관찰에 현출되었을 때 수색, 검증이 시작된다고 보아 압수·수색 영장과 달리 새로운 수색·검증 영장을 받아야' 한다는 견해[186]가 있다. 이는 압수·수색 영장의 집행 이후에 수사기관

183) 편의상 위 전 과정을 디지털 데이터 분석 과정이라고 하겠다.
184) 전승수, "형사절차상 디지털 증거의 압수수색 및 증거능력에 관한 연구" 서울대학교 대학원 법학과 박사학위논문, 제86쪽.
185) 오기두, "형사절차상 컴퓨터 관련 증거의 수집 및 이용에 관한 연구", 박사학위논문, 서울대학교 대학원 (1997), 제76-81쪽.
186) 조국, "컴퓨터 전자기록에 대한 대물적 강제처분의 해석론적 쟁점", 한국형사정책학회, 형사정책(제22권 제1호)(2010. 7.), 제109쪽.

의 시설 내에서 이루어지는 정보저장매체에 대한 관련 디지털 데이터의 검색[187] 등이 수색·검증이라고 전제로, 피의자나 변호인의 참여 없이 분석한 디지털 데이터는 형사소송법 제121조, 제122조, 제145조를 위반하여 증거능력이 부정된다고 한다.

다. 법원의 태도

법원은 전교조 압수·수색 준항고 기각 결정에 대한 재항고 결정[188]에서 "저장 매체 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 경우의 문서출력 또는 파일 복사의 대상 역시 혐의사실과 관련된 부분으로 한정되어야 함은 헌법 제12조 제1항, 제3항, 형사소송법 제114조, 제215조의 적법절차 및 영장주의의 원칙상 당연하다. 그러므로 수사기관 사무실 등으로 옮긴 저장매체에서 범죄 혐의와의 관련성에 대한 구분 없이 저장된 전자정보 중 임의로 문서출력 혹은 파일복사를 하는 행위는 특별한 사정이 없는 한 영장주의 등 원칙에 반하는 위법한 집행이 된다."고 판시하여 압수·수색 영장 집행의 일환으로 보고 있다.

라. 검토

수색이라는 견해나 법원의 태도는 정보저장매체에 저장된 디지털 데이터의 대량성으로 분석 과정에서 디지털 데이터를 확인하는 대상을 사건과 관련성이 있는 것으로 제한하여 피압수자의 권리를 보호하기 위함인 듯하다.

하지만, 이는 디지털 데이터의 비가시성으로 인하여 현실과 부합되지 않는다. 왜냐하면, 해당 디지털 데이터가 사건과 관련된 것인지를 파악하려면, 그 데이터를 검색하여 가시화할 수밖에 없기 때문이다. 그래서 수색이라는 견해도 수색 착수 전에는 사건과 관련된 디지털 데이터인지 확인할 수 없으므로 정보저장매체 자체를 검색하는 것을 허용하고 있다.[189]

---

187) '검색'이라고 표현하고 있으나, 정보저장매체에서 사건과 관련된 디지털 데이터를 찾는 방법이 검색만이 있는 것은 아니므로, '조사'가 적합한 표현이라고 하겠다.
188) 대법원 2011. 5. 26.자 2009모1190결정.
189) 오기두, "형사절차상 컴퓨터 관련 증거의 수집 및 이용에 관한 연구", 서울대학교 대학원 박사학위논문 (1997), 제80쪽.

생각건대 앞서 살펴본 바와 같이 디지털 데이터의 압수는 예외적인 상황의 경우 형사소송법 제106조 제3항 단서에 의하여 정보저장매체 자체를 압수할 수 있으므로, 정보저장매체 자체를 압수하면, 압수·수색 영장의 집행은 종료되었다고 하겠다. 그러므로 디지털 데이터의 분석행위는 압수·수색 영장 집행 종료 이후의 임의수사라고 할 것이고,[190] 피압수자의 권리 보호는 수사시관의 비례의 원칙 준수 및 법원의 디지털 압수물의 증거능력 제한으로 충분히 가능하다고 하겠다.

8. 참여의 문제

가. 문제점

법원은 전교조 압수·수색 준항고 기각 결정에 대한 재항고 결정[191]에서 압수·수색 현장뿐만 아니라, 예외적인 상황이 인정되는 경우 수사기관의 사무실에도 피압수자나 변호인이 참여하여야 한다고 판시하고 있다. 그런데, 위와 같이 수사기관의 사무실에서의 참여의 경우 법적 성질과 근거가 문제되고, 이를 인정할 경우 수사기관의 수사를 위축하게 할 우려를 넘어 수사방해의 우려도 있어 문제된다.

나. 입법례

형사소송법 제121조와 제122조에서 법원의 압수·수색의 경우 피고인 또는 변호인의 참여와 압수·수색에 대한 통지를 인정하고 있고, 동법 제123조에서 타인의 주거, 간수자 있는 가옥, 건조물, 항공기 또는 선차 내에서 압수·수색영장을 집행함에는 책임자 참여하도록 규정하고 있고,[192] 동법 제219조에서 수사기관의 압수·수색 절차

---

190) 박혁수, “디지털 정보에 대한 압수수색 실무 상 문제점” 제12회 대법원 형사실무연구회 특별 심포지엄 자유토론문(2012. 12. 17.), 제27쪽. 따라서 위 대법원 결정에서 영장주의에 위배되어 위법하다고 본 “범죄 혐의와의 관련성에 대한 구분 없이 저장된 전자정보 중 임의로 문서출력 혹은 파일복사를 하는 행위”라 함은 디지털 정보의 압수·수색과 관련하여 이루어지는 일체의 파일 복사 또는 출력 행위를 의미하는 것이 아니라 “조사 또는 수색을 거쳐 그 내용을 확인한 결과 혐의사실과 관련이 없다는 것을 확인하고도 그 디지털 정보를 증거로 사용한다는 최종적인 압수의 의사로 복사 또는 출력하는 행위”를 의미한다고 보아야 할 것이다.

191) 대법원 2011. 5. 26.자 2009모1190 결정.

192) 제121조(영장집행과 당사자의 참여) 검사, 피고인 또는 변호인은 압수·수색영장의 집행에 참여할 수 있다.

제122조(영장집행과 참여권자에의 통지) 압수·수색영장을 집행함에는 미리 집행의 일시와 장소를 전조에 규정한 자에게 통지하여야 한다. 단, 전조에 규정한 자가 참여하지 아니한다는 의사를 명시한 때 또는 급속을 요하는 때에는 예외로 한다.

제123조(영장의 집행과 책임자의 참여) ① 공무소, 군사용의 항공기 또는 선차 내에서 압수·수색영장을 집행함에

에 준용하고 있다.

비교법적으로 외국의 입법례를 보면, 일본 형사소송법이 법원의 압수·수색 과정에 피고인의 참여권을 인정하고 있을 뿐, 수사기관의 압수·수색 과정에 피의자의 참여권을 인정한 입법례는 우리나라 밖에 없다. 독일의 경우 형사소송법 제11조에서 수색에 있어 소유자의 참여권을 인정하고 있으나, 서류의 검열 과정에 소유자의 참여는 인정하지 않고 있다.[193]

다. 참여의 일반론

수사기관의 압수·수색 영장 집행의 경우 피의자, 변호인은 참여할 수 있고, 영장 집행자는 미리 집행의 일시와 장소를 통지하여야 한다. 통지의 방법에는 전화, 서면, 구두 등 제한이 없고, 집행 일시와 장소를 미리 통지하면 된다. 다만, 피의자, 변호인이 참여하지 않는다는 의사를 명시적으로 표현한 때나 급속을 요하는 경우는 통지하지 않을 수 있다. 여기서 '급속을 요하는 때'라고 함은 증거를 인멸할 염려가 있거나 증거가 멸실될 위험이 있어 즉시 집행할 필요가 있는 경우를 말하고,[194] 급속을 요하느냐 여부의 판단은 영장을 집행할 자가 한다.[195] 피의자가 아닌 제3자를 압수·수색 당사자로 할 경우에는 압수·수색 현장에 주거주 등 책임자를 참여하게 하여야 한다.

는 그 책임자에게 참여할 것을 통지하여야 한다.

② 전항에 규정한 이외의 타인의 주거, 간수자 있는 가옥, 건조물, 항공기 또는 선차 내에서 압수·수색영장을 집행함에는 주거주, 간수자 또는 이에 준하는 자를 참여하게 하여야 한다.

③ 전항의 자를 참여하게 하지 못할 때에는 인거인 또는 지방공공단체의 직원을 참여하게 하여야 한다.

193) 2004년 형사소송법 개정으로 서류의 검열과정에서 소유자의 참여권 규정이 삭제되었다. 디지털 데이터의 수색도 서류의 검열에 준하여 위 규정이 적용된다고 하겠다. 이에 대하여 독일 연방헌법재판소는 모든 경우 참여권을 보장하는 아니며, 검열에의 참여권이 보장되어야 하는가의 판단은 개별사안에서 효과적인 형사소추와 데이터침해의 강도를 고려하여 판단되어야 한다고 판시하였다.(BVerfG, 2 BvR 902/06 vom 16.6.2009, Absatz-Nr. 96)

194) 대법원 2012. 10. 11. 선고 2012도7455 판결은 "피의자 또는 변호인은 압수·수색영장의 집행에 참여할 수 있고, 압수·수색영장을 집행함에는 원칙적으로 미리 집행의 일시와 장소를 피의자 등에게 통지하여야 하나, '급속을 요하는 때'에는 위와 같은 통지를 생략할 수 있다. 여기서 '급속을 요하는 때'라고 함은 압수·수색영장 집행 사실을 미리 알려주면 증거물을 은닉할 염려 등이 있어 압수·수색의 실효를 거두기 어려울 경우라고 해석함이 옳고, 그와 같이 합리적인 해석이 가능하므로 형사소송법 제122조 단서가 명확성의 원칙 등에 반하여 위헌이라고 볼 수 없다."라고 판시하였다.

195) 백형구, 주석 형사소송법1, 한국사법행정학회(2009), 제397쪽.

라. 디지털 데이터 압수와 관련된 참여

디지털 데이터 압수와 관련, 예외적인 상황이 발생하여 정보저장매체 자체를 압수하는 경우에도 법원은 압수·수색 영장의 집행이 종료되지 않았다는 것을 전제로 "예외적인 사정이 인정되어 그 전자정보가 담긴 저장매체 자체를 수사기관 사무실 등으로 옮겨 이를 열람 혹은 복사하게 되는 경우에도, 그 전체 과정을 통하여 피압수·수색 당사자나 그 변호인의 계속적인 참여권 보장"되어 "압수·수색의 대상인 저장매체 내 전자정보의 왜곡이나 훼손과 오·남용 및 임의적인 복제나 복사 등을 막기 위한 적절한 조치가 이루어져야만 그 집행절차가 적법한 것으로 될 것이다"라고 판시하여 예외적 상황의 경우에도 수사기관의 사무실도 참여를 보장하여야 한다고 하고 있다.[196]

마. 검토

예외적 상황이 인정되는 경우 압수·수색 영장의 집행은 종료되고 위의 법원의 태도는 형사소송법 제106조 제3항 개정 이전의 태도로 변경이 필요하다는 것은 앞서 살펴보았다. 그러므로 예외적인 상황인 경우 형사소송법 제121조, 제122조, 제123조 상의 참여에 관한 규정의 적용될 여지는 없다 하겠다.

한편, 원칙적으로 압수·수색 현장에서 디지털 데이터를 출력, 복제하는 경우에도 피의자, 변호인의 참여는 디지털 데이터의 취약성, 매체 독립성 등의 특징에 비추어 현실적으로 적용하기 어렵다고 생각된다. 쉬운 조작으로 디지털 데이터의 은닉, 삭제, 폐기가 가능하고 이를 찾거나 복원하는 작업은 가능성에 기대어 행할 수밖에 없기 때문이다. 그러므로 디지털 데이터의 압수·수색 의 경우 현행 형사소송법 제122조 단서 규정을 탄력적으로 적용하여 통지를 하지 않을 수 있다고 해야 할 것이다.

물론 예외적으로 수사기관의 사무실에서 정보저장매체의 봉인해제 및 이미지 파일 생성시 피의자나 변호인이 참여하는 경우가 있는바, 이는 영장 집행에 의한 참여가 아니라, 디지털 데이터의 무결성을 확보하기 위한 조치라고 하겠다.[197]

196) 대법원 2011. 5. 26.자 2009모1190 결정.
197) 전승수, "디지털 정보에 대한 압수수색영장의 집행", 법조 제670호(2012. 7.), 제273쪽.

생각건대 전술한 예외적 사유 판단기준 중 압수·수색 현장에서 출력, 복제하는 것이 곤란한 경우, 즉 3. 출력·복사, 현장에서의 이미징에 의한 집행이 피압수자 등의 영업활동이나 사생활의 평온을 침해하는 경우, 4. 집행현장에서의 하드카피·이미징이 물리적으로 불가능하거나 극히 곤란한 경우[198]에 해당하는 경우에는 피의자, 변호인의 참여를 보장하는 것이 타당하다고 생각된다. 왜냐하면 이 경우에는 정보저장매체 자체를 압수한 이유가 압수·수색 현장에서 원칙적인 방법으로 디지털 데이터를 압수할 수 있었으나 피압수자의 이익을 위하거나 시간이 오래 걸리는 등 물리적으로 불가능하였기 때문이고, 해당 디지털 데이터 정밀 분석의 필요성은 낮고, 대량의 디지털 데이터 중에서 사건과 관련된 디지털 데이터를 선별하는 과정이 대부분이므로, 압수·수색 현장에서 참여를 보장하는 것과 같이 참여를 보장하는 것이 국민의 기본권을 더욱 두텁게 보장하는 방법이기 때문이다.

한편, 압수·수색의 피의자, 변호인의 참여에 대한 규정은 공판단계에서 법원에 의하여 행하여지는 압수·수색은 필요한 증거가 대부분 수집되어 극히 예외적으로 이루어지므로 문제가 적지만, 수사기관의 압수·수색의 경우 그대로 적용하기는 어렵다. 수사기관이 수집한 증거의 내용에 대하여 보안이 요구되는 때도 있고, 수사기관이 수집한 증거의 내용을 알게 되면, 수사를 방해하고, 불리한 상황이라 판단하고 도주할 우려도 있기 때문이다. 그러므로 이와 관련하여 영장 집행의 일시와 장소를 미리 통지하면 영장 집행의 목적을 달성하지 못할 염려가 있는 경우, 예컨대 피의자가 통지를 받고 압수할 물건을 은닉, 파기할 염려가 있는 경우에는 통지의 예외를 명문으로 인정하는 것이 입법론으로 타당하다고 생각된다.[199]

198) 예외적 상황 판단기준 중에 1. 피압수자 등이 협조하지 않거나, 협조를 기대할 수 없는 경우, 2. 사건과 관련된 디지털 데이터가 삭제, 은닉, 폐기된 등 안티포렌식 정황이 발견되는 경우 3. 집행현장에서의 하드카피·이미징이 기술적으로 불가능하거나 극히 곤란한 경우(해당 정보저장매체를 기술적으로 정밀 분석해야 할 필요가 있으므로, 피의자, 변호인의 참여가 부적절)는 피의자, 변호인의 참여를 제한하여야 할 것이다.

199) 백형구, 주석 형사소송법1, 한국사법행정학회(2009) 제397쪽.

제7장 디지털 포렌식 모델에 대한 새로운 접근

제1절 현재 우리나라 디지털 포렌식 절차

형사소송법 제106조 제3항의 개정으로 우리나라의 디지털 포렌식 절차에 있어 많은 변화를 가져왔다. 앞서 검토한 바와 같이 현재의 디지털 포렌식 관련 쟁점과 절차를 정리하면, 다음과 같다.

1. 디지털 포렌식 관련 쟁점

디지털 데이터는 압수의 대상에 해당하고, 이에 대하여는 명문으로 규정할 필요가 있다. 압수·수색 영장에 기재된 장소 이외의 원격지에 저장된 디지털 데이터에 대한 대책을 강구할 필요성이 있고, 현장용 디지털 포렌식 도구의 성능 문제가 중요한 문제가 되었다. 현행 형사소송법 제106조 제3항은 디지털 데이터에 대한 압수방법을 제한하는 규정으로 이에 대하여는 개정하자고 하는 의견이 있으나, 피압수자의 권리 보호를 위하여 위 규정의 개정 필요성은 없다고 하겠다.

정보저장매체 자체를 압수한 예외적인 경우는 정보저장매체 자체의 압수로 압수·수색 영장의 집행은 종료한 것이므로, 이후의 과정은 임의수사라고 할 것이다. 법원이 압수·수색 영장 발부시 압수의 방법을 제한을 두는 등 예외적인 사유에 해당하는지 여부에 대한 판단 기준을 제시하고, 판단 주체를 법원이 하려고 하나, 결국 사전에 제시된 압수·수색 방법에 대한 판단기준은 추상적이고 일반적일 수밖에 없고, 현장에서 법원이 제시한 예외적인 사유에 해당하는지 여부에 대한 판단은 결국 현장에서 수사기관이 할 수 밖에 없게 되고, 법원은 예외적 사유에 해당하는지 여부에 대한 판단을 압수한 디지털 데이터에 대한 증거능력을 판단함으로서, 수사기관의 광범위한 디지털 데이터 압수·수색에 대한 우려를 사후적으로 제한한다.

정보저장매체를 분석하는 행위는 압수물에 대한 임의수사에 해당하므로, 분석 과정의 피의자나 변호인의 참여는 인정되지 않는다고 하겠다. 다만, 예외 사유 중 “출력·복사, 현장에서의 이미징에 의한 집행이 피압수자 등의 영업활동이나 사생활의

평온을 침해하거나 집행현장에서의 하드카피·이미징이 물리적으로 불가능하거나 극히 곤란한 경우는 피의자의 권리 보호를 위하여 분석 과정에 대하여 참여할 수 있다.

2. 디지털 포렌식 절차

압수·수색 현장에서 정보저장매체에 저장된 디지털 데이터 중 사건과 관련 있는 것만 출력, 또는 복사하는 방법으로 압수하는 것이 원칙이다. 압수·수색 현장에서 사건과 관련된 데이터를 조사하여 변경되지 않는 방법으로 복제하여 압수하면서, 압수한 디지털 데이터의 목록과 확인서를 작성 교부한다. 디지털 압수물을 검찰의 시스템에 업로드하고 디지털 포렌식 수사관은 결과보고서를 작성하여 일선 수사팀에 송부한다. 업로드된 디지털 데이터는 색인 과정을 통하여 직접 수사를 하고 있는 일선 수사팀에서 검색, 출력, 복제하여 수사에 활용하고, 법정에 증거로 제출한다.

현장에서 사건과 관련된 디지털 데이터를 출력, 복제하는 방법이 불가능하거나, 압수의 목적을 달성하기에 현저히 불가능한 예외적인 경우에는 정보저장매체 자체를 압수하는 방법으로 디지털 데이터에 대한 압수를 할 수 있다. 정보저장매체 자체를 압수한 후, 정보저장매체의 이미지 파일을 생성하고, 이를 시스템에 업로드, 업로드된 디지털 압수물의 분석 과정을 거쳐 사건과 관련된 디지털 데이터를 선별한다. 그리고 색인 과정을 거쳐 일선 수사팀에서 직접 수사에 활용할 수 있도록 하고, 디지털 포렌식 수사관은 결과보고서를 작성하여 일선 수사팀에 송부한다. 일선 수사팀은 이를 검색하여 수사에 활용하고, 법정에 증거로 제출한다.

제2절 우리나라 디지털 포렌식 절차의 특징

앞서 살펴보았듯이, 우리나라의 디지털 포렌식 절차는 몇 가지 특징이 있다. 디지털 데이터에 대한 원칙과 예외의 압수·수색의 방법으로 인한 절차가 나뉘게 된다. 그리고 특히 디지털 데이터의 현장 압수·수색 원칙으로 인하여 디지털 증거물의 무결성 등의 보장을 위하여 각 절차별 확인서 등의 확인 절차가 필요하다. 한편, 대용량·이종의 디지털 데이터를 일선 수사팀에서 직접 분석할 수 있도록 하는 시스템

(IDEAS)의 사용으로 인하여 디지털 포렌식 절차에 일선 수사팀이 개입하는 특징이 있다. 끝으로 디지털 압수물의 폐기와 관련된 부분에서 특징이 있다.

1. 압수·수색 방법에 따른 특징

형사소송법 제106조 제3항에 의하여 디지털 데이터의 압수·수색의 방법이 원칙적 현장 출력, 복제, 예외적 정보저장매체 자체 압수로 규정되어 있다. 이에 따라서 각각의 절차가 기술적인 부분, 참여 등의 적용 여부가 나뉘게 된다.

현장 압수의 원칙으로 압수·수색현장에서의 디지털 데이터가 사건과 관련된 것인지, 안티 포렌식 행위가 있는지 등을 조사하는 단계가 매우 중요하게 되었다.

2. 각 절차별 확인

그리고 디지털 데이터의 압수의 경우 각 단계별 문서화가 중요하다. 특히 압수·수색 현장에서 해당 정보저장매체에서 사건과 관련된 디지털 데이터만을 출력, 복제, 복사하는 경우 디지털 압수물의 진정성, 무결성을 확인하기 위하여 기술적인 방법으로는 한계가 있기 때문에 문서화가 더욱 중요하게 되었다.

3. 디지털 포렌식 절차에 일선 수사팀의 역할

디지털 압수물의 종류도 한정되어 있고, 양도 적을 때에는 디지털 포렌식 수사관이 분석한 디지털 압수물로 일선 수사팀에서 바로 수사에 활용할 수 있었다. 그러나 디지털 압수물의 종류의 다양화, 대용량화에 따라 디지털 포렌식 수사관의 분석만으로는 수사에 활용할 수 없게 되었다. 그러므로 디지털 포렌식 수사관이 1차로 분석한 디지털 압수물에 대하여 일선 수사팀에서 2차로 분석하여 수사에 활용하는 단계가 필요하게 되었다.

IT 지식이 많지 않은 일선 수사팀이 디지털 압수물을 분석하려면, 쉽게 검색 및 분석이 가능한 시스템이 갖추어 있어야 한다. 물론 어플리케이션으로 개인의 PC에서 검색 및 분석할 수도 있지만, 이미 디지털 압수물은 고성능의 PC로도 분석하기

에 용량이 과다하여 시스템을 활용하는 것이 효과적이다. 현재 검찰이 디지털 포렌식 수사관만의 분석에서 벗어나, 일선에 직접 수사하는 수사팀이 디지털 압수물에 대하여 검색과 분석을 통합적으로 할 수 있는 시스템(IDEAS)을 갖춘 것도 이 때문이다.

4. 디지털 압수물의 폐기

끝으로, 디지털 압수물에 대한 폐기도 우리나라 디지털 포렌식 절차의 특징이다. 디지털 압수물은 개개의 디지털 포렌식 수사관의 PC에 저장되어 있는 것이 아니라, 관리의 편의성과 접근 통제를 위하여 중앙집중형 시스템으로 통합하여 보관하고 있는바, 이에 대하여 법원의 판결이 확정되거나, 불기소 처분 등으로 더 이상 증거로서 가치가 없는 디지털 압수물에 대한 폐기를 하여야 한다. 이는 법률적으로는 일선 수사팀에서 수행할 것이나, 기술적으로 디지털 포렌식 수사관이 하여야 할 것이다.

제3절 우리나라의 현실에 맞는 디지털 포렌식 절차 모델 제시

위와 같은 우리나라의 디지털 포렌식 절차에 대한 특징으로 기존의 디지털 포렌식 절차 모델에 변화가 필요하게 되었다. 기존의 디지털 포렌식 절차 모델과 비교하여 현행 형사소송법이 디지털 데이터의 압수·수색 방법을 원칙과 예외로 구분하고 있고, 이에 따라 디지털 압수물의 무결성 등을 유지하기 위하여 각 단계별로 확인이 필요하며, 디지털 포렌식 수사관 개인이 수행하는 절차 위주에서 일선 수사팀이 수사에 활용하기 위하여 2차로 분석하는 절차로 변화되고, 중앙집중형으로 관리하고 있는 디지털 압수물의 폐기도 디지털 포렌식 절차에 포함되게 된다.

1. 기존의 디지털 포렌식 절차 모델

검찰의 실무상 검찰의 디지털 포렌식 절차 모델은 원칙적으로 압수·수색 준비 → 압수·수색 현장에서 정보저장매체 수색 → 정보저장매체에서 사건과 관련된 디지털 데이터 조사 → 사건관련 파일 복제, 목록 작성 교부, 확인서 작성 → 디지털 압수

물 업로드, (분석), 색인 → 일선 수사부서에서의 검색, 출력, 복제 → 사건 종료 후 디지털 압수물의 처리의 절차로 진행된다.[200]

현재 검찰은 내부규정인 '디지털 증거 수집 및 분석 규정'[201]과 디지털 수사망(DNET)을 이용하여 실무상 위와 같은 절차로 디지털 포렌식 업무를 수행하고 있다.[202]

그러나 경찰청의 포렌식 프로세스 모델[203]은 사전준비 → 증거수집 → 조사 → 분석의뢰, 접수, 운반 → 증거분석 → 결과보고서 → 보존 및 증거관리로 7개의 과정으로 되어 있는데, 이는 형사소송법 개정이전인 2006년의 가이드라인이고, 초기의 DFRWS Investigative Model과 크게 다르지 않다.

그러므로 검찰은 내부규정을 바탕으로 실무상 진행하는 디지털 포렌식 절차에 대한 명문의 근거 규정이 필요하고, 경찰의 경우 급변한 국내 디지털 포렌식 환경을 고려하여 새로운 디지털 포렌식 절차 모델이 필요하다고 하겠다.

2. 디지털 포렌식 절차 모델 제시

가. 새로운 디지털 포렌식 절차 모델 제시

그러므로 새로운 우리나라 디지털 포렌식 절차 모델을 다음과 같이 제시한다.

준비(Preparation) → 정보저장매체 수색(Search) → 조사(Examination) → 사건과 관련된 디지털 데이터 획득(Acquisition) → 1차 분석(1st Analysis) → 시스템 업로

---

200) 한편, 예외적으로 압수·수색 현장에서 사건과 관련된 디지털 데이터를 출력, 복제할 수 없는 경우에는 현장에서 정보저장매체에 저장되어 있는 디지털 데이터 전체를 복제하는 방법과 정보저장매체 자체를 압수하는 방법으로 나누어진다.
전자의 경우 압수·수색 준비 → 압수·수색 현장에서 정보저장매체 수색 → 정보저장매체에서 사건과 관련된 디지털 데이터 조사 → 이미지 파일, 복제본 디스크의 생성 → 정보저장매체 전부 복제, 이미징 확인서 작성 → 디지털 압수물 시스템에 업로드 → 업로드한 디지털 압수물 다운로드 받아 분석 → 분석한 디지털 압수물 업로드, 색인 → 일선 수사부서에서의 검색, 출력, 복제 → 사건 종료 후 압수물의 처리의 절차로 진행된다.
후자의 경우는 압수·수색 준비 → 압수 수색 현장에서 정보저장매체 수색 → 정보저장매체에서 사건과 관련된 디지털 데이터 조사 → 압수할 정보저장매체의 분리 → 정보저장매체 압수 확인서 작성 → 이미지 파일 생성 및 이미지 파일 시스템에 업로드 및 정보저장매체의 환부, 가환부 → 업로드한 디지털 압수물 다운로드 받아 분석 → 분석한 디지털 압수물 업로드, 색인 → 일선 수사부서에서의 검색, 출력, 복제 → 사건 종료 후 디지털 압수물의 처리의 절차로 진행된다.

201) 대검예규 제616호 (2012. 11. 6.)

202) 일선 수사팀에서의 2차 분석은 근거 규정이 없는 상태로 실무상 행하여지고 있다.

203) 경찰청, 디지털 증거처리 표준 가이드라인(2006. 12.).

드, 색인 (System Upload & Index) → 2차 분석(2nd Analysis) → 제출(Presentation) → 디지털 압수물 폐기(Disposal) 순이다.

현장 획득 불가능하거나 곤란한 경우[204]에는 위 절차에서 정보저장매체 수색(Search) 이후에 "압수(Seizure) → 복구(Recover) ↔ 조사(Examination)" 단계로 대체되고 사건과 관련된 디지털 데이터 획득(Acquisition) 이후는 동일하다.

나. 디지털 포렌식 절차 모델의 세부 설명

제시된 모델은 디지털 데이터의 압수 방법에 따라 절차가 나뉘어 있으며, 압수·수색 현장, 디지털 포렌식 사무실, 일선 수사팀 사무실로 장소별로 각 절차가 구분된다. 그리고 디지털 포렌식 수사관이 행한 모든 절차에 대하여 디지털 압수물의 무결성 유지를 위하여 피압수자나 변호인 등 참여인에게 확인서를 받는 등 문서화(Documentation)를 해야 한다.

(1) 준비(Preparation) 단계

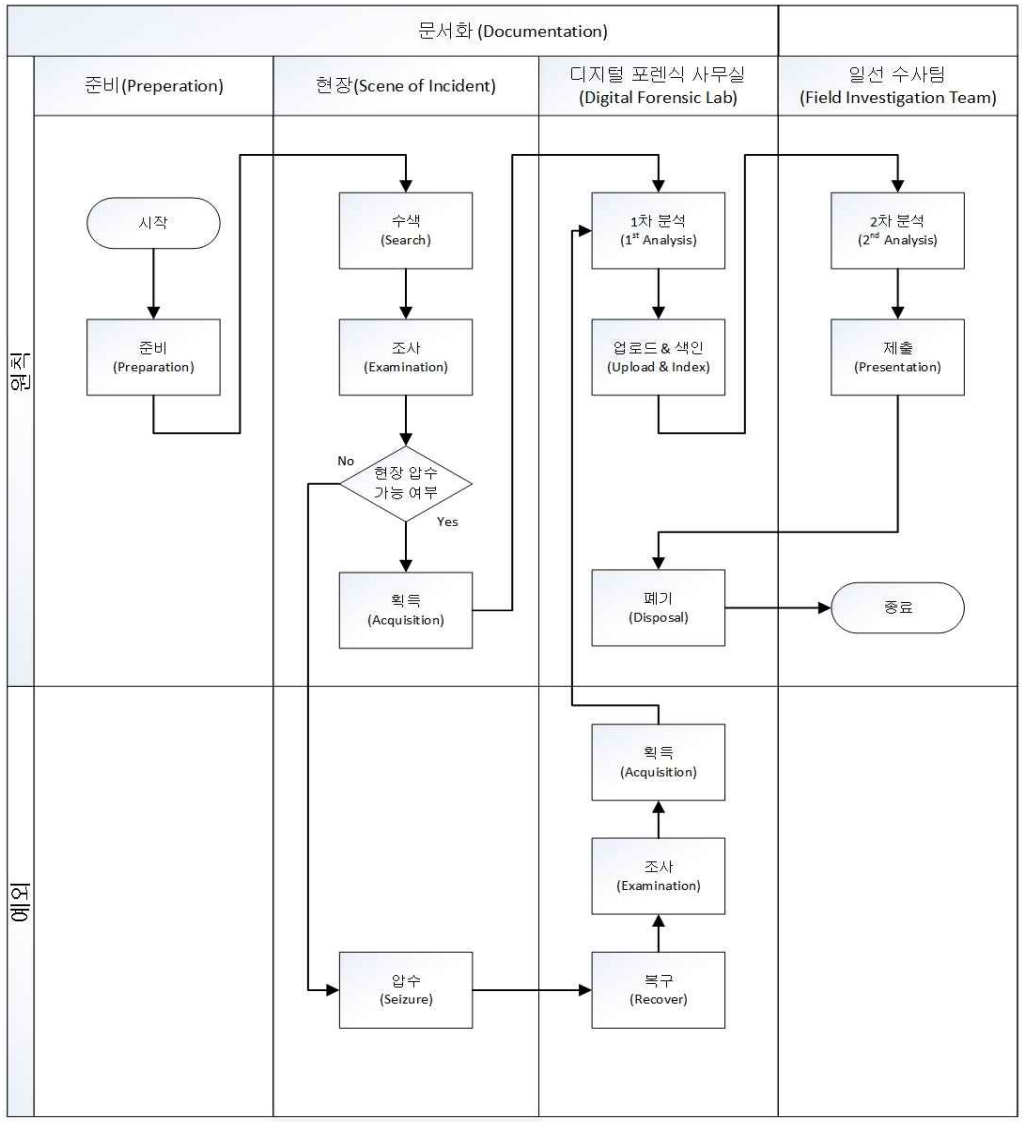
세부적으로 준비(Preparation) 단계는 해당 사건과 관련된 압수·수색 장소에 있는 정보저장매체의 종류 및 규모, 압수 예상된 디지털 데이터의 종류 등을 파악하여 필요한 인력과 장비를 예상하고, 관련 교육이 필요한 경우 디지털 포렌식 수사관에게 미리 숙지시킨다.

(2) 수색(Search) 단계

그리고 압수·수색 현장에서 정보저장매체 수색(Search), 조사(Examine), 선별(Selection), 획득(Acquisition), 문서화(Documentation)의 순으로 단계를 거친다. 정보저장매체 수색(Search) 단계는 압수·수색 현장에서 정보저장매체 자체가 있는지를 찾는 절차이다. PC나 서버뿐만 아니라, 현장에서 USB나 휴대전화 등에 이르기까지 정보저장매체를 찾는 단계이다.

---

204) 1. 피압수자 등이 협조하지 않거나, 협조를 기대할 수 없는 경우, 2. 사건과 관련된 디지털 데이터가 삭제, 은닉, 폐기된 등 안티포렌식 정황이 발견되는 경우 3. 출력·복사, 현장에서의 이미징에 의한 집행이 피압수자 등의 영업활동이나 사생활의 평온을 침해하는 경우, 4. 집행현장에서의 하드카피·이미징이 물리적, 기술적으로 불가능하거나 극히 곤란한 경우 5. 기타 이에 준하는 경우



[표15] 새로운 디지털 포렌식 절차 모델

(3) 조사(Examination) 단계

조사(Examination) 단계는 수색된 정보저장매체의 상태를 살펴보는 단계로, 디지털 데이터 삭제, 암호화 등 안티 포렌식 여부에 대하여 조사하고, 사건과 관련된 디지털 데이터를 찾아보는 단계이다.

세부 단계로는 안티 포렌식 여부나 사건과 관련된 디지털 데이터를 찾는 탐지(Detect) 단계, 안티 포렌식 여부나 사건과 관련된 디지털 데이터인지를 판단하는 평가(Assess) 단계, 안티 포렌식 여부나 사건과 관련된 디지털 데이터인지를 확정하는 확정(Confirm) 단계가 있다. 위 단계들은 일방향으로 진행되는 것이 아니라, 압수가 종료될 때까지 각 디지털 압수물 별로 탐지, 평가, 확정 후 다시 새로운 디지털 압수물에 대한 탐지, 평가, 확정 단계로 넘어가게 된다.

[표16] 조사 단계 세부 절차

(4) 획득(Acquisition) 단계

획득(Acquisition) 단계는 조사 단계에서 확정된 사건과 관련된 디지털 데이터를 획득하는 단계로 출력(Print), 복제(Imaging), 복사(Copy)의 방법으로 수행된다. 문서화(Documentation) 단계는 수색된 정보저장매체, 압수한 디지털 데이터의 목록, 압수·수색 현장에서의 참여자의 확인 등 압수와 관련된 사항에 대하여 문서화를 하는 단계이다.

한편, 조사 단계에서 현장에서 디지털 데이터를 획득할 수 없거나 곤란한 경우에는 정보저장매체 자체를 압수하는 압수(Seizure) 단계를 거쳐 디지털 포렌식 사무실 등 제3의 장소에서 별도의 절차가 진행된다.[205]

디지털 포렌식 사무실 등 제3의 장소에서 압수한 정보저장매체의 디지털 데이터를 복구하는 복구(Recover) 단계, 위 (3)의 조사(Examination) 단계를 거친 다음, 획득(Acquisition) 단계를 이동한다. 원칙에서의 획득 단계는 압수·수색 현장에서 행해지나, 여기에서의 획득 단계는 디지털 포렌식 사무실 등 제3의 장소에서 행하는 차이가 있다. 그러므로 무결성 유지는 물론 과도한 획득이 되지 않도록 노력해야 한다. 경우에 따라 피압수자나 변호인이 참여를 하는 경우도 있다.

205) 전술한 바와 같이 현장에서 획득이 곤란한 경우에는 피압수자의 권리 보장을 위하여 참여를 허용한다.

(5) 1차 분석(1st Analysis) 단계

디지털 포렌식 수사관은 디지털 포렌식 사무실 등 제3의 장소에서 획득된 디지털 압수물에 대하여 1차 분석을 한다. 1차 분석은 획득한 디지털 압수물의 상태를 확인하거나 기술적인 분석을 하는 단계이다. 이 단계에서 디지털 포렌식 수사관의 임무는 사실상 종료되는 것으로 분석 보고서 등을 작성하여 일선 수사팀에 송부한다.

(6) 시스템 업로드 및 색인(System Upload & Index) 단계

시스템 업로드(System Upload) 단계는 현장에서 획득된 디지털 압수물이나 제3의 장소에서 복구하여 획득된 디지털 압수물을 관리의 편의와 일선 수사팀의 2차 분석(2nd Analysis)을 위하여 시스템에 업로드 하는 단계이다. 시스템에 업로드가 완료되면, 디지털 포렌식 수사관 PC 등 정보저장매체에 저장된 디지털 압수물은 즉시 삭제한다. 색인(Index) 과정은 시스템에 업로드된 디지털 압수물을 검색의 편의를 위하여 색인을 하는 단계이다.

(7) 2차 분석(2nd Analysis)

일선 수사팀이 수행하는 단계로 검색 및 분석(Search & Analysis) 단계, 검색 및 분석 단계는 사건의 내용을 가장 잘 파악하고 있는 일선 수사팀에서 디지털 압수물을 직접 검색하고 통합적으로 분석하면서 수사에 활용하는 단계이다.

(8) 제출(Presentation) 단계

제출(Presentation) 단계는 일선 수사팀이 2차 분석을 통하여 디지털 압수물을 선별하여 법정에 '디지털 증거'를 제출하는 단계이다. 이 단계에서는 디지털 포렌식 수사관의 분석보고서나 일선 수사팀이 작성한 보고서도 법정에 제출될 수 있다.

(9) 폐기(Disposal) 단계

끝으로 법원의 판결이 확정되거나, 불기소 처분 등의 이유로 더 이상 증거로서 가치가 없는 디지털 압수물은 폐기하는 폐기(Disposal) 단계가 있다. 유체물인 압수물의 경우 환부가 원칙이나, 디지털 압수물은 출력, 복제, 복사 등 피압수자의 소유를 침해하지 않는 방법으로 획득하기 때문에, 이를 환부하는 것은 의미가 없기 때문에

폐기[206]를 원칙으로 한다. 디지털 압수물은 중앙집중형으로 보관하고 있기 때문에 일선 수사팀의 요청하면, 디지털 포렌식 수사관이 폐기하는 형식으로 한다.

206) 디지털 압수물의 폐기는 경제성을 고려하여 적절한 방법으로 행하는 것이 타당할 것으로 보인다.

제8장 결론

본 논문은 디지털 포렌식 절차 모델과 디지털 포렌식 현황을 살펴보고, 수사기관 특히, 검찰의 디지털 포렌식 절차를 고찰하면서, 현재 디지털 포렌식 관련하여 우리나라에서 논의되고 있는 쟁점을 다루었다. 그리고 우리나라 현실에 적합한 디지털 포렌식 절차 모델을 제시하였다.

우선 '디지털 증거'라는 용어가 일반적으로 사용되나, 정확하지 않은 용어이다. 압수한 디지털 데이터 모두가 증거로 제출되지는 않기 때문이다. 특히, 압수물에 대한 관리를 하고 있는 수사기관은 더욱 용어의 사용에 주의해야 한다. 압수한 디지털 데이터가 가장 정확한 표현이나, 본 논문에서는 '디지털 압수물'이라는 용어를 사용하겠다.

어떠한 절차로 디지털 포렌식을 하는데 효율적으로 수사의 목적을 달성할 수 있는지에 대한 연구가 디지털 포렌식 절차 모델이다. 이에 대하여 1995년 Computer Forensic Investigative Process를 시작으로 2013년 Integrated Digital Forensic Process Model 등 수 많은 디지털 포렌식 절차 모델이 발표되었다. 이러한 디지털 포렌식 절차 모델은 초기에는 절차를 표현하는 데 그쳤으나, 초기의 모델을 기반으로 몇 가지 절차를 추가하거나 순서를 바꾸는 등 발전된 디지털 포렌식 절차 모델이 연구되었으며, 최근에는 모든 사건의 경우를 포함할 수 있는 '통합' 디지털 포렌식 절차 모델의 연구가 활발히 진행되고 있는 실정이나, 결국 디지털 포렌식은 기술적인 측면만 있는 것이 아니라, 법률적인 측면도 있기 때문에 각국의 디지털 포렌식 현실, 특히 법률적인 현실에 디지털 포렌식 절차도 좌우될 수밖에 없다.

해외의 디지털 포렌식 현황은 각국의 특징에 맞는 기관과 법 규범을 구축하고 있다. 디지털 포렌식 관련 기관은 미국의 NIJ, 네덜란드의 NFI 등이 기술적인 도구 및 시스템 개발이나 표준 확립과 더불어 절차 규정 등의 법적인 부분에도 전문적으로 연구하고 있다. 각국의 법 현실은 디지털 데이터의 압수의 대상 여부는 대부분 인정하고 있고, 피압수자의 권리를 중요시하는 면이 부분적으로 보이나, 아직 수사 목적을 달성하는데 더 중점을 두고 있는 것으로 보인다.

우리나라의 경우 수사기관인 경찰청 사이버안전국과 검찰의 디지털수사과를 중심으로 디지털 포렌식을 이끌고 있다. 디지털 포렌식 절차에 있어서는 형사소송법 개정 이전에 판례에 의하여 형성되었는데, 디지털 데이터를 압수의 대상이 된다는 것을 전제로 원칙적으로 압수·수색 현장에서 디지털 데이터를 출력, 복사하는 방법으로 집행하여야 하고, 예외적인 사정이 있을 경우에 한하여 정보저장매체 자체를 이미징하거나, 수사기관의 사무실 등 외부로 반출할 수 있다고 하였고, 예외적인 경우의 수사기관 사무실로 옮긴 후의 과정도 전체적으로 압수·수색 집행의 일환이 된다고 하여 피압수자의 권리 보호를 강조하였다.

이 후 형사소송법의 개정으로 제106조 제3항에서 “법원은 압수의 목적물이 정보저장매체인 경우에는 기억된 정보의 범위를 정하여 출력하거나 복제하여 제출받아야 한다. 다만, 범위를 정하여 출력 또는 복제하는 방법이 불가능하거나 압수의 목적을 달성하기에 현저히 곤란하다고 인정되는 때에는 정보저장매체 등을 압수할 수 있다”고 규정하여 디지털 데이터의 압수에 대하여 명문으로 규정하였지만, 디지털 데이터의 압수에 대하여 여전히 논란의 여지를 남겼다.

한편, 검찰은 디지털 데이터의 대용량화와 효율적인 디지털 압수물의 활용을 위하여 디지털 수사망이라는 시스템을 구축하기에 이르렀다. 디지털 포렌식 업무를 통합적으로 관리하는 디지털수사통합업무관리시스템(DFISII), 디지털 압수물을 사건별로 보관하고 관리하는 디지털증거보관시스템, 일선 수사팀에서 디지털 압수물을 직접 검색, 분석함으로써, 방대한 디지털 압수물을 효율적으로 수사에 활용할 수 있는 통합디지털증거분석시스템(IDEAS)으로 구성되어 있다.

검찰의 디지털 포렌식 절차는 원칙적으로 압수·수색 준비, 압수·수색 현장에서 정보저장매체 수색, 수색한 정보저장매체에서 사건과 관련된 디지털 데이터 조사, 사건과 관련된 디지털 데이터의 획득, 문서화, 디지털 압수물 시스템에 업로드, 색인, 수사팀에서 검색, 분석, 디지털 압수물 폐기의 순이다.

예외적인 경우 현장에서 압수·수색 준비, 압수·수색 현장에서 정보저장매체 수색, 수색한 정보저장매체에서 사건과 관련된 디지털 데이터 조사, 정보저장매체 전체를 이미징하거나, 정보저장매체 자체를 압수(이후 이미징, 정보저장매체의 반환), 문서화, 디지털 압수물 시스템에 업로드, 분석, 색인, 수사팀에서 검색, 분석, 디지털 압

수물 폐기의 순이다.

현재 우리나라에서 디지털 포렌식 관련 논란이 있는 부분을 간략히 정리하면, 디지털 데이터는 압수의 대상이고, 피압수자의 협력의무는 명문의 규정이 필요하고, 원격지 압수·수색은 필요성은 있으나, 허용 범위나 방법 등 아직 논의가 더 필요하며, 압수·수색 현장에서의 디지털 포렌식이 더욱 중요해진바, 현장용 디지털 포렌식 도구가 갖추어야 할 기능을 발전시켜야 할 필요가 있겠다. 그리고 형사소송법 제106조 제3항 단서는 예외적인 경우 정보저장매체 자체를 "압수 할 수 있다"고 규정하고 있어 정보저장매체를 압수하면 압수·수색 영장의 집행은 종료되었다 할 것으로, 이와 관련된 형사소송법 개정 전의 법원의 태도는 변경되어야 하고, 법원이 우려했던 정보저장매체 자체의 압수에 대한 피압수자의 권리 보호는 비례의 원칙, 법원의 위법하게 수집된 디지털 압수물에 대하여 증거능력 부정하는 방법 및 현장에서 출력, 복제가 곤란한 경우 사건과 관련된 디지털 데이터의 선별 과정의 참여 보장으로 해결할 수 있다. 동항은 피압수자의 권리 보호를 위하여 필요한 규정으로 개정보다는 이를 준수하는 방법을 보완하는 방향으로 논의가 되어야 하고, 예외에 해당하는지 여부에 대한 판단기준은 법원이 사전 제한을 하려하지만, 결국 압수·수색 현장에서 수사기관이 판단할 수밖에 없고, 법원은 증거능력에 대한 판단을 함으로써 사후에 견제할 수 있다.

우리나라의 현실에 맞는 디지털 포렌식 절차를 제시하면, 준비(Preparation) → 정보저장매체 수색(Search) → 조사(Examination) → 사건과 관련된 디지털 데이터 획득(Acquisition) → 1차 분석(1st Analysis) → 시스템 업로드, 색인 (System Upload & Index) → 2차 분석(2nd Analysis) → 제출(Presentation) → 디지털 압수물 폐기(Disposal) 순이다.

흔히 1999. ~ 2007. 기간은 디지털 포렌식의 황금기라고 하는 반면, 그 이후부터 현재까지는 '디지털 포렌식 위기'라고 한다. 스토리지의 급격한 증가, 하드웨어 인터페이스와 임베디드 저장 장치의 증가, 운영체제와 파일 포맷의 다양화, 암호화, 클라우드 시스템의 확산 등의 기술적이 어려움뿐만 아니라, 디지털 포렌식에 대한 법적인 제한이 늘어나게 되었기 때문이다. 이러한 위기는 수사기관의 입장에서는 새로운 도전에 직면하게 된 것이다. 우리나라도 디지털 데이터에 대한 압수·수색에 대하여 규정하면서, 수사기관의 디지털 데이터에 대한 광범위한 압수를 제한하는 형

태의 규정을 형사소송법에 명시하였다. 피압수자의 권리를 보호하기 위하여 수사에 있어 여러 가지 제한은 앞으로 더욱 강화될 것이고, 외국의 경향도 디지털 포렌식과 관련하여 피압수자의 권리 보호를 강화하는 방향으로 나아가고 있는 것으로 보인다. 우리나라의 디지털 포렌식 관련 형사소송법 규정은 우리나라에만 있는 '이상한' 규정이 아니라, 우리나라에서 '최초로' 규정된 선진적인 규정이라 할 수도 있다.

그러므로 수사기관은 형사소송법 개정으로 과거에 비하여 디지털 데이터 압수가 어렵고, 효과적이지 못하다고 불만을 늘어놓을 것이 아니라, 지나치게 수사의 효율성만을 강조하지 않았는지 반성할 필요가 있다. 피압수자의 권리를 보호하면서 수사의 목적을 달성하기 위하여 디지털 포렌식 절차의 확립이 필요하다. 형사소송법 개정이후 우리나라의 디지털 포렌식 절차 모델에 대한 연구는 거의 없었다. 본 논문이 디지털 포렌식 분야에 있어 피압수자의 권리를 보장하는 동시에 수사의 목적을 효율적으로 달성할 수 있도록 조금이나마 도움이 되길 바란다.

참고문헌

Ⅰ. 국내자료

노명선, “디지털증거 압수수색에 관한 법률의 문제점과 개선방안”, 2012년 디지털증거 압수수색에 관한 개정법률(안) 공청회 자료

독고지은, “디지털 증거 압수수색에 대한 개정 형사소송법의 규제와 집행에 관한 연구 -영장 집행시 제기되는 쟁점을 중심으로-”, 법조(통권680호), 법조협회(2013. 5)

대검찰청, “과학수사 실무 매뉴얼”(2014)

대검철청, “사이버범죄방지를 위한 국제공조방안 연구 - 유럽사이버범죄방지협약을 중심으로”(2009. 12.)

박혁수 “디지털 정보에 대한 압수수색 실무 상 문제점” 제12회 대법원 형사실무연구회 특별심포지엄 자유토론문(2012. 12. 17.)

백형구, 주석 형사소송법1, 한국사법행정학회(2009)

손동권, “새로이 입법화된 디지털 증거의 압수·수색제도에 관한 연구”, 형사정책(제23권 제2호)(2011)

송봉규, 장석헌, “경찰의 디지털 포렌식 실태와 개선방안”, 한국경찰연구 제12권 제2호(2013)

신동운, 신형사소송법(제4판), 법문사(2012)

양근원, “형사절차상 디지털 증거의 수집과 증거능력에 관한 연구”, 경희대학교 대학원 법학과 박사학위논문(2006)

오기두, “디지털증거 압수수색에 관한 법률의 문제점과 개선방안”의 토론문, 2012년 디지털증거 압수수색에 관한 개정법률(안) 공청회 자료

오기두, “전자정보의 검증 수색 압수에 관한 개정 형사소송법의 함의”, 한국형사소송법학회 발표문(2012. 2. 17.)

오기두, “형사절차상 컴퓨터 관련 증거의 수집 및 이용에 관한 연구”, 박사학위논문, 서울대학교 대학원(1997)

이완규, “디지털 증거 압수수색과 관련성 개념의 해석”, 법조(2013.11.)

이상진, “디지털 포렌식 개론”(2010)

이숙연, “디지털증거의 압수수색”, 형사법 실무연구(2011)

이숙연, “전자정보에 대한 압수수색과 기본권, 그리고 영장주의에 관하여”, 헌법학 연구 제18권 제1호(2012)

이숙연, “형사소송에서의 디지털증거의 취급과 증거능력”, 고려대학교 정보경영공학전문대학원 정보경영공학과 박사학위논문(2010)

이윤재, “디지털증거의 압수수색영장의 집행에 있어서의 협력의무” 한국형사법학회, 형사법연구 제24권 제2호(2012)

이주원, “디지털 증거에 대한 압수수색제도의 개선”, 안암법학(37권)(2012)

임한희, “개정된 형사소송법에 적합한 현장 디지털 증거 추출도구 필요요건에 관한 연구”, 고려대학교 정보보호대학원 석사학위논문(2012)

원혜옥, “정보저장매체의 압수수색”, 형사판례연구 22

조광훈, “형사소송법 제106조의 쟁점과 개정안 검토”, 법조 제694호(2014. 7)

전승수, “디지털 정보에 대한 압수수색영장의 집행”, 법조(2012. 7.)

전승수, “형사절차상 디지털 증거의 압수 수색 및 증거능력에 관한 연구”, 서울대학교 대학원 박사학위논문, (2011)

정교일, “디지털 증거의 압수와 공판정에서의 제출방안”, 대검찰청, 형사법의 신동향 통권 제25호(2010. 4.)

정웅석, 백승민, 형사소송법(전정 제4판)(2011)

조국, “컴퓨터 전자기록에 대한 대물적 강제처분의 해석론적 쟁점”, 한국형사정책학회, 형사정책(제22권 제1호)(2010. 7.)

Ⅱ. 국외자료

Ademu O., Chris O., David S., "A New Approach of Digital Forensic Model for Digital Forensic Investigation", International Journal of Advanced Computer Science and Application(2011).

Agawal A., Gupta M., Gupta S., Gupta C., "Systematic Digital Forensic Investigation Model", International Journal of Computer Science and Security(2011).

Beebe N., Clark J. "Hierarchical Objectives based Framework for the Digital Investigation Process" DFRWS(2004).

B. Carrier & E. H. Spafford, “Getting Physical with the Digital Investigation Process”, International Journal of Digital Evidence, Vol. 2, No. 2(2003).

C. Ryan Reetz, “Warrant Requirement for Searches of Computerizes Information", 67 B.U.L.Rev 179, 197(1987).

Department of Justice, US, Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition

F. C. Freiling & B. Schwittay, “Common Process Model for Incident and Computer Forensics”, in Proceedings of Conference on IT Incident Management and IT Forensics, Stuttgard, Germany(2007).

G. Palmer, "DTR-T001-01 Technical Report. A Road Map for Digital Forensic Research", Digital Forensics Workshop (DFRWS), Utica, New York(2001).

Josh Goldfoot, "The Physical Computer and the Fourth Amendment", 16 Berkley J. Crim. L. 112, 157(2011).

Kohn M., Eloff M., Eloff JHP., "Integrated Digital Forensic Process Model", International Journal of Computer Science and Security(2013.)

M. Kohn, J. H. P. Eloff, & M. S. Olivier, “Framework for a Digital Forensic Investigation”, in Proceedings of the ISSA 2006 from Insight to Foresight Conference, Sandton, South Africa(2006).

M. K. Rogers, J. Goldman, R. Mislan, T. Wedge & S. Debrota, “Computer Forensic Field Triage Process Model”, presented at the Conference on Digital Forensics, Security and Law(2006).

M. M. Pollitt, “Computer Forensics: An Approach to Evidence in Cyberspace”, in Proceeding of the National Information Systems Security Conference, Baltimore, MD, Vol. II(1995).

M. Reith, C. Carr & G. Gunsh, “An Examination of Digital Forensics Models”, International Journal of Digital Evidence, Vol. 1, No. 3(2002).

NFI, "XIRAF_Online Advanced Forensic Analysis"(2012)

Orin S. Kerr, “Search Warrants in an Era of Digital Evidence”, 75 MISS. L. J. 85(2005).

P. Sundresan, “Digital Forensic Model based on Malaysian Investigation Process”, International Journal of Computer Science and Network Security, Vol. 9, No. 8(2009).

Ritu Agarwal, Suvarna Kothari, "Review of Digital Forensic Investigation Frameworks", Information Science and Applications Volume 339(2015)

Valjarevic A., Venter H., "Harmonized Digital Forensic Investigation Process Model", IEEE(2012).

V. Baryamereeba & F. Tushabe, “The Enhanced Digital Investigation Process Model”, in Proceeding of Digital Forensic Research Workshop, Baltimore, MD(2004).

W. Alink, R.A.F. Bhoedjang, P.A. Boncz, A.P. de Vries, “XIRAF –- XML-based indexing and querying for digital forensics”, DFRWS, digital investigation(2006)

Yunus Yusoff, Roslan Ismail and Zainuddin Hassan, “Common Phases Of Computer Forensics Investigation Model”, International Journal of Computer Science & Information Technology (IJCSIT), Vol 3, No 3,(2011.6.)

Ⅲ. 판례자료

대법원1999. 12. 1, 99모161 결정

대법원 2002. 7. 12. 선고 2002도745 판결

대법원 2007. 12. 13. 선고 2007도7257 판결

대법원 2009. 3. 12. 선고 2007도763 판결

대법원 2011. 5. 26.자 2009모1190 결정

대법원 2012. 10. 11. 선고 2012도7455 판결

United States v. Marbury, 732 F. 2d, 390, 399-400(5th Cir. 1984).

United States v. David, 756 F. Supp. 1385, 1390(D.D.N.1991).

United States v. Chan, 830 F. Supp. 531, 534-535(D.N.D. Cal. 1993).

BVerfG, 2 BvR 902/06 vom 16.6.2009, Absatz-Nr. 96

Abstract

New Approach of Digital Forensics Process Model

Jee Hong Kim

Department of Mathematical Information Science

The Graduate School of Convergence Science & Technology

Seoul National University

The digital data are utilized in most part of life due to increased use of various digital devices. The investigative agencies began to pay attention at digital devices accordingly, and the time that is difficult to prove crime without digital data has come. However, because the digital data have different features compared to the material objects, precautions are required in the seizure.

It is important to regulate a specific procedure to accomplish the purpose of investigation after seizing the digital data, and this is called the "Digital Forensic Process Model". Digital forensics are different according to the legal characteristics of each country, because not only the technical but also the legal issues need to be considered.

The revised version of the Korean Criminal Procedure Act stipulated the seizure of digital data by substantive enactment on January 1st of 2012. It was a major change in the standard of digital data seizure from information 'storage device' to 'digital data' related suspicion. Although there are debates on the revised

Criminal Procedure Act, researches on the methodology of digital data seizure under legal regulation are scarce.

The aim of present study was to investigate the digital forensic process models and the current state of digital forensics, and to suggest a new digital forensic process model through reviewing the digital forensic process of investigative agency, especially the Korean Prosecutors' Office.

In Korea, institution of digital forensics are located at the National police agency and the Korean Prosecutors' Office, and digital forensic process was based on precedents before the revised Criminal Procedure Act. However, some precedents that stands against the present law need to be changed. The Korean Prosecutors' Office has built a system called "Digital Investigation Network", which is utilized in the mass storage of digital data and effective 'digital seized article'.

The principal digital forensic process of the Korean Prosecutors' Office is preparation of seizure and research, search of data storage device on-the-spot, investigation of digital data related suspicion through data storage device, capture of digital data related suspicion (otherwise, imaging the whole data storage device or seizing data storage device), documentation, uploading system of seized digital devices (otherwise, analyzing), index, searching and analysis at first-line investigation squad, and discarding the 'digital seized article'.

Digital data are objects of seizure, and cooperating duty of the parties seized needs substantive enactment. Remote place seizure and investigation is needed and a permission range or method requires further discussion. The function of field instruments for digital forensic needs to be developed. By the Clause 3 of Article 106 of Criminal Procedure Act, the attitude of the court about seizure of

digital data has to be changed.

To suggest a digital forensic process which is appropriate for Korean reality, the flow goes as follows: Preparation → Search (data storage device)→ Examination → Acquisition(of digital data related suspicion) → 1st Analysis → System Upload & Index → 2nd Analysis → Presentation → Disposal (of 'digital seized article')

Recent overseas trend shows that digital forensic process moves in the direction which emphasizes the protection of the parties seized rights. The Korean code of criminal procedure as regards to digital forensic is not a "strange" regulation but the "first" advanced regulation. Therefore, the investigative agency (such as Prosecutors' Office) should try to protect the rights of the parties seized and establish the digital forensic process to accomplish the goal of investigation.

key words : Digital evidence, Digital seized article, Digital forensics process model

Student Number : 2013-24050