연구총서 16-AA-01

디지털포렌식 통합모델 구축에 관한 연구

탁희성 | 이원상

A Study on a Model Frame for the Integration of Digital Forensic Processes

KIC 한국형사정책연구원
KOREAN INSTITUTE OF CRIMINOLOGY

발간사

디지털 포렌식은 디지털 기기를 매개로 하여 발생한 특정행위의 사실관계를 법정에서 규명하고 증명하기 위한 기술에 기반한 방법과 절차라고 할 수 있습니다. 특히 디지털 데이터가 법적으로 유효한 증거자료로서 제시되기 위해서는 디지털 데이터의 물리적·논리적 취약성을 뒷받침할 수 있는 기술적인 방법을 통해 진정성·무결성·신뢰성· 원본성 등이 확보되어야 하는데, 디지털 포렌식은 이와 같이 디지털 데이터의 입증가치를 수집단계에서부터 폐기단계에 이르기까지 신뢰성 있게 유지할 수 있도록 하는 기술적·절차적·법적 요소로 구성된 포괄적인 프로세스라고 할 것입니다.

현재 우리나라의 경우 각 정부기관의 필요에 따라 디지털 포렌식 시스템이 독자적으로 운용되고 있으며, 각 기관별 운용지침이 있지만, 각 기관들이 표준적인 모범으로 삼아 준수할 수 있는 디지털 포렌식 지침은 아직 마련되어 있지 않습니다. 디지털 증거가 수사를 위한 lifecycle의 시작단계에서 부터 관련 기준들을 충족하는 모범실무에 기반한 표준적인 운용절차를 활용하여 적절히 취급되어질 수 있다면, 형사사법시스템 전체를 통하여 디지털 증거관리의 일관성을 확보할 수 있고, 따라서 증거오염으로 인한 입증가치의 훼손을 피할 수 있다고 할 것입니다. 다만 현재 우리의 디지털 포렌식 시스템은 그와 같은 표준적인 운용절차나 모범 실무를 마련하지 못한 채 운용되고 있기 때문에 언제든지 그 신뢰성 검증에서 이의가 제기될 우려가 있고, 따라서 수사기관이 어렵게 수집하고 분석한 자료들을 법정 증거로 활용하지 못하는 문제가 발생할 수 있다고 할 것입니다.

따라서 본 연구는 우리나라 형사사법기관별로 운용하고 있는 디지털 포렌식 시스템을 검토하여 실무에서 발생하고 있는 문제점이 무엇이고, 실무에서 요구되는 디지털 포렌식 시스템의 구체적인 내용이 무엇인지를 파악하여 IT 기술수명의 짧은 주기와

포렌식 수사의 신속성과 기밀성에 부합할 수 있는 전체적인 프로세스를 모색해 보고자 하는데 목적을 두고 수행되었습니다. 그리고 이를 위해서는 디지털 포렌식 도구와 절차, 랩에 대한 세계적인 수준의 인증시스템을 갖추어야 하는 바, 본 연구에서 제시하는 통합 디지털 포렌식 모델내에 이와 같은 인증시스템을 구축할 수 있는 방안도 함께 제시하였습니다. 디지털 증거가 법정에서 신뢰할 수 있는 유효한 증거로서 활용될 수 있도록 뒷받침할 수 있는 디지털 포렌식 프로세스를 구축하는데 본 연구가 작은 기여를 할 수 있기를 바라는 바입니다.

마지막으로 이 연구를 성실하게 수행해준 탁희성 선임연구위원 그리고 공동연구로 참여해주신 조선대학교 법학과 이원상 교수님의 노고에 취하와 감사를 드립니다.

2016년 12월

한국형사정책연구원

원장 강 진 환

목 차

국문요약 ····· 1

| 제1장 | 디지털 포렌식에 있어서 새로운 접근방식의 필요성 (탁희성) ····· 17

제1절 서론 ····· 19
1. 연구의 필요성 및 목적 ····· 19
2. 연구방법 ····· 22
제2절 디지털 포렌식 프로세스의 기본 구조 및 개요 ····· 24
1. 디지털 포렌식의 기본 개념 ····· 24
2. 디지털 포렌식의 구성요소 ····· 27
가. 기술적 요소 ····· 27
1) 디지털 포렌식 도구 ····· 27
2) 디지털 포렌식 전문가 ····· 29
3) 디지털 포렌식 실험실 ····· 31
나. 절차적 요소 ····· 32
1) 보관의 연속성(chain of custody) ····· 32
2) 통합관리정책 ····· 34
다. 법률적 요소 ····· 35
1) 적법절차의 준수 ····· 35
2) 증거법적 요구사항 ····· 36
3. 디지털 포렌식의 기본원칙 ····· 37
가. 무결성 원칙 ····· 38
나. 적법절차의 원칙 ····· 39
다. chain of custody 원칙 ····· 40
라. 재현의 원칙 ····· 40

4. 디지털 포렌식 프로세스의 필요성 ····· 40
가. 기관내 포렌식 업무품질의 질적 수준 유지 ····· 42
나. 법정 증거로서 디지털 데이터의 동일성 및 무결성 입증을 위한 절차적 수단 ····· 43
다. 형사소송법 개정에 따른 포렌식 전문가 증언의 신뢰성 입증 자료 ····· 44
5. 디지털 포렌식 프로세스 모델의 변화 ····· 46
가. 기존 디지털 포렌식 프로세스 모델 ····· 47
1) Computer Forensic Investigative Process(1984) ····· 47
2) DFRWS Model(2001) ····· 47
3) Forensic Process Model(2001) ····· 49
4) Abstract Digital Forensic Model(2002) ····· 49
5) IDIP(The Integrated Digital Investigation Process) Model(2003) ··· 51
6) Enhanced Digital Investigation Process Model(EDIP) (2004) ····· 54
7) Computer Forensics Field Triage Process Model(CFFTPM)(2006) ···· 55
8) Digital Forensic Model based on Malaysian Investigation Process (DFMMIP)(2009) ····· 58
9) Systematic Digital Forensic Investigation Model(2011) ····· 60
10) Harmonized Digital Forensic Investigation Process Model (2012, 2014) ····· 64
11) Integrated Digital Forensic Process Model ····· 69
나. 기존 디지털 포렌식 프로세스 모델의 변화 경향 분석 ····· 72

| 제2장 | 현행 디지털 포렌식 시스템 및 프로세스 비교 (탁희성) ····· 75

제1절 형사사법기관별 디지털 포렌식 시스템 및 프로세스 ····· 77
1. 검찰의 디지털 포렌식 시스템(DFIS) ····· 77
가. 디지털 포렌식 업무 현황 ····· 77
나. 디지털 포렌식 절차 ····· 78
1) 디지털 포렌식 수사관의 증거수집 및 분석 규정 ····· 79
2) 과학수사 실무매뉴얼 ····· 80

2. 경찰의 디지털 포렌식 절차 ····· 83
가. 디지털 포렌식 업무 현황 ····· 83
나. 디지털 포렌식 절차 ····· 85
1) 디지털 증거수집 및 처리 등에 관한 규칙 ····· 86
2) 현장 수사관을 위한 디지털 증거 압수·수색 가이드라인 ····· 87
3) 디지털 포렌식 표준 가이드라인 ····· 88
제2절 디지털 포렌식에 대한 판례 경향 ····· 90
1. 디지털 포렌식 절차에 대한 법원의 태도 ····· 90
가. 서울중앙지법 2007.4.16. 선고 2006고합1365 등, 서울고등법원 2007.08.16. 선고 2007노929 판결 ····· 91
나. 대법원 2013.7.26. 선고 2013도2511, 서울고등법원 2013.02.08. 선고 2012노805 판결 ····· 94
2. 디지털 증거의 압수·수색과 관련한 판례의 경향 ····· 96
가. 압수·수색의 방법에 관한 법원의 태도 ····· 96
1) 디지털 증거에 대한 법원의 압수 대상 및 방법의 제한 ····· 96
2) 대법원 2011.5.26. 자 2009모1190 결정(원심 서울중앙지방법원 2009. 9. 11.자 2009보5 결정) ····· 97
3) 서울중앙지방법원 2012.02.23. 선고 2011고합1131 판결 ····· 98
4) 대법원 2015.7.16. 자 2011모1839 전원합의체 결정 ····· 99
나. 참여권 보장에 관한 법원의 태도 ····· 100
1) 대법원 2011.5.26. 자 2009모1190 결정 ····· 100
2) 대법원 2015.1.22. 선고 2014도10978 전원합의체 판결 ····· 101
3) 대법원 2015. 7.16. 자 2011모1839 전원합의체 결정 ····· 102
다. Plain View 관련 법원의 태도 ····· 102
제3절 현행 디지털 포렌식 프로세스의 문제와 한계 ····· 104
1. 디지털 포렌식 운영 현황에 대한 전문가 면접조사 ····· 104
가. 조사 목적 및 방법 ····· 104
나. 인터뷰 항목 ····· 105
2. 인터뷰 결과에 나타난 현행 디지털 포렌식 프로세스의 한계 ····· 106
가. 디지털 포렌식 전문인력의 부족 ····· 106
나. 디지털 포렌식 도구의 신뢰성 확보의 한계 ····· 108
다. 디지털 포렌식 프로세스 표준화 작업에 대한 인식의 한계 ····· 110
라. 형사소송법 개정에 따라 제기되는 실무상의 문제 ····· 111

| 제3장 | 주요 국가들의 디지털 포렌식 시스템 및 프로세스 (탁희성·이원상) ····· 113

제1절 미국의 디지털 포렌식 시스템 ····· 115
1. 디지털 포렌식 기관 ····· 115
가. 국립사법연구소(National Institute of Justice:NIJ) ····· 115
1) NIJ 개요 ····· 115
2) NIJ의 표준 개발 ····· 116
3) 디지털 포렌식 분야의 NIJ 표준과 가이드라인 ····· 117
4) 디지털 포렌식 분야의 NIJ 프로젝트 ····· 119
나. RCFL(Regional Computer Forensic Laboratory) ····· 121
1) RCFL의 구성과 임무 ····· 121
2) RCFL의 관리감독 ····· 122
3) RCFL의 서비스 ····· 122
4) RCFL 서비스 품질 강화를 위한 인증 지원노력 ····· 123
다. DCFL(Defense Computer Forensic Laboratory) ····· 124
2. 디지털 포렌식 업무 관련 지침 및 가이드라인 ····· 126
가. Electronic Crime Scene Investigation : A Guide for first Responders ····· 126
1) 목적과 기본원칙 ····· 126
2) 지침서의 구성 ····· 127
나. Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors ····· 132
1) 지침서의 목적 ····· 132
2) 압수와 수색 문제 ····· 133
3) 디지털 증거의 무결성, 개시, 공개(Integrity, Discovery and Disclosure of Digital Evidence) ····· 137
4) 법정제출과 증거법칙 ····· 139
5) 디지털 증거의 프레젠테이션 ····· 143
다. Forensic Examination of Digital Evidence: A Guide for Law Enforcement ····· 145
1) 목적과 원칙 ····· 145

2) 정책 및 절차의 개발 ····· 145
3) 증거 평가(Evidence Assessment) ····· 146
4) 증거 획득(Evidence Acquisition) ····· 148
5) 증거 조사(Evidence Examination) ····· 149
6) 기록과 보고(Documenting and Reporting) ····· 150
3. 디지털 포렌식에 대한 법적 평가 ····· 151
가. 디지털 포렌식 도구에 대한 법원의 태도 ····· 153
1) People v. Rodreiguez, No.Fo31606 ····· 153
2) United States v. habershaw, 2001 WL 1867803(2002 D. Mass) ···· 154
나. 디지털 포렌식 프로세스에 대한 법원의 태도 ····· 154
1) Simon Property Group, L.P. v. mySimon, Inc. 194 F.R.D.639 (S.D.Ind.2000) ····· 155
2) United States v. Bunty, 617 F. Supp. 2d 359 (E.D. Pa. 2008) ··· 156
다. 디지털 포렌식 전문가에 대한 법원의 태도 ····· 157
1) Galaxy Computer Services, Inc. v. Baker ····· 158
2) Nucor Corp v. Bell, 2008 WL 4442571 (D.S.C. Jan. 11, 2008) ··· 159
3) United States v. Hilton ····· 160
제2절 영국의 디지털 포렌식 시스템 ····· 160
1. 디지털 포렌식 기구 ····· 160
가. Forensic Science Service(FSS) ····· 160
나. FSS 폐쇄에 따른 대응방향 ····· 162
1) 국제표준 인증기준을 통한 법과학서비스 기관의 관리 모색 ····· 162
2) 민간분야 포렌식 서비스의 활용 ····· 163
3) 경찰 과학수사연구소 ····· 164
나. Forensic Science Regulator(FSR) ····· 164
1) 설립 및 기능 ····· 164
2) 책임과 목표 ····· 165
3) FSR의 권한 ····· 168
4) FSR의 실무와 행동규범(Codes of Practice and Conduct) ····· 169
2. 디지털 포렌식 관련 지침 및 가이드라인 -Good Practice Guide for Digital Evidence ····· 172
가. 개요 ····· 172
나. 적용대상 ····· 173

다. 디지털 증거에 관한 원칙 ····· 173
라. 디지털 포렌식 프로세스 ····· 174
1) 계획(Plan) ····· 174
2) 수집(Capture) ····· 174
3) 분석(Analysis) ····· 175
4) 제출(Presentation) ····· 175
5) 일반적 사항(general) ····· 176
제3절 EU의 디지털 포렌식 시스템 ····· 177
1. 유럽 법과학연구소 네트워크(ENFSI) ····· 177
가. ENFSI의 개요 ····· 177
나. ENFSI의 조직체계 ····· 178
다. FIT의 개요 ····· 179
라. 유럽에 있어서 ENFSI의 의의 ····· 180
2. 디지털 포렌식 관련 지침 및 가이드라인 ····· 182
가. Best Practice Manual for the Forensic Examination of Digital Technology ····· 182
1) 목적과 범위 ····· 182
2) 구성내용 ····· 183
나. Guidelines on Digital Forensic Procedures for OLAF staff ····· 191
1) 목적 ····· 191
2) 구성내용 ····· 192
다. Electronic evidence - a basic guide for First Responders ····· 197
1) 목적 ····· 197
2) 구성내용 ····· 197
제4절 독일의 디지털 포렌식 시스템 ····· 202
1. 독일의 디지털 포렌식 모델 구축 현황 분석 ····· 202
가. 연방형사청의 범죄과학 연구소 ····· 202
나. 기술개발·서비스 및 혁신 기술센터(TESIT) ····· 205
다. 니더작센주의 포렌식 과학 연구소 ····· 206
1) 범죄기술연구소 개요 ····· 206
2) 정보통신기술 관련 포렌식 ····· 207
3) 법과학 품질개선 노력 ····· 207
4) 니더작센주 범죄기술연구소의 시사점 ····· 208

라. 독일의 디지털 포렌식 관련 판결 ····· 209
1) 이메일 압수·수색 관련 연방헌법재판소 결정 ····· 209
2) 온라인 수색 관련 연방헌법재판소 결정 ····· 210
마. 독일 범죄과학연구소의 시사점 ····· 211
제5절 네델란드의 디지털 포렌식 시스템 ····· 214
1. 네델란드 디지털 포렌식 연구소((Nederlands Forensisch Institut: NFI) ··· 214
가. 설립목적 ····· 214
나. NFI의 법과학 품질 보장 체계 ····· 215
다. NFI의 결과물 및 서비스 ····· 217
1) 법과학 결과물 제공 ····· 218
2) 법과학 서비스 제공 ····· 222
라. 컨설턴트 서비스 ····· 225
마. 트레이닝, 워크숍 및 교육 제공 ····· 226
바. NFI 모바일 포렌식 절차 ····· 227
사. 네덜란드 포렌식 연구소의 시사점 ····· 232
제6절 주요 외국의 디지털 포렌식 시스템에 있어서의 시사점 ····· 234

| 제4장 | 디지털 포렌식 프로세스 통합을 위한 사전적·예비적 고려사항 (탁희성) ····· 241

제1절 디지털 포렌식 프로세스 통합의 필요성 ····· 243
1. 법률적 프로세스와 기술적 프로세스의 유기적 연계 ····· 243
2. 디지털 포렌식 업무에 대한 일관성 있는 신뢰기준 확보 ····· 245
가. 디지털 포렌식 도구에 대한 신뢰 기준으로서의 검증 ····· 245
나. 디지털 포렌식 분석관에 대한 신뢰 기준으로서 자격인증 ····· 246
다. 디지털 포렌식 프로세스의 통합적 요구사항으로서 디지털 포렌식 분석실에 대한 인증의 확보 ····· 248
제2절 디지털 포렌식 프로세스 구축을 위한 국제적 표준 요건의 충족 ·· 249
1. 디지털 포렌식 프로세스에 대한 인증의 필요성 ····· 249
2. 디지털 포렌식 전문가 자격 인증을 위한 표준 ····· 251
가. 포렌식 전문가 인증위원회 표준(Standards for Accrediting Forensic

Specialty Certification Boards) ····· 251
1) 개요 ····· 251
2) 인증 기구 ····· 251
3) 인증 표준 ····· 251
4) 재인증 ····· 252
5) 최초의 인증을 위한 심사 ····· 253
나. 디지털 포렌식 자격 위원회(DFCB)의 인증 자격 ····· 253
3. 디지털 포렌식 도구에 대한 검증 기준 ····· 253
가. CFTT 프로젝트 ····· 254
나. CFReDS 프로젝트 ····· 255
4. 디지털 포렌식 분석실 인증 표준 ····· 256
가. ISO/IEC 17025 ····· 257
1) 관리요건 ····· 258
2) 기술요건 ····· 260
나. ISO 9001 ····· 265
1) 품질관리시스템(Quality Management System) ····· 265
2) 리더십(Leadership) ····· 266
3) 계획(Planning) ····· 267
4) 지원(Support) ····· 267
5) 운영(Operation) ····· 268
6) 성과 평가(Performance Evaluation) ····· 270
7) 개선(Improvement) ····· 270
다. ISO/IEC 27001 ····· 270
1) 리더십 ····· 271
2) 계획(Planning) ····· 272
3) 자격(Competence) ····· 273
4) 정보의 문서화(Documented Information) ····· 274
5) 운영(Operation) ····· 274
6) 실적 평가(Performance evaluation) ····· 274
7) 개선(Improvement) ····· 274
제3절 디지털 포렌식 프로세스에 대한 법적 심사기준 ····· 275
1. 디지털 증거에 대한 법적 심사기준의 한계 ····· 275
2. 디지털 포렌식과 Daubert Test 기준의 부적합성 ····· 276

가. Daubert standards ····· 277
나. 디지털 포렌식과 Daubert 기준의 부적합성에 대한 논의 ····· 278
다. Daubert 기준의 확장으로서 금호타이어 판결 ····· 279
3. 디지털 포렌식에 적합한 법적 평가기준의 재정립 ····· 279
가. Daubert test에 대한 환상 ····· 279
나. 디지털 포렌식에 적합한 법적 평가기준 재검토 ····· 281

| 제5장 | 디지털 포렌식 프로세스 통합 프레임 구축을 위한 정책적 제언 (탁희성) ····· 283

제1절 디지털 포렌식 프로세스 통합 모델 프레임 ····· 285
1. 디지털 포렌식 프로세스 통합관리시스템 구축 ····· 285
가. 통합관리시스템의 기본 개요 ····· 285
나. 통합관리시스템의 기본원칙 확립 ····· 286
다. 통합관리시스템의 구성 ····· 288
1) 절차적 지침의 수립 및 유지 ····· 288
2) 품질 관리시스템 구축 ····· 289
3) 표준의 적용 및 유지관리 ····· 291
2. 디지털 포렌식 프로세스간 연계시스템 구축 ····· 292
가. 기술적 프로세스와 법률적 프로세스의 연계 ····· 293
1) 압수·수색의 적법성 확보를 위한 프로세스 연계 ····· 293
2) 디지털 증거의 증거능력 확보를 위한 프로세스 연계 ····· 294
나. 포렌식 업무 프로세스간 피드백 시스템 ····· 296
다. 포렌식 업무간 권한 통제시스템 확보 ····· 297
제2절 주요 프로세스별 고려사항 ····· 297
1. 준비 및 수집단계 ····· 297
가. 적법절차 준수 ····· 297
나. 포장과 이송 및 보존 ····· 298
2. 분석 및 추출 단계 ····· 299
가. 디지털 포렌식 분석관(조사관)의 자격 및 전문성 유지 ····· 299
1) 자격 및 능력 검증 ····· 299

2) 교육훈련 ····· 300
3) 포렌식 분석관으로서의 의무와 책임 ····· 300
나. 디지털 포렌식 도구 및 방법론 ····· 301
3. 결과물 제출 단계 ····· 302
가. 결과물에 대한 검증 ····· 302
나. 보고서 작성 ····· 303
4. 법정 증언단계 ····· 304
가. 포렌식 분석관에 의한 법정 증언 준비 ····· 304
나. 효과적인 증언 방식 ····· 305
제3절 디지털 포렌식 프로세스 통합을 위한 정책적 제언 ····· 306
1. 디지털 포렌식 프로세스 통합을 위한 모델 프레임 ····· 306
2. 디지털 포렌식 프로세스 통합모델 구축을 위한 제언 ····· 308
가. 법과학적·기술적 관점에서의 제언 ····· 308
1) 디지털 포렌식의 표준화에 대한 요청 ····· 308
나. 디지털 포렌식 도구 검증절차 마련 ····· 309
다. 디지털 포렌식 전문가에 관한 기술적·법적·윤리적 기준 확립 ····· 311
3. 디지털 포렌식 프로세스 통합을 위한 정책적 제언 ····· 312
가. 기관간 디지털 증거에 대한 chain of custody 방식의 표준화 ····· 312
나. 디지털 포렌식 결과에 대한 재검증 절차 도입 ····· 313
다. 형사소송법 개정에 따른 디지털 포렌식에 대한 법적 판단기준 마련 ···· 315

참고문헌 ····· 319

Abstract ····· 333

그림 차례

[그림 1] DFRWS Model ····· 48
[그림 2] Abstract Digital Forensic Model ····· 50
[그림 3] IDIP Model ····· 51
[그림 4] six phases in the physical crime scene investigation ····· 53
[그림 5] six phases in the digital crime scene investigation ····· 53
[그림 6] EDIP Model ····· 54
[그림 7] CFFTPM Phase ····· 56
[그림 8] DFMMIP Model ····· 58
[그림 9] SRDFIM 모델 ····· 61
[그림 10] HDFIP 모델 ····· 65
[그림 11] IDFPM 모델 ····· 71
[그림 12] EU내 디지털 포렌식 연구소 ····· 182
[그림 13] NFI 디지털 수사 절차 ····· 221
[그림 14] NFI 모바일 포렌식 순서도 1/3: (경찰청 국외훈련 보고서) ····· 228
[그림 15] NFI 모바일 포렌식 순서도 2/3: (경찰청 국외훈련 보고서) ····· 229
[그림 16] NFI 모바일 포렌식 순서도 3/3: (경찰청 국외훈련 보고서) ····· 230
[그림 17] 현장 보존 프로세스의 순서도 1/2: (경찰청 국외훈련 보고서) ····· 231
[그림 18] 현장 보존 프로세스 순서도 2/2: (경찰청 국외훈련 보고서) ····· 232
[그림 19] 우리에게 주는 시사점 ····· 235
[그림 20] 디지털 포렌식 프로세스 통합관리시스템 모델 프레임 ····· 306
[그림 21] 단계별 프로세스 연결망내 단계별 표준요구사항 ····· 307

국문요약

1. 연구목적과 방법

디지털 포렌식은 디지털 기기를 매개로 하여 발생한 특정행위의 사실관계를 법정에서 규명하고 증명하기 위한 기술에 기반한 방법과 절차라고 할 수 있다. 특히 디지털 데이터가 법적으로 유효한 증거자료로서 제시되기 위해서는 디지털 데이터의 물리적·논리적 취약성을 뒷받침할 수 있는 기술적인 방법을 통해 진정성·무결성·신뢰성·원본성 등이 확보되어야 하는데, 디지털 포렌식은 이와 같이 디지털 데이터의 입증가치를 수집단계에서부터 폐기단계에 이르기까지 신뢰성 있게 유지할 수 있도록 하는 기술적·절차적·법적 요소로 구성된 포괄적인 프로세스라고 할 수 있다. 따라서 디지털 포렌식 분야는 IT 기술의 개발과 더불어 지속적으로 변화되어야만 하고, 항상 새로운 지식과 기술에 개방되어 있어야만 한다. 특히 디지털 포렌식을 활용한 수사에 있어서는 다양한 IT 지식과 기술이 뒷받침되어야만 하고, 이를 위해서는 다양한 IT 전문가 그룹의 네트워크 구축을 통해 각 분야에서 요구되는 지식과 기술들이 언제든지 신속하게 공유될 수 있어야 한다.

현재 우리의 경우 각 정부기관의 필요에 따라 디지털 포렌식 시스템이 독자적으로 운용되고 있으며, 각 기관별 운용지침이 있는 정도이며, 각 기관들이 모범으로 삼아 준수할 수 있는 디지털 포렌식 지침은 아직 마련되어 있지 않다. 즉 현재 우리의 디지털 포렌식 시스템은 그와 같은 표준적인 운용절차나 good practice를 마련하지 못한 채 운용되고 있기 때문에 언제든지 그 신뢰성 검증에서 이의가 제기될 우려가 있고, 따라서 어렵게 수집하고 분석한 자료들을 증거로 활용하지 못하는 문제가 발생할 수 있다. 더욱이 각 기관별로 디지털 포렌식 시스템을 운용하면서 기관간 협업이 제대로 이루어지지 못함으로 인해 급속히 변화하는 지식과 기술을 빠르게 습득하고 활용하는데 한계가 있을 수 밖에 없다고 할 것이다.

이에 본 연구는 우리나라 형사사법기관별로 운용하고 있는 디지털 포렌식 시스템을 검토하여 실무에서 발생하고 있는 문제점이 무엇이고, 실무에서 요구되는 디지털 포렌식 시스템의 구체적인 내용이 무엇인지를 파악하여 IT 기술수명의 짧은 주기와 포렌식 수사의 신속성과 기밀성에 부합할 수 있는 전체적인 프로세스를 모색해 보고자 한다. 이와 관련하여 디지털 포렌식 분야에 있어서 앞서가고 있는 미국, 영국 등 주요 국가의 디지털 포렌식 시스템을 비교분석하여 봄으로써 향후 다양한 디지털 기술과 관련 범죄수사에 대한 대응역량을 강화할 수 있는 통합적인 디지털 포렌식 프로세스 모델을 제시해보고자 하는데 연구목적을 두고 있다. 이를 위한 연구방법으로는 먼저 디지털 포렌식의 기본 프레임에 대한 논의와 아울러 기존의 디지털 포렌식 프로세스 모델의 유형을 검토해 보고자 한다. 그리고 현재 각 정부기관에 설치되어 운용중인 디지털 포렌식 기구의 현황 및 운용방식 등을 검토함과 아울러 디지털 포렌식 업무에 종사하는 전문가들이 디지털 증거를 취급함에 있어서 필요성이 요구되는 디지털 포렌식 프로세스와 그 한계가 무엇인가를 전문가 인터뷰를 통해 살펴보고자 한다. 또한 주요 국가 - 미국, 영국, 독일, 네델란드, EU- 의 디지털 포렌식 시스템과 프로세스의 수준을 비교검토하여, 우리의 디지털 포렌식 프로세스 마련에 도움이 될 수 있는 방향성이 무엇인가를 제시해 보고자 한다.

마지막으로 통합적인 디지털 포렌식 프로세스의 주요 기능과 인증 기준·표준화지침·기술적 프로세스와 법률적 프로세스의 연계방안 등을 검토하여, 디지털 증거의 법적 신뢰도를 제고할 수 있는 디지털 포렌식 프로세스 모델 프레임을 제시해 보고자 한다.

2. 디지털 포렌식에 있어서 새로운 접근방식의 필요성

디지털 포렌식 초기에는 포렌식 도구와 분석결과의 신뢰성에 주로 논의의 초점이 맞추어졌고, 그 다음에는 Chain of Custody, 즉 보관의 연속성을 통한 무결성의 입증에 초점이 맞추어졌으며, 이제는 전체적인 디지털 포렌식 프로세스 자체에 대한 신뢰성으로 논의의 중심이 옮겨가고 있다고 보여진다. 즉 기술수준이 고도화될수록 오히려 디지털 데이터의 입증가치를 확보할 수 있는 상황은 점점 더 취약해지고 있기

때문에, 디지털 증거를 확보해서 폐기할 때까지의 각 단계별로 고도의 일관성과 검증 가능성을 유지할 수 있는 과학적 입증방법이 요구되고 있고, 이를 뒷받침하기 위해 신뢰할 수 있는 프로세스 구축의 필요성과 중요성에 대한 인식이 높아져 가고 있다고 할 수 있다.

1984년 초부터 미국의 FBI와 다른 사법기관들이 컴퓨터 증거를 조사하기 시작하면서 조사를 수행함에 있어서 채택된 프로세스나 절차가 조사의 결과에 직접적 영향력을 갖는다는 인식을 갖게 되었고, 따라서 공식화된 프로세스가 도입되기 시작했다. 즉 컴퓨터 포렌식에 있어서 부적절한 프로세스를 선택하는 경우 불완전하거나 실효성 없는 결과를 초래할 우려가 있을 뿐만 아니라, 임의적이거나 구조화되지 않은 방식으로 확보된 증거들이 법정에서 허용되지 않을 수 있는 위험이 있다고 보았던 것이다.

이와 같이 구조화된 표준 프로세스의 존재는 컴퓨터 포렌식 조사관이 준수해야할 적절한 매카니즘을 제공하는 방식이 되기 때문에, 수년간에 걸쳐 다수의 컴퓨터 포렌식 조사 프로세스가 새롭게 개발되거나 기존모델에 대한 개선방안들이 제안되어왔다.

그동안 제안되어온 디지털 포렌식 프로세스 모델들이 절차적 프레임을 제시하는 방식의 변화를 보면, 이전 모델이 제시한 결과를 분석한 후 이를 토대로 새로운 단계를 추가하거나 기존 단계를 보다 구체적으로 세분화하여 새로운 프로세스의 프레임을 제시하는 방식, 기존 모델들이 제시한 유효한 단계들을 서로 통합하거나 조화시키는 방식으로 프로세스 프레임을 제시하는 방식을 취하고 있다. 특히 최근으로 올수록 디지털 포렌식 프로세스 모델은 통합과 조화라는 개념을 사용하고 있으며, 그와 함께 절차상 표준의 준수를 중요한 기준으로 삼고 있음을 볼 수 있다. 즉 표준화된 절차의 활용이 디지털 증거의 허용가능성을 높일 수 있을 뿐만 아니라, 전체적인 포렌식 조사 프로세스에 있어서의 사람에 의한 오류를 최소화할 수 있다는 인식이 높아져가고 있다고 볼 수 있다.

3. 현행 디지털 포렌식 시스템 및 프로세스 비교

대검찰청은 국가 디지털 포렌식 센터를 두고 있으며, 그 안에 디지털 수사담당관실

에서 디지털 포렌식 업무를 수행하고 있다. 하지만 폭증하는 디지털 증거분석 업무로 말미암아 압수수색 및 증거분석 지원을 위해 7개의 지검내에 디지털 포렌식 수사팀을 확대하여 설치·운영중에 있다.

검찰은 디지털 포렌식을 위하여 D-NET 시스템을 두고 있는데, 이는 디지털수사팀을 온라인으로 연계하여 신속한 수사지원시스템을 제공하고, 디지털증거분석 업무의 편의성 및 증거 관리의 엄격성을 향상시키기 위한 디지털수사 네트워크라고 할 수 있다. D-NET은 디지털 수사 통합업무관리시스템(DFIS II), 디지털 증거관리시스템, 통합디지털 증거분석 시스템(IDEAS), 원격디지털수사공조시스템 등으로 구성되어 있다. 검찰은 디지털 포렌식 업무의 적법성 확보를 위한 규정 및 내부 지침, 실무매뉴얼 등을 두고 있는데, 디지털 포렌식 수사관의 증거 수집 및 분석 규정(2015.7.16.개정), 디지털 포렌식 압수지원 절차에 관한 지침 (2015.7.16.개정), 전국 디지털수사망 운영지침 개정(2015.7.16.개정), 과학수사 실무매뉴얼 등이 그것이다.

경찰청 디지털 포렌식센터는 사이버테러대응센터 기술지원팀으로 시작되었다가 2010년 디지털 포렌식팀으로 변경되었으며, 2014년 사이버안전국이 출범하면서 디지털 포렌식센터로 개편되었다. 경찰청 사무분장규칙 제27조의4에 규정된 디지털 포렌식센터의 분장업무의 내용을 보면, 디지털 포렌식 기획, 첨단기법개발, 모바일포렌식, 컴퓨터포렌식으로 구분되어 있으며, 정책기획 및 지원, IT 환경 분석 및 신규 추적기법, 도구 개발, 스마트폰 등 모바일기기 분석기법 개발, 악성코드 등 디지털기기 증거분석기법 개발 등 의 업무를 수행하는 것으로 규정되어 있다. 경찰은 디지털 포렌식 절차와 관련한 근거규정으로 '디지털 증거 수집 및 처리 등에 관한 규칙'[1]을 두고 있으며, 실무매뉴얼로는 '현장수사관을 위한 디지털 증거 압수수색 길라잡이'와 '디지털 증거처리 표준 가이드라인'이 있다.

한편 현재 디지털 포렌식 업무를 수행함에 있어서 전문가들이 인식하고 있는 현행 디지털 포렌식의 문제점과 한계가 무엇이고, 디지털 포렌식 프로세스에 대한 인식은 어떠한지 살펴보고자 디지털 포렌식 전문가들을 대상으로 개별 또는 집단 인터뷰를 실시하였다.

---

1) 경찰청 훈령 제766호, 2015.5.22. 제정.

인터뷰 방법은 개별 인터뷰의 경우에는 해당 기관을 직접 방문하여 디지털 포렌식 담당자를 대상으로 하였고, 집단 인터뷰의 경우에는 정부기관, 대학 그리고 민간영역(로펌, 디지털 포렌식 업체 등)에서 디지털 포렌식 업무를 직접 수행하거나 지원하고 있는 전문가들을 대상으로 하였다. 개별 인터뷰는 3개 정부기관에서 6명에 대해 실시하였고, 집단 인터뷰는 15명에 대해 실시하였다.

전문가 인터뷰 항목은 크게 해당 기관의 디지털 포렌식 업무 구조, 전체적인 디지털 포렌식 절차 진행 방식 및 관련 업무지침 내용, 디지털 포렌식 도구 관련 사항, 디지털 포렌식 전문가 관련 사항, 형사소송법 개정에 따른 준비 현황 등으로 구성하였다.

인터뷰 결과에 나타난 현행 디지털 포렌식 프로세스의 한계는 다음과 같다.

첫째, 디지털 포렌식 전문인력의 부족이다. 인터뷰 조사 결과, 현행 디지털 포렌식 프로세스가 디지털 포렌식의 절차적 표준에서 일반적으로 요구되는 사항들을 제대로 준수하지 못하는 가장 큰 장애요소로서 전문인력의 부족을 지적하였다. 즉, 디지털 증거의 압수·수색을 요하는 현장수요는 급증하고 있는데 비해서 디지털 포렌식 조사를 전담할 수 있는 전문인력의 공급은 늘어나지 못하고 있고 오히려 축소되는 기관들도 있는 것으로 나타났다. 이러한 디지털 포렌식 업무 인력의 부족현상은 포렌식 조사관 1인이 분석한 결과에 대하여 다른 분석관에 의한 교차검증도 사실상 불가능하게 만듦으로써 분석결과의 신뢰성을 보다 구체적으로 담보하기 어렵게 하고 있다는 점에서도 문제가 있다고 할 것이다.

둘째, 디지털 포렌식 도구의 신뢰성 확보의 한계이다. 인터뷰 결과에 따르면, 거의 모든 디지털 포렌식 전문가들 - 학계나 실무계 모두 -은 도구 인증의 필요성에 대한 요구가 매우 높은 것으로 나타났다. 즉 현재 상용도구이건 자체개발 도구이건 간에 기능적 요구사항에 대한 확인 및 검증을 할 수 있는 공식적인 절차나 기구가 없기 때문에, 해당 도구를 이용하는 전문가의 입장에서도 신뢰성 내지 정확성 문제에 확신을 갖기 어려운 측면이 있다는 것이다. 디지털 포렌식 도구의 인증과 관련하여 전문가들은 현재 우리의 IT 기술력에 비추어 볼 때, 민간주도하에 미국의 CFTT와 같이 디지털 포렌식 도구의 기능적 요구사항 구현의 정확성을 확인 내지 검증할 수 있는 시스템을 만들 수는 있지만, 민간주도 인증시스템을 만드는 경우 해당 기관의 공신력과 전문성을 문제 삼을 여지가 있기 때문에 정부 주도의 공신력 있는 인증기구의

도입이 필요하다는 의견을 제시했다.

셋째, 디지털 포렌식 프로세스 표준화 작업에 대한 인식의 한계이다. 유럽이나 미국의 경우와 달리 우리의 경우에는 아직까지는 디지털 포렌식 프로세스 표준화에 대한 논의가 거의 행해지고 있지 않다. 디지털 포렌식 업무를 담당하는 전문가들도 프로세스 표준화의 필요성에 대한 인식이 별로 없으며, ISO 인증을 받기 위한 요구사항들이 우리의 디지털 포렌식 업무와는 상당한 괴리가 있어서 ISO 인증에 대해서는 부정적인 입장을 나타내는 것이 일반적인 경향이라고 할 것이다. 실제 인터뷰에 응했던 대부분의 전문가들이 프로세스 표준화에 대해서는 거의 생각해 본적이 없었던 것으로 나타났으며, 프로세스 표준화의 필요성에 대해서도 현재의 절차로 충분히 chain of custody를 유지할 수 있고, 법원에서도 프로세스 표준이나 인증문제가 다투어지지 않는 현실에서 표준화에 대한 논의는 큰 의미가 없는 것으로 생각하는 것으로 나타났다.

넷째, 2016년 5월 29일 형사소송법 제313조 제2항이 개정되면서, 진술서의 작성자가 공판준비나 공판기일에서 그 성립의 진정을 부인하더라도 과학적 분석결과에 기초한 디지털 포렌식 자료, 감정 등 객관적 방법으로 성립의 진정함이 증명되는 때에는 증거로 할 수 있게 되었다. 이 규정의 개정으로 앞으로 디지털 포렌식 분야에서 논의되어야 할 사안은 디지털 포렌식 전문가의 자격과 그 분석결과에 대한 신뢰도 검증, 제출된 디지털 포렌식 자료의 기초가 된 과학적 분석이 무엇인가에 대한 입증 등이라 할 수 있다. 이와 관련하여 정부기관의 포렌식 전문가들은 법정증언을 위한 훈련의 필요성 및 디지털 포렌식에 적용된 과학적 기술의 신뢰도 입증, 분석결과의 신뢰성 입증 방식 등의 문제에 대하여 고민은 하고 있지만, 아직까지는 준비가 안되어 있는 것으로 보여졌다.

4. 주요 국가들의 디지털 포렌식 시스템 및 프로세스

미국의 디지털 포렌식 시스템을 보면, NIJ(National Institute of Justice), RCFL(Regional Computer Forensic Laboratory), DCFL(Defense Computer Forensic Laboratory)를 중심으로 디지털 포렌식 업무가 수행되고 있으며, 이들 기관들은 ISO 17025 인증을 받았거나 받고자 노력하고 있는 상태에 있다. 디지털 포렌식

업무 관련 지침 및 가이드라인으로는 Electronic Crime Scene Investigation: A Guide for first Responders, Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors, Forensic Examination of Digital Evidence: A Guide for Law Enforcement를 활용하고 있다.

영국의 디지털 포렌식 시스템은 Forensic Science Service(FSS) 폐쇄 이후 민간분야 포렌식 서비스 업체와 경찰 과학수사연구소로 업무가 이전되면서 ISO 17025인증 확보가 문제가 되었지만, Forensic Science Regulator(FSR)가 설립되어 법과학서비스 제공자들이 공통적인 표준을 준수할 수 있도록 자문과 지침을 제공하고 있다. FSR은 실무와 행동규범(Code of Practice and Conduct)을 마련하였는데, 이는 ISO/IEC 17025에 맞추어 조정된 것으로 실험에 기반한 법과학 서비스의 제공자들이 형사사법시스템 내에서의 고객의 요구사항을 충족하는 일관된 결과와 서비스를 제공할 수 있는 능력을 입증할 수 있는 관리시스템에 관한 요건들을 명시하고 있다. 이와 함께 영국은 Association of Chief Police Officers(ACPO) Crime Business Area에 의해 제작된 Good Practice Guide for Digital Evidence을 토대로 하여 디지털 증거에 관한 기본원칙과 디지털 포렌식 프로세스 단계별 구성요소들을 구체적으로 명시하고 있다.

한편 유럽은 법과학 분야의 전문지식을 공유하고, 교환하기 위해서 만들어진 네트워크인 ENFSI(European Network of Forensic Science Institutes)을 두고 있는데, 크게 Quality & Competence Committee와 Research & Development Committee의 두 상임위원회가 있다. 전자는 주로 자질과 경쟁력을 발전시킬 수 있는 정책, 전문가작업그룹 및 회원들에 대한 조언, 회원 연구소들에 대한 최선의 실무와 국제적 표준 적용과 관련된 업무들을 수행하고, 후자는 ENFSI의 연구개발 정책, 전문가작업그룹 및 회원들에 대한 연구개발 관련 조언, 연구소간 국제적인 협동연구 촉진 등의 업무들을 수행하고 있다.[2] 그리고 ENFSI에는 총 17개의 전문가작업그룹이 존재하고 있다. 이 전문가 작업그룹 가운데 정보기술 포렌식 작업그룹((Forensic Information Technology: FIT)이 2015년 11월 “Best Practice Manual for the Forensic Examination of Digital Technology”이라고 하는 디지털 포렌식 매뉴얼을 만들어서

2) http://www.enfsi.eu/about-enfsi/structure/standing-committees;2016.9.30.

회원 연구소에 제공한 바 있다. 해당 매뉴얼은 ENFSI 회원 연구소들에 대해 관련 절차에 대한 프레임워크와 품질재고 원칙들, 훈련 과정과 포렌식 조사를 위한 접근방법 등을 제시해 주고 있다. 특히 해당 매뉴얼은 국제적으로 표준화된 절차가 각 지역에 맞게 적용될 수 있도록 지원을 해 주고 있다. 이외에도 유럽 국가들에 적용가능하도록 마련된 디지털 포렌식 지침 및 가이드라인으로는 Guidelines on Digital Forensic Procedures for OLAF staff, Electronic evidence - a basic guide for First Responders 등이 있다.

주요국의 디지털 포렌식 시스템 구축현황을 살펴보면 크게 네 가지 부분에서 주목해야할 점들이 있다. 첫째로, 디지털 포렌식에 있어서는 반드시 국제규격을 준수할 필요가 있다는 것이다. 앞서 살펴본 바와 같이 미국은 물론 유럽 주요 국가들도 국제표준인 ISO의 규격과 유럽의 규격인 ENFSI의 규격을 만족시키는 범위 내에서 디지털 포렌식 업무를 수행하고 있다. 특히 유럽의 경우 디지털 포렌식 가이드라인내에 ISO 표준의 적용 및 준수를 요구하고 있다. 이와 같이 디지털 포렌식 가이드라인에 규정된 표준을 적용하는 경우 어느 기관에서 디지털 포렌식을 수행하더라도 해당 결과에 대한 품질을 보증 받을 수 있게 될 것이고, 법원의 입장에서도 그 결과를 증거로 채택하지 않을 이유가 없게 될 것이다. 이는 우리 법원 뿐 아니라 해당 결과가 다른 국가의 법원에서 사용되는 경우에도 매우 유용하므로 디지털 포렌식에 있어서는 국제적인 표준을 준수할 필요가 있다. 둘째, 디지털 포렌식 기관들은 자신의 기관에 적합한 모델을 설정할 필요가 있다는 것이다. 다만, 해당 모델은 단순히 자신의 기관에만 적합한 방식으로 만들기 보다는 국제기준 및 지역기준을 수용하여 자신의 기관에 맞도록 커스터마이징 한 것이어야 할 것이다. 물론 우리나라의 경우에는 지역기준이라는 것이 없기 때문에 유럽의 ENFSI 또는 미국의 의 규격을 참조하면 유용할 것이다.

5. 디지털 포렌식 프로세스 통합의 필요성

디지털 포렌식 프로세스는 단순히 디지털 포렌식 업무내용을 순서에 따라 배치하는 데서 그치는 것이 아니라, 전체 프로세스에 적용되는 관리 및 운용정책과 시스템 내에서 각 단계별로 디지털 증거가 이동하는 과정이 정확하게 기록되고, 각 단계별

구성요소에 대한 표준화 요구사항이 적용되어야 한다. 이렇게 함으로써만 디지털 포렌식 업무에 사용되는 프로세스와 절차가 적합한 품질을 유지할 수 있고, 법정에 신뢰성 있는 결과를 제공할 수 있다고 할 것이기 때문이다. 따라서 이와 같이 포렌식 업무 절차를 전체적으로 관리·통제할 수 있다는 점에서 통합적인 포렌식 프로세스로 규정될 수 있을 것이다. 디지털 포렌식에 있어서 프로세스 구축을 통한 각 절차의 통합적인 관리 및 통제의 필요성이 요구되는 이유는 다음과 같다.

첫째, 디지털 증거를 수반하는 사건에 있어서는 법률적 지식과 수사실무상의 경험을 지닌 수사관과 과학적 지식과 기술적 경험을 지닌 디지털 포렌식 조사관(분석관)의 유기적인 협조와 연계가 전제되지 않으면, 증거의 신뢰성을 물론이고 수사절차 자체에 대한 신뢰성 까지 이의가 제기될 수 있다. 따라서 법률적 프로세스와 기술적 프로세스의 유기적인 연계 및 상호 협력지원을 가능하게 하기 위해서는, 수사기관내의 디지털 포렌식 업무에 대한 거버넌스 프레임워크를 확대하여 기존의 수사업무를 디지털 포렌식 프로세스내로 통합함으로써 일관된 정책적·기술적 프레임안에서 각 단계별 프로세스간 피드백과 인터페이스를 구축할 필요가 있다.

둘째, 디지털 포렌식 프로세스를 통해 신뢰할 수 있는 결과를 산출하고, 확보한 정보의 품질이 강력한 입증가치를 유지하기 위해서는 디지털 포렌식 프로세스내에서 요구되는 인적·기술적 품질수준을 증명할 수 있는 표준적인 기준이 포렌식 프로세스 안에 적용되어 있어야 한다.

셋째, 디지털 포렌식 프로세스의 통합에 있어서 궁극적으로 확보되어야 하는 것은 디지털 포렌식 분석실 자체에 대한 인증 확보의 문제라고 할 수 있다. 이는 앞에서 기술한 디지털 포렌식 절차별 요구사항 - 절차적 연계성, 도구, 분석관 -을 모두 포괄하는 문제라고도 할 수 있다. 즉, 디지털 포렌식 분석실 자체에 대한 국제적 표준에 따른 인증을 확보하게 되면 절차적·도구적·인적 신뢰성도 함께 인증되는 것이고, 디지털 포렌식 업무품질 자체에 대한 신뢰성을 인정받는 것이기 때문에 가장 기본적이고 중요하지만 가장 어려운 문제라고도 할 수 있다.

6. 디지털 포렌식 프로세스 통합을 위한 사전적· 예비적 고려사항

디지털 포렌식 프로세스로서 지털 데이터를 수집 및 선별하여 분석하는 과정 - 탐색, 복구, 추출 등 -을 거쳐, 결과를 제출하는 절차, 그 과정에서 사용되는 디지털 포렌식 도구, 그리고 그 도구를 사용하여 포렌식 절차를 진행하는 디지털 포렌식 분석관, 그리고 그에 의해 산출된 결과를 기술한 포렌식 보고서에 이르는 모든 것이 과학적 지식을 기반으로 한 전문성 그리고 기술적 지식과 경험이 요구되는 영역이라 할 수 있다. 이와 같이 과학과 기술이 지배하는 영역을 법적 판단안으로 가져와서 법적인 관점에서의 신뢰성을 판단하기 위해서는, 최소한 그 적용된 과학과 기술이 유효하다는 검증을 전제로 독자적인 사법적 평가가 이루어져야 할 것이다. 즉 디지털 증거는 디지털 기술에 적합한 도구에 기반하여 산출되는 것이기 때문에, 물리적으로는 내용 확인이 어려운 형태의 디지털 증거를 인식가능한 상태의 자료로 전환하여 혐의사실을 입증할 수 있는 형태로 법정에 제출하기까지의 과정에 적용된 과학적 방법과 기술적 원리에 대한 이해가 전제되어야 그 신뢰성을 판단할 수 있다고 할 것이다. 다만 과학적 이론과 기술적 운용방식을 제대로 이해하기 어려운 판사에게 과학적 이론이나 기술의 운용이 정확한 것인가의 여부를 결정하도록 요구할 수는 없지만, 최소한 과학으로서의 건전성 또는 응용 기술로서의 유효성을 적합하게 하는 기준을 충족하는가의 여부를 확인하여 판단하도록 요구할 필요는 있다고 할 것이다.

디지털 기술의 발전과 함께 디지털 포렌식 기술의 개발속도도 점차 빨라지고 있고, 요구되는 기술영역도 점차 다양화되어 가고 있는 상황에서, 도구나 전문가 또는 프로세스에 대한 공식적인 검증도 없이 그에 대한 법적 신뢰를 어떻게 판단할 것인가에 대한 문제는 언제든지 제기될 수 있다고 할 것이다. 그리고 형사소송법 개정으로 “과학적 분석결과에 기초한 디지털 포렌식 자료에 의한 증명”으로 증거능력을 인정할 수 있게 되었으므로, 디지털 포렌식 자료의 신뢰성 뿐만 아니라 그 기초가 된 과학적 분석의 신뢰성에 대한 입증이 요구될 수 밖에 없다. 따라서 이에 대한 법적 판단기준을 어떻게 정립할 것인가에 대한 논의가 필요하다고 할 것이다.

7. 디지털 포렌식 프로세스 통합을 위한 모델 프레임

디지털 포렌식 프로세스가 일관성과 신뢰성을 갖출 수 있도록 함에 있어서는 그 전체적인 프로세스 운용에 공통적으로 적용할 수 있는 통합관리시스템을 갖추는 것이 전제되어야 한다. 즉, 기관이 수행한 디지털 포렌식 프로세스에 의해 산출된 결과의 정확성 및 신뢰성에 영향을 미칠 수 있는 주요 요인 - 문서화된 절차의 정확성, 직원에 대한 교육·훈련, 프로세스의 지속적인 개선 및 유지, 포렌식 업무수행을 위한 환경적 조건, 기관이 포렌식 업무에 사용하는 하드웨어, 소프트웨어, 장비 등 -이 적절히 관리 및 통제할 수 있는 관리시스템이 필요하다고 할 것이다.

통합관리시스템은 디지털 포렌식 업무를 수행하는 기관의 모든 영역 - 즉, 시설, 직원, 도구 및 장비, 절차, 교육 훈련 등 -, 그리고 수행되는 모든 활동 - 수집, 분석, 기록, 보존, 증언 등 -에 적용되어야 한다. 즉 통합관리시스템은 디지털 포렌식 업무를 수행하는 기관에 있어서의 모든 지침·절차·규정·표준·인증 등을 포괄하는 표준운영절차이자, 기관의 디지털 포렌식 업무목표 즉 디지털 증거의 신뢰성 확보를 위한 일관된 정책적 뒷받침이라고 할 수 있다. 이러한 접근방법은 하나의 일관된 시스템에서 디지털 포렌식 업무 프로세스와 절차들을 총괄적으로 관리할 수 있게 할 뿐만 아니라, 업무간 효율적 연계를 가능하게 함으로써 포렌식 프로세스가 관련 업무에 적합한 방식으로 운용·심사·유지·통제된다는 것을 보장할 수 있게 한다.

디지털 포렌식 기관은 신뢰할 수 있는 디지털 증거를 확보하기 위한 디지털 포렌식 프로세스 통합관리시스템을 구축함에 있어서 기본적으로 준수되어야 할 다음과 같은 업무원칙을 가지고 있어야 한다.

첫째, 디지털 포렌식 프로세스 전체에 걸쳐 디지털 증거는 변경되어서는 안된다.

둘째, 디지털 포렌식 업무를 수행하는 직원은 관련 자격과 교육훈련 기록을 유지해야 한다.

셋째, 디지털 증거에 취해진 모든 조치들은 엄격히 기록되어야 한다.

넷재, 디지털 증거와 관련한 모든 법규와 관련 원칙들을 준수해야 한다.

또한 디지털 포렌식의 신뢰성 확보와 관련하여 요구되는 국제적인 표준으로서 ISO 인증이 요구되는 상황하에서 ISO 표준에 따른 구체적인 기준들을 준수해야 하기 때문

에, 이러한 표준들이 통합관리시스템을 통해서 유지 및 관리될 수 있도록 해야 할 필요성이 있다고 할 것이다.

통합관리시스템이 전체적인 디지털 포렌식 프로세스에 대한 정책적인 측면과 절차적인 측면에서의 요구사항을 총괄적으로 관리하는 것이라고 본다면, 프로세스 연계시스템은 그러한 정책적·관리적 요구사항이 적용된 보다 세부적이고 구체적인 실무상 업무연계 프로세스라고 할 수 있을 것이다. 즉 디지털 증거를 수반하는 사건처리가 이루어지는 실무에서 이러한 법률적·기술적·정책적 분야가 체계적이고 유기적으로 연계될 수 있는 표준업무 프로세스를 개발하여, 서로의 업무에 대한 협조와 지원, 피드백이 가능한 시스템이 갖추어질 필요가 있다고 할 것이다. 이를 위해서는 먼저 기술적 프로세스와 법률적 프로세스의 연계가 가능하도록 해야 하며, 포렌식 업무 프로세스간 피드백 시스템과 포렌식 업무간 권한 통제시스템이 확보될 필요가 있다.

주요 프로세스별 고려해야 할 사항은 다음과 같다고 할 수 있다. 준비 및 수집단계에서는 적법절차 준수와 포장과 이송 및 보존절차 확보, 분석 및 추출단계에서는 디지털 포렌식 분석관의 자격 및 전문성 유지, 디지털 포렌식 도구 및 방법론을 확보해야 할 것이다. 결과물 제출단계에서는 결과물에 대한 검증절차 및 신뢰성 있는 보고서 작성이 이루어져야 하고, 마지막 법정 증언단계에서는 포렌식 분석관에 의한 법정 증언에 대비한 훈련, 효과적인 증언방식 교육 및 훈련을 통해 결과의 신뢰성이 훼손되지 않도록 해야 할 것이다.

8. 디지털 포렌식 프로세스 통합을 위한 정책적 제언

가. 법과학적·기술적 관점에서의 제언

디지털 포렌식 업무를 수행하는 기관에서 디지털 포렌식과 관련한 모든 절차- 법적, 기술적 - 가 일관된 프로세스안에서 진행될 수 있도록 하기 위해서는 이를 포괄하여 관리할 수 있는 통합관리시스템이 필요하다고 할 것이다. 그리고 이러한 디지털 포렌식 프로세스 통합관리시스템을 통해서 포렌식 업무품질유지, chain of custody를 통한 증거의 무결성 담보, 그리고 궁극적으로 디지털 포렌식 자체에 대한 신뢰성을

확보하기 위해서는 품질관리시스템, 프로세스 연계시스템, 표준운영정책시스템이 하위범주를 구성할 필요가 있다. 통합관리시스템이 디지털 포렌식 프로세스 통합을 위한 정책적·관리적 프레임이라고 한다면, 실무적인 포렌식 프로세스 통합은 프로세스 연계시스템을 통해서 확보될 수 있다고 할 것이다. 즉 프로세스 연계시스템하에서 단계별 프로세스 연결망을 구축하는 것이 그것인데, 준비 단계, 수집 단계, 조사 및 분석 단계, 제출 단계, 증언 단계, 보존 및 관리 단계를 선순환적 피드백이 가능하도록 구성하는 것이다.

디지털 증거에 대한 신뢰를 뒷받침할 수 있는 디지털 포렌식이 법정에서 신뢰할 수 있는 기술과 절차로서 허용되기 위해서는 디지털 포렌식 분야에 적용가능한 국제적 표준에의 인증, 포렌식 프로세스에 대한 표준적인 지침의 활용 등이 논의되는 것은 필연적이라 할 수 있다. 국내 디지털 포렌식의 현실적 여건에 비추어 볼 때 디지털 포렌식을 담당하는 핵심기관들 조차 ISO 인증이 용이하지는 않은 것으로 보인다. 하지만 디지털 포렌식에 있어서 기술적·절차적 표준을 마련하고자 하는 노력은 앞으로 더욱 증가할 수 밖에 없는 디지털 증거의 현실적 필요성에 비추어 볼 때, 그리고 형사소송법 개정으로 디지털 포렌식 자료에 대한 정확성 및 신뢰성에 대한 입증을 요하는 법적 기준에 부합하기 위해서는 절대적으로 필요한 작업이라 할 것이다.

현재 다양하게 개발되어 사용되고 있는 디지털 포렌식 도구가 그 기능적 요구사항에 부합하게 작동하고, 정확한 결과를 산출한다는 것을 테스트하고 공식적으로 확인해 줄 수 있는 절차가 없기 때문에, 국제적으로 검증된 몇몇 도구를 제외하고는 언제든지 법정에서 그 도구의 정확성 및 신뢰성을 문제삼을 수 있고, 그에 의해 산출된 디지털 증거의 신뢰성에 대해서도 이의가 제기될 수 있다. 이와 같이 디지털 포렌식 도구를 검증함에 있어서는 그 기술적 요구사항의 정확한 구현 및 산출결과의 정확성에 대한 확인도 중요하지만, 완벽한 도구란 불가능하기 때문에 도구에 내재된 결함 및 결과산출에 있어서의 오류율이 결과의 신뢰성을 담보하는데 있어서 용인가능한 수준인지에 대한 확인도 필요하다고 할 것이다. 미국 국립표준기술연구소(NIST)의 CFTT 프로젝트를 모델로 삼아 디지털 포렌식 도구의 검증방법론을 개발하고, 도구에

대한 공식적인 테스트와 테스트 결과를 공개함으로써, 도구에 대한 공적인 신뢰를 제공하는 방식을 도입하는 것도 고려해보는 것도 바람직하다고 할 것이다.

디지털 포렌식에 대한 법적인 신뢰를 부여할 수 있는 또 다른 판단기준은 그 업무에 적합한 전문적인 지식과 기술을 가진 사람에 의해서 행해졌는가이다. 현재 우리의 디지털 포렌식 분야에서 포렌식 전문가의 전문성을 검증할 수 있는 국가 차원의 기구는 마련되어 있지 않으며, 다만 학회가 중심이 된 국가공인 민간자격제도로서 디지털 포렌식전문가 자격시험이 유일한 전문가 인증방법이 되고 있다.국가공인이기는 하지만 전문가 자격을 부여하기 위해 요구하고 있는 자격이나 시험내용 등이 관련분야의 광범위한 승인이나 공인된 기준 없이 주관 기관 자체적으로 개발한 내용으로 구성되어 있기 때문에 그 자격증을 신뢰하지 못하는 경우도 있음을 볼 수 있다. 따라서 국가에서 포렌식 전문가 인증위원회(가칭)를 두고 디지털 포렌식을 포함한 각 포렌식 분야별 전문가로서 갖추어야 할 기술적, 법률적, 윤리적 기준을 표준화된 항목으로 구체적으로 정립하고, 각 분야별 민간자격증을 부여하는 기구들로 하여금 최소한 포렌식 전문가 인증위원회에서 제시한 표준항목들에 대한 검증시스템을 갖추도록 하는 것이 자격증에 대한 공신력을 제공함과 아울러 자격증을 소지한 사람에 대한 법과학 전문가로서의 공적인 신뢰를 확보하는데도 도움이 될 것으로 생각한다.

나. 정책적 관점에서의 제언

각 정부기관마다 디지털 포렌식 업무를 수행함에 있어서 디지털 증거를 수집 및 처리하는 방식에 차이가 있게 되면 디지털 증거에 대한 chain of custody에 문제가 발생할 수 있다. 즉 디지털 증거를 수집한 기관이 chain of custody를 잘 유지했더라도 그 증거를 이송받은 기관이 증거보존절차를 제대로 갖추지 못했거나 분석 프로세스에 있어서 권한통제가 제대로 유지되지 못한다면 디지털 증거에 대한 chain of custody에 대한 신뢰에 문제가 생길 수밖에 없다.따라서 조사 및 수사권한이 있는 기관에서 포렌식 업무를 수행함에 있어서는 디지털 증거를 수집·처리하는 방식의 표준화가 필요하며, 최소한 기관간에 공유해야 하는 디지털 증거에 대해서는 chain of custody가 단절되지 않을 수 있는 표준방식을 확립해야 할 것으로 생각된다.

다음으로 디지털 포렌식 분석관이 산출한 결과물이 최종적으로 법정에 제출되기 전에 그 내용이 기술적·법률적·절차적으로 정확한가에 대한 검토가 행해질 필요가 있다. 디지털 포렌식 보고서에 대한 최종적인 검토에 있어서 가장 중요한 것은 기술적 정확성에 대한 검증이라 할 수 있다. 만약 법정에 제출된 이후 반대 당사자에 의해 기술적으로 산출된 결과가 재현될 수 없거나 결과가 잘못 산출된 것이라는 이의가 제기되는 경우에는 동 사안에 있어서 디지털 증거가 절대적인 중요성을 갖는 것이라 할지라도 법적 신뢰성이 배제될 수 있기 때문이다. 따라서 디지털 포렌식 분석관이 최종적으로 산출한 결과에 대해서는 다른 동료 분석관에 의한 재검증 작업이 이루어지는 것이 바람직하다.

과학적 증거의 허용성에 대한 판단기준으로 가장 일반적으로 언급되는 것이 Daubert test이지만 디지털 포렌식과 관련하여서는 논의된 경우가 많지 않았다. 하지만 형사소송법 제313조 제2항의 개정으로 '과학적 분석결과에 기초한 디지털 포렌식 자료, 감정 등 객관적 방법으로 성립의 진정함이 증명되는 때에는 증거로 할 수 있다'는 규정이 들어옴으로서, 디지털 포렌식 자료에 대한 법적 판단이 필요한 경우가 생길 수 있게 되었다고 할 수 있다. 즉 디지털 포렌식 자료가 정확하고 신뢰성있게 산출되었다는 것이 입증되어야 그로부터 디지털 증거의 성립의 진정성을 증명할 수 있기 때문이다. 따라서 과학적 분석결과에 기초한 디지털 포렌식 자료가 정확하고 신뢰성 있게 산출되었다는 것이 포렌식 분석관의 증언에 의해 입증되어야 하는데, 이러한 과학적 증거에 대한 전문가 증언의 허용가능성에 대한 법적 판단기준이 무엇이어야 하는가에 대한 논의가 필요하다고 할 것이다. 일반적인 과학적 증거에 대한 전문가 증언의 법적 판단기준으로서 적용되어온 Daubert test 기준이 디지털 포렌식 도구로부터 산출된 결과에도 적용된다고 하는 것이 Daubert test를 확립하고 적용해 온 미 연방대법원의 입장이다.[3] 따라서 디지털 증거를 추출·분석·복구하기 위해 사용된 기초가 된 방법론이나 기술들이 건전하고 유효한 것인가, 그 결과로서 산출된 증거가 신뢰할 수 있는가에 대하여 Daubert test 기준에 따른 법적 판단이 행해져야 하는 것이다. 그런데 Daubert test가 제시하고 있는 기준은 디지털 포렌식의 본질적

3) David Watson/Andre Jones, op.cit., p. 4.

성격에 부적합한 측면이 있다. 따라서 과학적 증거에 범용적으로 적용되는 일반적 판단기준을 디지털 포렌식 영역에서 어떻게 해석하고 적용할 것인가를 고민할 필요가 있다고 생각한다.

제1장

KOREAN INSTITUTE OF CRIMINOLOGY

디지털 포렌식에 있어서 새로운 접근방식의 필요성

탁 희 성

제1장

디지털 포렌식에 있어서 새로운 접근방식의 필요성

제1절 서론

1. 연구의 필요성 및 목적

현대사회에 있어서 IT 기술의 발전속도는 하루가 다르게 가속화되어가고 있으며, 이를 기반으로 한 다양한 디지털 매체의 등장과 사물인터넷, 스마트폰 및 소셜네트워크 확산, UHD 기술, 클라우드 서비스, 정보저장매체의 대용량화 등으로 인해 디지털 데이터의 생성이 급증하고 있다. 특히 디지털 데이터의 활용이 고부가가치를 갖는 산업재로 인식되면서, 우리사회 거의 모든 영역에서 생산되는 정보가 디지털 방식으로 생성됨에 따라 디지털 데이터의 양이 급속하게 증가하고 있는 것이 현실이다. 한 조사연구[1]에 따르면 2014년 1,360억 기가바이트(GB)에서 2020년에는 8,470억 기가바이트(GB) 까지 증가할 것으로 예측되며, 전세계적으로는 44조 기가바이트(GB)에 이를 것으로 예측되고 있다.

이와 같이 디지털 데이터가 생활 전반에 걸쳐 생성되고 있기 때문에 범죄와 관련해서도 디지털 데이터는 밀접한 연관성을 가질 수 밖에 없다. 과거 사이버범죄에 국한되었던 디지털 증거가 이제는 기존의 전통적인 일반범죄에 있어서도 중요한 입증자료로서의 필연성이 인정되고 있기 때문에 형사사법시스템내에서 디지털 증거가 차지하는 비중은 점차 확대될 수 밖에 없다.

하지만 범죄수사와 관련하여 수집가능한 디지털 데이터의 다양성과 용량의 방대함

1) 한국 EMC, "디지털 유니버스 보고서: 대한민국 디지털 데이터 조사", http://korea.emc.com/about/news/press/2014/20140612.htm; 2016.5.20.

으로 인해 수사실무상 법적으로 유효한 디지털 데이터를 확보하는데는 여러 가지 법적·기술적 한계에 부딪치는 측면이 있다. 이러한 디지털 증거와 관련한 수사실무상의 어려움을 뒷받침하는 것이 디지털 포렌식으로, 디지털 데이터의 효율적인 선별·분석·저장·관리 및 보호를 신속하고 정확하게 지원할 수 있는 기술에 기반한 방법과 절차로서 의미를 갖고 있다. 즉 정보처리시스템과 다양한 디지털 매체에 저장된 방대한 데이터를 효율적이며 반복가능한 방법으로 수색(검색)을 가능하게 하는 디지털 포렌식은 디지털 데이터 관련 수사에 있어서 필수적으로 요구되고 있다.

디지털 포렌식은 디지털 기기를 매개로 하여 발생한 특정행위의 사실관계를 법정에서 규명하고 증명[2]하기 위한 기술에 기반한 방법과 절차라고 할 수 있다. 특히 디지털 데이터가 법적으로 유효한 증거자료로서 제시되기 위해서는 디지털 데이터의 물리적·논리적 취약성을 뒷받침할 수 있는 기술적인 방법을 통해 진정성·무결성·신뢰성·원본성 등이 확보되어야 하는데, 디지털 포렌식은 이와 같이 디지털 데이터의 입증가치를 수집단계에서부터 폐기단계에 이르기까지 신뢰성있게 유지할 수 있도록 하는 기술적·절차적·법적 요소로 구성된 포괄적인 프로세스라고 할 수 있다. 따라서 디지털 포렌식 분야는 IT 기술의 개발과 더불어 지속적으로 변화되어야만 하고, 항상 새로운 지식과 기술에 개방되어 있어야만 한다. 특히 디지털 포렌식을 활용한 수사에 있어서는 다양한 IT 지식과 기술이 뒷받침되어야만 하고, 이를 위해서는 다양한 IT 전문가 그룹의 네트워크 구축을 통해 각 분야에서 요구되는 지식과 기술들이 언제든지 신속하게 공유될 수 있어야 한다.

디지털 포렌식은 이와 같은 기술적 지식의 뒷받침과 아울러 포렌식 기술을 적용하고 활용하는 과정에서 발생할 수 있는 법률적 문제 - 프라이버시 침해, 위법수집증거, 보관의 연속성의 단절에 따른 무결성 훼손, 전문증거 배제 등 -를 최소화하고, 디지털 데이터가 법정에서 증거능력을 부여받을 수 있는 법률상 요건들을 준수해야 하기 때문에 디지털 증거에 대한 규범적 지식과 이해가 수반되어야 한다. 즉, 디지털 포렌식은 컴퓨터 공학에 대한 기술, 사법체계에서 준수해야 하는 법률 그리고 사실관계를 확인하는 수사(조사)에 대한 전문적 지식이 결합된 분야이며, 특히 디지털 포렌식에 특화된 기술적 지식은 법률적으로 허용될 수 있는 범위 내에서 필요한 기술적 지식[3]이

---

2) http://forensic-proof.com/archives/3357; 2006.4.2.

라 할 수 있다.

이와 관련하여 미국, 영국, EU 등에서는 디지털 포렌식 프로세스의 중요성에 대한 인식하에 디지털 포렌식 가이드라인 또는 Good Practice, Best Practice Manual 등을 제시하고 있다. 이러한 지침이나 매뉴얼 등은 디지털 포렌식 조사를 위한 프레임 워크를 제공함으로써 수집한 자료의 증거능력을 확보할 수 있는 식별·획득·수집·분석 등 디지털 포렌식 프로세스 전 과정에 걸쳐 준수해야할 사항을 제시하고 있을 뿐만 아니라, 이러한 프로세스를 통해 각 기관들이 신뢰할 수 있는 결과들을 산출하고, 표준화된 업무관행을 통해 업무품질 및 수준을 어느 정도 통제 가능하도록 하고 있다.

현재 우리의 경우 각 정부기관의 필요에 따라 디지털 포렌식 시스템이 독자적으로 운용되고 있으며, 각 기관별 운용지침이 있는 정도이며, 각 기관들이 모범으로 삼아 준수할 수 있는 디지털 포렌식 지침은 아직 마련되어 있지 않다. 디지털 증거가 수사를 위한 lifecycle의 시작부터 관련 기준들을 충족하는 good practice에 기반한 표준적인 운용절차를 활용하여 적절히 취급되어질 수 있다면, 형사사법시스템 전체를 통한 일관성을 확보할 수 있고, 따라서 증거오염으로 인한 입증가치의 훼손을 피할 수 있다고 할 것이다. 그런데 현재 우리의 디지털 포렌식 시스템은 그와 같은 표준적인 운용절차나 good practice를 마련하지 못한 채 운용되고 있기 때문에 언제든지 그 신뢰성 검증에서 이의가 제기될 우려가 있고, 따라서 어렵게 수집하고 분석한 자료들을 증거로 활용하지 못하는 문제가 발생할 수 있다. 더욱이 각 기관별로 디지털 포렌식 시스템을 운용하면서 기관간 협업이 제대로 이루어지지 못함으로 인해 급속히 변화하는 지식과 기술을 빠르게 습득하고 활용하는데 한계가 있을 수 밖에 없다고 할 것이다.

물론 디지털 포렌식의 특성상 특정분야의 전문화된 기술을 기반으로 한다는 점에서 보면 각 기관의 고유한 업무상 필요에 부합하는 디지털 포렌식 시스템을 운용하는 것이 불가피한 측면이 있는 것도 사실이다. 하지만 그로 인해 디지털 포렌식에 필수적으로 요구되는 기술 및 도구의 개발과 인증, 절차의 표준화, 체계적인 전문가 교육 및 훈련, 법률적인 프로세스와의 연계 등이 제대로 갖추어지지 못한 상태에서 대증요법적으로 디지털 포렌식이 운용됨에 따라, 대내적으로는 수사의 효율성이 저하되거나 궁극적으로 법정 증거로서의 신뢰를 확보하지 못하는 문제가 발생할 수 있고, 대외적

3) 래리 다니엘/라즈 다니엘(백제현 역), 포렌식 전문가와 법률가를 위한 디지털 포렌식, 2012, 77면.

으로는 국제적인 수준의 기술적·법적 표준과 인증에 기반한 디지털 포렌식 서비스를 제공하지 못하는 문제가 있을 수 있다.

이에 본 연구는 우리나라 형사사법기관별로 운용하고 있는 디지털 포렌식 시스템을 검토하여 실무에서 발생하고 있는 문제점이 무엇이고, 실무에서 요구되는 디지털 포렌식 시스템의 구체적인 내용이 무엇인지를 파악하여 IT 기술수명의 짧은 주기와 포렌식 수사의 신속성과 기밀성에 부합할 수 있는 전체적인 프로세스를 모색해 보고자 한다. 이와 관련하여 디지털 포렌식 분야에 있어서 앞서가고 있는 미국·영국 등 주요 국가의 디지털 포렌식 시스템을 비교분석하여 봄으로써, 향후 다양한 디지털 기술과 관련 범죄수사에 대한 대응역량을 강화할 수 있는 통합적인 디지털 포렌식 프로세스 모델을 제시해보고자 하는데 연구목적을 두고 있다.

그리고 디지털 포렌식의 대상 내지 객체를 개발하는 것은 현실적으로 대부분 민간기업이기 때문에 이들과의 협력적인 관계가 구축되지 않으면 신속하고도 효율적인 포렌식 업무를 수행하는 것이 대단히 어려울 수 있는 바, 국가 업무와 민간 업무의 상호협력이 가능한 디지털 포렌식 플랫폼으로서 국가 디지털 포렌식 모델이 제시되는 경우, 우리의 수준높은 IT 지식과 기술이 뒷받침되는 포렌식 기술, 절차, 도구, 랩 등의 분야에서 세계적인 표준을 제시하는 것도 가능하다고 할 수 있다. 이를 위해서는 디지털 포렌식 도구와 절차, 랩에 대한 세계적인 수준의 인증시스템을 갖추어야 하는 바, 본 연구에서 제시하는 통합 디지털 포렌식 모델내에 이와 같은 인증시스템을 구축할 수 있는 방안도 함께 모색해 보고자 한다.

2. 연구방법

본 연구는 급속히 확산되고 있는 디지털 환경하에서 범죄수사에 필수적인 기능을 담당하는 디지털 포렌식이 디지털 데이터의 입증가치와 분석결과의 신뢰성을 담보할 수 있는 프로세스를 제시해보고자 한다.

디지털 포렌식의 초기에는 프로세스에 초점을 맞추기 보다는 결과로서 제공되는 증거의 내용에 초점을 맞추었다고 하면, 이제는 디지털 증거의 입증가치 자체가 정확하고 신뢰할 수 있는 프로세스를 통해 생성되지 않으면 그 결과에 대한 신뢰를 담보하

기 어려운 경우가 발생하기 때문에 프로세스의 필요성과 중요성에 대한 인식이 높아져가고 있다. 따라서 디지털 포렌식에 있어서 프로세스의 의미와 그 필요성에 대한 인식을 제고하고, 고도의 일관성과 검증가능성을 수반하는 과학적 입증방법에 기반한 프로세스의 구성요소들을 검토해보고자 한다. 이를 위하여 먼저 현행 디지털 포렌식 시스템의 운영현황을 분석하여 법과학적 수사방법으로서 디지털 포렌식의 신뢰성을 향상시키는데 장애가 되는 요인들을 검토하여 그 개선방안을 모색해 보고자 한다.

그리고 이와 함께 주요 국가들의 디지털 포렌식 시스템을 비교하여 우리의 디지털 포렌식에의 시사점을 도출해 보고자, 주요 국가(미국, 영국, 독일, 네델란드, EU)의 디지털 포렌식 센터의 구성 및 운용 프레임, 디지털 포렌식 프로세스 업무 매뉴얼, 프로세스를 구성하는 기술적·인적·규범적 요소 및 각 구성요소에 대한 인증기준 등을 검토해 보고자 한다.

이러한 비교검토를 토대로 우리의 형사사법시스템내에서 디지털 포렌식의 신뢰를 규범적으로 담보할 수 있는 디지털 포렌식 프로세스 모델을 제시해보고자 하는데, 이에 우선하여 기술적·법적·정책적으로 선결되어야 할 과제들이 무엇인가를 살펴보고, 디지털 포렌식 과정을 관리하고 최적화하는데 활용할 수 있는 절차적 프레임을 제안해보고자 한다. 이와 관련하여 각 절차를 구성하는 도구, 전문가, 실험실, 분석방법 등과 관련한 인증기준의 마련가능성과 인증방법, 표준적 지침을 위한 가이드라인을 모색해 보고자 한다. 또한 급속히 발전하고 있는 디지털 포렌식에 대한 기술적 지식과 정보를 체계적으로 수용하여 범죄에 효과적으로 대응할 수 있는 디지털 포렌식 통합모델의 프레임을 제시해 보고자 한다.

이와 같이 통합적인 디지털 포렌식에 있어서 기술적·절차적·법적으로 표준화된 프로세스를 준수하는 경우, 절차의 적절성 및 그로부터 산출된 결과에 대한 증거품질의 적합성에 대한 공적인 승인이 어느 정도 가능하기 때문에 법정에서 그에 대한 이의를 제기할 우려가 감소함으로써 디지털 증거의 법적 신뢰성의 수준을 제고할 수 있을 것으로 생각된다.

이를 위한 연구방법으로는 먼저 디지털 포렌식의 기본 프레임에 대한 논의와 아울러 기존의 디지털 포렌식 프로세스 모델의 유형을 검토해 보고자 한다. 그리고 현재 국가기관에 설치되어 운용중인 디지털 포렌식 기구의 현황 및 운용방식 등을 검토함

과 아울러 디지털 포렌식 업무에 종사하는 전문가들이 디지털 증거를 취급함에 있어서 필요성이 요구되는 디지털 포렌식 프로세스와 그 한계가 무엇인가를 전문가 인터뷰를 통해 살펴보고자 한다.

또한 주요 국가 - 미국, 영국, 독일, 네델란드, EU - 의 디지털 포렌식 시스템과 프로세스의 수준을 비교검토하여, 우리의 디지털 포렌식 프로세스 마련에 도움이 될 수 있는 방향성이 무엇인가를 제시해 보고자 한다.

마지막으로 통합적인 디지털 포렌식 프로세스의 주요 기능과 인증 기준·표준화 지침·기술적 프로세스와 법률적 프로세스의 연계방안 등을 검토하여, 디지털 증거의 법적 신뢰도를 제고할 수 있는 디지털 포렌식 프로세스 모델 프레임을 제시해 보고자 한다.

제2절 디지털 포렌식 프로세스의 기본 구조 및 개요

1. 디지털 포렌식의 기본 개념

디지털 포렌식은 고도로 전문화되고 빠르게 성장하는 포렌식 과학의 한 분야로서, 원래 컴퓨터 포렌식이란 용어가 사용되었지만 2001년 8월 미국 대학의 연구진들과 컴퓨터 포렌식 전문가들이 '디지털 포렌식 연구 워크숍'을 개최하면서 정식으로 디지털 포렌식이라는 용어가 사용되기 시작[4]하였다. 이후 2003년 SWGDE(Scientific Working Group Digital Evidence)과 ASCLD(American Society of Crime Laboratory Directors)의 협력하에 디지털 포렌식이 정식 법과학 분야로 인식되면서 랩인증프로그램의 한 분야로 채택되었다.[5]

일반적으로 디지털 포렌식은 '디지털 소스로부터 디지털 증거를 보존·수집·증명·식별·분석·해석·기록·제출하기 위하여 과학적으로 이끌어내고 증명하는 방법'으로 정의된다.[6] 하지만 법률적인 사안에서 디지털 증거를 확보하고자 하는 과학적인 수사

---

4) http://www.dfrws.org/about.html
5) John Barbara, "Digital Evidence Accreditation: ASCLD/LAB sets a standard of Acceptability", Law Enforcement Technology Vol.31, Issue.2, 2004.
6) Gary Palmer, "A road Map for Digital Forensics Research", DFRWS, Nov.2001;

기법으로서 디지털 포렌식을 의미하는 경우에 있어서 디지털 포렌식은 디지털 매체에서 확보한 증거로 부터 특정한 범죄행위의 사실관계를 법적으로 규명하고 증명하기 위한 절차와 방법이라고 정의할 수 있다.[7)]

디지털 포렌식은 기본적으로 4가지의 기본개념 즉, 증거의 수집·보존·분석·제출로 구성되어 있는데, 이는 디지털 증거를 확보하기 위한 전체적인 디지털 포렌식 프로세스를 구성하는 메인 프레임이라고 할 것이다.

먼저 증거의 수집은 압수 등의 방법으로 디지털 데이터를 확보하여 디지털 포렌식 기관으로 이전하는 것을 말한다. 이 경우 디지털 데이터는 적법한 방식으로 수색되고 압수되어져야 하며, 이 과정에서 적용된 프로세스는 관련된 증거법칙을 준수해야만 한다. 이 단계가 적절히 실행되지 못하면 그 증거는 허용될 수 없고, 사용된 수집방법이 법적으로 승인된 것이 아니면 증거에서 배제될 수 있다. 즉 증거의 수집은 디지털 포렌식의 첫 번째 단계로서, 원본 데이터에 대한 최초의 접촉이 발생하기 때문에 데이터의 무결성이 손상되거나 훼손될 가능성이 크다는 점에서 수집을 개시하기 전에 철저한 사전적 준비와 주의가 요구되는 경우라 할 수 있다. 또한 현장에서 수집된 디지털 데이터가 포렌식 센터에 도착할 때까지 포장과 이송을 위한 사전적 예방조치 - 정전기나 자기장에의 노출 방지, 압수된 디지털 매체의 작동 방지 등 -가 취해져야 한다.

두 번째 증거의 보존은 디지털 포렌식 분야에서 가장 많이 언급되고 그 준수여부가 증거능력의 가부를 판가름할 정도로 중요한 것으로, 흔히 Chain of Custody 라고 불리는데 통상 보관의 연속성 또는 보관의 연계성으로 번역되고 있다. 즉 Chain of Custody의 증명은 입증자료로 사용하고자 하는 디지털 데이터가 수집 단계에서부터 어떠한 변경·치환 또는 조건의 변화가 부재했다는 것을 보여주는 것으로, 해당 데이터에 대한 증거기반을 마련하는데 있어서 필수적으로 요구되는 것이다. Chain of Custody의 적절성 여부에 대해서는 3가지 유형의 입증을 필요로 하는데, ⅰ) 증거가 그것이 의도하고자 한 것이라는 입증, ⅱ) 압수된 시점부터 법정에 제출되는 시점까지 그 증거를 보유했던 각각의 개인들에 의한 지속적인 보유에 대한 입증, ⅲ) 그것을

---

http://www.dfrws.org

7) 디지털 포렌식은 형사분야 뿐만 아니라 민사, 저작권, 특허 등 여러 분야의 분쟁해결의 수단으로 활용되고 있으며, 점점 더 많은 분야에서 그 기능을 활용하고자 하고 있다.

보유했던 각 사람들에 의해 증거자료가 한 사람으로부터 다른 사람의 보관으로 넘어가는 순간까지 실질적으로 동일한 조건하에 있었다는 입증 등이 그것이다. 디지털 포렌식 프로세스에 있어서 각 단계별로 문제를 야기할 수 있는 수많은 쟁점들이 존재하지만, 모든 단계에 걸쳐서 핵심적인 문제는 Chain of Custody를 개발하고 유지하는 것이라 할 수 있다. 따라서 디지털 포렌식 프로세스에 있어서는 정확하게 행해진 모든 것, 사용된 모든 도구와 프로세스, 적용된 분석방법, 저장 및 이송시 요건, 증거에 접촉한 사람 등 모든 사항을 문서화하는 것이 절대적으로 중요하다.

세 번째 증거분석은 법률적 사안에 따라 확보된 디지털 데이터 중에서 입증자료로 제출할 수 있는 항목들을 찾아내고 수집하는 과정이다. 즉, 디지털 증거가 수집되고 보존되면, 사건을 재구성하고 관련정보를 추출하기 위해 분석되어야 하는 것이다. 이 경우 각 사건마다 입증내용이 다르기 때문에 디지털 증거를 분석함에 있어서도 분석하는 사람의 역량 내지 숙련된 지식, 분석도구의 유형, 디지털 포렌식에 특화된 기법 등이 영향을 미치게 된다. 또한 입증내용이 지니는 법률적 의미에 대한 이해가 뒷받침되어야 정확한 분석과 추출이 가능하다는 점에서 볼 때, 분석자가 어느 정도의 법적 지식을 지니고 있는가도 영향을 미칠 수 있다.

네 번째 증거제출은 일반적인 디지털 포렌식 프로세스의 마지막 단계로서, 포렌식 분석결과를 분석보고서로 작성하여 분석을 의뢰한 사법기관에 제출하는 것이다. 디지털 포렌식 분석결과를 보고서로 작성하는 경우 공식적으로 참조할 수 있는 표준이나 지침이 현재로서는 없기 때문에, 각 기관별로 자체적으로 마련한 보고서 작성기준에 따르고 있다. 다만 보고서의 내용으로서 포렌식 분석관의 경력 및 인증 자격, 분석과정에서 사용한 도구 및 분석을 수행한 절차, 분석된 결과에 대한 명확한 설명, 원본 무결성 보존을 위해 취해진 조치, 분석된 증거를 확인하는 방법 등은 필수적으로 기재되어야 한다.[8] 디지털 포렌식 프로세스에 따라서는 분석결과를 의뢰한 기관에 제출하는 것으로 프로세스가 완료되는 것이 아니라, 분석에 참여한 전문가가 법정증언을 하거나 감정서를 작성하는 등의 법정절차에 참여하는 것 까지 포함되는 경우도 있다. 하지만 포렌식 분석관이나 조사관들은 이러한 법정절차에 숙련되어 있지 않기 때문에 문제가 발생할 수 있으며, 따라서 포렌식 분석관이나 조사관들의 법정 증언을

8) 래리 다니엘/라즈 다니엘(백제현 역), 포렌식 전문가와 법률가를 위한 디지털 포렌식, 2012, 16면.

지원할 수 있는 별도의 프로그램이나 교육이 뒷받침될 필요가 있다.

2. 디지털 포렌식의 구성요소

가. 기술적 요소

1) 디지털 포렌식 도구

현재 디지털 포렌식 분야에서는 다양한 포렌식 도구들이 사용되고 있는데, 이는 디지털 데이터의 존재양식이 다양해짐에 따라 각 영역별로 세분화된 전문도구들이 개발되고 있기 때문이다. 일반적으로 디지털 포렌식 도구는 자료조사 도구, 증거수집 도구, 네트워크 및 인터넷 분석도구, 데이터 분석도구 등으로 유형화할 수 있고, 소프트웨어 방식과 하드웨어 방식으로 구분해 볼 수 있다.

하지만 어떤 형태의 도구이든 간에 법과학적 타당성이 고려된 최소한의 기준을 충족해야 하며, 법과학적 관점에서의 요구사항들이 충족되었는지의 여부가 확인되어야 한다. 디지털 포렌식 도구가 법과학적 타당성이 고려된 최소한의 기준을 충족했는지의 여부는 정의가능성, 예측가능성, 반복성, 검증가능성으로 판단할 수 있다.[9] 그리고 도구의 신뢰성은 테스트를 거쳐 검증과 확인[10]이 이루어져야 한다.

미국의 경우 디지털 포렌식 도구에 대한 테스트와 검증을 수행하는 국립표준기술연구소(NIST: National Institute of Standards and Technology)가 있는데, 여기에서 포렌식 도구 검증 프로그램(Computer Forensics Tool Testing Program:CFTT)을 두고 디지털 포렌식 도구에 대한 검증방법을 개발하고 있다. CFTT 프로젝트는 컴퓨터 포렌식 도구의 신뢰성을 확보하고자 하는 법집행공동체의 절실한 필요성에서 비롯된 것으로, 일반적인 도구 사양(조건)의 개발, 테스트 절차, 테스트 기준, 테스트 세트, 테스트 하드웨어에 의해 컴퓨터 포렌식 소프트웨어 도구를 테스트하기 위한 방법론을

9) 래리 다니엘/라즈 다니엘(백제현 역), 포렌식 전문가와 법률가를 위한 디지털 포렌식, 2012, 44-45면.

10) 검증(validation)은 시스템이나 컴포넌트 개발 도중 혹은 마지막에 요구사항을 충족하는지 판단하기 위해 평가하는 절차이며, 확인(verification)은 주어진 개발단계에서 제품이 각 단계의 시작점에 주어진 조건을 만족하는지를 결정하기 위해 시스템이나 컴포넌트를 평가하는 과정이다 ; T.Wilson/J.Slay, "Digital Forensics"; exploring validation, verification & certification", Systematic Approaches to Digital Forensic Engineering, 2005, First International Workshop on digital forensics, 2005, pp.48-55.

제시하고자 하는데 목적을 두고 있다.[11] 그리고 그 결과는 도구제작자가 도구를 개선하고, 사용자가 컴퓨터 포렌식 도구의 확보와 이용에 관하여 충분한 정보에 입각한 선택을 하며, 이해관계 있는 당사자들이 도구의 성능을 이해하는데 필요한 정보를 제공[12]하는데 기여한다. 그리고 이 프로그램에서 수행하는 컴퓨터 포렌식 도구에 대한 검증은 적합성 테스트와 품질 테스트에 관한 국제적 인증방법에 근거하고 있다고 밝히고 있다.[13]

NIST에 의해 개발된 CFTT 테스팅 방법론은 기능성 중심인데, 이는 포렌식 조사활동들이 별개의 기능들로 분리되어 있어서 테스트 방법론도 그러한 유형별로 개발되기 때문이다.[14] CFTT 테스팅 절차는 법집행공동체의 대표로 구성된 운영위원회에 의해 관리·감독되며, 이 위원회에서 도구의 유형과 실제 테스팅을 할 도구를 선정하게 된다. 이와 같이 테스트를 할 도구의 유형과 그 유형가운데 최소한 하나의 도구를 선정한 후 개발 프로세스는 1) NIST와 법집행직원은 요구사항, 주장(assertion), 테스트 케이스 문서를 개발하며, 2) 도구유형의 사양은 컴퓨터 포렌식 공동체의 구성원에 의한 동료심사를 위해 그리고 다른 이해관계 당사자들에 의한 공개적인 논평을 위해 웹사이트에 게시하며, 3) 적절한 코멘트와 피드백을 사양 안에 구체화시키며, 4) 테스트 환경을 도구유형에 맞게 디자인[15]하는 순서로 진행한다고 밝히고 있다. 이와 같이 도구의 유형에 관한 사양을 개발하고 도구를 선정한 후 테스트 프로세스는 1) 테스트할 도구를 확보하고, 2) 도구 설명서를 검토하며, 3) 그 도구에 의해 지원되는 특징들에 따라 관련 테스트 케이스를 선정하고, 4) 테스트 전략을 개발하며, 5) 테스트를 실행하고, 6) 테스트 보고서를 작성하고, 7) 운영위원회가 테스트 보고서를 검토한 후, 8) 제작자가 테스트 보고서를 검토하고, 9) 지원소프트웨어를 웹에 게시하고, 마지막으로 10) DHS(cyberfetch.org)가 테스트 보고서를 웹에 게시한다.[16]

이와 함께 NIST는 2014년 디지털 포렌식 실무자들을 위한 지침과 국가적 표준을 개발하기 위하여 디지털 증거 소위원회를 설립함으로써, 디지털 증거처리를 위한 표

11) http://www.cftt.nist.gov/ ; 2016.6.5.
12) http://www.cftt.nist.gov/ ; 2016.6.5.
13) http://www.cftt.nist.gov/ ; 2016.6.5.
14) http://www.cftt.nist.gov/Methodology_Overview.htm : 2016.6.5.
15) http://www.cftt.nist.gov/Methodology_Overview.htm : 2016.6.5.
16) http://www.cftt.nist.gov/Methodology_Overview.htm : 2016.6.5.

준을 개발하고 연구하는 업무를 지속적으로 진행하고 있다.

EU의 ENFSI(European Network of Forensic Science Institutes)도 "GUIDELINES FOR BEST PRACTICE IN THE FORENSIC EXAMINATION OF DIGITAL TECHNOLOGY"[17]에서 디지털 포렌식 도구에 관한 요건들을 제시하고 있다. 이 가이드라인에 의하면 디지털 포렌식 분야에서 활용되는 소프트웨어 도구들은 기본적으로 유효한 라이센스를 가지고 있어야 한다고 전제하면서, 포렌식 도구를 보존도구·복구도구·조사도구로 구분하여 그 각각에 요구되는 조건들을 기술하고 있다. 그리고 이러한 도구들은 그 목적에 적합해야 하고, 감사기능이 내재되어 있어야 하고 프로세스 로그파일을 생성할 수 있어야 할 뿐만 아니라, 그 도구의 사용이 수사에 중요한 데이터에 어떠한 영향도 미치지 않는다는 점이 사전에 확인되어야 한다고 기술하고 있다.[18] 그리고 이와 같이 다양한 유형의 디지털 포렌식 소프트웨어 도구는 그 이용이 정의되어야 하고, 적절성과 신뢰성을 확인하기 위한 테스트 규칙이 확립되어야 할 뿐만 아니라 이러한 모든 테스팅 프로그램들이 완벽하게 기록되어야 한다고 되어 있다.[19]

2) 디지털 포렌식 전문가

디지털 포렌식 전문가는 기본적으로 컴퓨터와 소프트웨어 등에 대한 전문적 지식을 갖고 있어야 하며, 이와 아울러 데이터 추출 및 복구에 특화된 도구에 대한 지식과 법과학적으로 데이터를 분석하는 기법에 특화된 전문지식을 지녀야 한다. 즉, 디지털 포렌식 전문가는 단순히 컴퓨터 공학적 지식을 습득하는 것을 넘어서서 증거의 관점에서 복구된 데이터를 분석하여 데이터에 대한 사실관계를 확인할 수 있어야 하는 것이다.

따라서 디지털 포렌식 전문가에 대한 교육과 훈련에 있어서 중요한 것은 증거의 관점 특히 법적인 측면에서 데이터를 다루고, 주장된 행위를 조사하며, 법률이 허용하는 범위내에서 분석작업을 하여 법률적 쟁점에 관한 분석 결과물을 제시할 수 있어야 한다는 것이다.[20]

---

17) https://cryptome.org/2014/03/forensic-digital-best-practice.pdf; 2016.4.5.
18) https://cryptome.org/2014/03/forensic-digital-best-practice.pdf; 2016.4.5. pp.13-14.
19) https://cryptome.org/2014/03/forensic-digital-best-practice.pdf; 2016.4.5. p.14.
20) 래리 다니엘/라즈 다니엘(백제현 역), 포렌식 전문가와 법률가를 위한 디지털 포렌식, 2012, 80면.

실무적인 관점에서 디지털 포렌식 전문가의 자격은 디지털 포렌식에 관한 전문적인 기술 교육을 이수하고 디지털 증거분석에 대한 경력이 있어야 하는 것 뿐 아니라, 해당 분야에 대한 전문성도 증명할 수 있는 전문가여야 한다. 그리고 법정에서 전문가 증언을 해야 하는 경우, 디지털 포렌식 전문가는 자신의 분야에 관한 기술적 지식을 일반인이 이해할 수 있도록 논리적으로 표현해야 하며, 판사로 하여금 해당 분석결과의 신뢰성을 의심케 하거나 분석절차상 증거의 오염가능성을 의심케 할 여지가 생기지 않도록 법적인 쟁점에 대한 분명한 이해를 갖추어야 한다.

현재 디지털 포렌식 전문가의 전문성을 검증할 수 있는 합의된 국제적 기준이나 검증시스템은 구축되어 있지 않다. 다만 국가에 따라 디지털 포렌식 전문가의 전문성을 검증할 수 있는 기준 내지 매뉴얼을 갖고 있는 경우가 있다. 미국의 경우 디지털 포렌식 분야에 있어서 전문가 검증을 위한 실무 매뉴얼과 전문가 관리 및 전문가 증언을 관리하기 위한 지침을 갖고 있다. NIST의 "Crime Scene Investigation: A Guide for Law Enforcement", NIJ의 "Electronic Crime Scene Investigation: A Guide for First Responders" 등이 그것이다. EU의 ENFSI(European Network of Forensic Science Institutes)도 Best Practice Manual for the Forensic Examination of Digital Technology[21]를 두고 디지털 포렌식 부서내 기술인력의 책임과 의무에 관한 규정, 훈련과 평가에 관한 규정, 자격시험 관련 규정 등을 두고 있다. 그리고 영국의 ACPO(Association of Chief Police Officers)도 사법기관에 근무하는 포렌식 담당 직원에 관한 지침(ACPO Good Practice and Advice Guide for Managers of e-Crime Investigation)[22]을 두고 있는데, 여기에는 디지털 포렌식 조사업무에 적절한 기술적 능력을 보유해야 함에 있어서 갖추어야 할 최소한의 기준을 제시하고 있으며, 이와 아울러 관리문제 - 보안문제, 증거물관리, 불법자료 통제정책, 장비의 최소 요구사항, 기록 유지, 업무의 연속성, 증거의 제출, 보존과 폐기 등 -, 조사문제 - 위험평가, 프로세스 품질유지, 피고측에의 대응, 제한된 자료, 전문가들간 회의 등 -, 일반적인 문제 - 관련 법률의 개정내용과 그 영향 등 -, 포렌식 문제 - 동료심사, 도구에 대한

21) http://www.enfsi.eu/sites/default/files/documents/enfsi-bpm-fit-01_2.pdf; 2016.4.5.
22) http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf; 2016.4.5.

이중적 확인- 등을 기술하고 있다.[23] 그리고 훈련과 관련한 내용 등도 함께 기술되어 있다. 즉 포렌식 전문가들은 최소한 자신의 분야에 적용되는 모범실무지침을 알고 있어야 하고, 분석과정에서 이를 준수하였음을 보장할 수 있어야 한다는 것을 명확히 하고 있는 것이다.

3) 디지털 포렌식 실험실

법과학에 있어서 전문성은 일반적으로 실험실 인증, 분석관 및 조사관의 공인, 프로세스 가이드라인 등에 의해 유지된다. 디지털 포렌식에 있어서도 실험실은 신뢰할 수 있는 결과를 산출하고, 확보한 정보의 품질을 최대화하며, 강력한 증거를 생산할 수 있는 등 IT 조사분야에 있어서의 업무품질을 제고할 수 있는 중요한 중요한 요소로 평가된다.

국제적으로는 국제표준인 ISO/IEC 17025에 의해 디지털 포렌식 분석실에 대한 인증을 시행하고 있으나, 일반 법과학 실험 등에 대한 시험기관 인증을 중심으로 설계되어 있어서 디지털 포렌식에 적합한 것은 아니다. 미국의 경우 ISO/IEC 17025에 기초하여 ASCLD/LAB(American Society of Crime Laboratory Directors/Laboratory Accreditation Board)에서 포렌식 실험실에 대한 인증을 수행하고 있다. 즉 디지털 포렌식이 ASCLD/LAB 인증프로그램에 포함되면서 디지털 포렌식에 대한 통일된 표준 및 적격성 등에 관한 합의가 이루어지게 되었다. 랩인증 매뉴얼에 따르면 행정적 절차, 조직구성, 권한부여, 관리감독, 커뮤니케이션, 훈련과 개발, 통제, 개별 DB 표본 통제, 품질시스템, 숙련도 검사, 개인별 적격성 심사, 물리적 설비, 설계, 보안, 건강과 안전 등과 관련한 표준과 평가기준이 제시되어 있다. 하지만 미국법체계를 중심으로 설계되어 있고, 인증에 시간과 비용의 소요가 크다는 문제가 있다.

EU의 ENFSI는 회원국들의 디지털 포렌식 실험실 환경에 적용될 수 있도록 국내 규제요건과 국제적 기준에 따른 디지털 포렌식 표준운용절차를 구축하는데 도움이 될 수 있는 기술적인 지침들을 제공하고 있다. 이에 따르면 디지털 포렌식 실험실은 인적 자원, 장비, 시설과 환경조건, Reference materials, 기록보관, 방법론, 측정의 불확실성에 대한 검증 및 평가, 프로세스 검증, 기능(도구 또는 사람에 기반한) 검증,

---

23) http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_and_Advice_for_Manager_of_e-Crime-Investigation.pdf; 2016.4.5.

직원에 대한 능력 테스트 등과 관련한 관리시스템을 갖추도록 하고 있다.[24]

나. 절차적 요소

1) 보관의 연속성(chain of custody)

보관의 연속성은 법률적 맥락에서 디지털 증거를 법정에서 증거로서 허용하기 위해 요구되는 무결성 입증방법 가운데 하나이다. 보관의 연속성에 대한 입증은, 조건의 변경·대체·변화의 부재를 입증함으로써 당해 증거의 기초를 구축하는데 필수적인 것이라 할 수 있다. 이러한 보관의 연속성은 기존의 물리적 증거에 대해서도 요구되어 왔던 무결성 입증방법으로, 물리적 증거의 경우에는 증인에 의해 용이하게 오염 내지 변개 여부가 확인될 수 있기 때문에 반드시 보관의 연속성에 의한 입증이 뒷받침되어야만 증거로서 허용되는 것은 아니었다.

하지만 디지털 포렌식에 있어서 보관의 연속성에 대한 입증은 디지털 데이터를 법정 증거로서 사용하기 위한 절대적인 필수요구사항이라 할 수 있다. 즉 디지털 증거는 그것이 수집되는 단계부터 법정에 제출되는 단계에 이르기까지의 각 단계에서 물리적 이전방식이 아니라 전자적 방식을 통한 논리적 이전이 이루어지기 때문에, 그 과정에서 고의 내지 과실(포렌식 도구 또는 전문가의 오류로 인한) 또는 우연히(보관 환경이나 조건으로 인한) 발생한 증거의 오염·훼손·변개 여부가 드러나거나 확인되지 않는다. 즉 디지털 증거는 그것이 수집되는 순간부터 그것이 증거로서 법정에서 허용될 때까지 발생가능한 모든 위험으로부터 안전하게 유지·관리·보존·통제되어 왔다는 히스토리가 객관적으로 입증됨을 보여주는 보관의 연속성을 통해서만 증거로서의 무결성과 신뢰성을 담보할 수 있다고 할 것이다.

따라서 보관의 연속성에 대한 명확한 입증이 결여되면 그 증거가 부적절하게 처리되었거나 변경되었다는 이유로, 또는 다른 방식으로 오염되었다는 이유로 그 증거의 신뢰성과 입증가치에 이의가 제기될 수 있고, 따라서 보관의 연속성에 있어서 설명되지 못하는 단절은 결국 디지털 증거를 배제하는데 사용될 수 있는 것이다.[25] 즉 디지털

---

24) ENFSI, Best Practice manual for the Forensic Examination of Digital Technology, ENFSI-BPM-FIT-01, ver.01, Nov. 2015.

25) Eoghan Casey, Digitak Evidence and Computer Crime-Forensic Science, Computers and the Internet, 2004, p. 175.; 탁희성/이상진, 디지털 증거분석도구에 의한 증거수집절

포렌식 프로세스는 궁극적으로 chain of custody를 구현하기 위한 것이라고도 할 수 있다.

디지털 증거에 대한 보관의 연속성에 있어서 기본적으로 준수되어야 하는 3가지 단계는 다음과 같다.

"ⅰ) 데이터 수집단계에서의 무결성 확보이다. 이 단계에서는 디지털 증거의 유형에 따라 매뉴얼화 된 절차가 필요하며, 현장에서 수집된 데이터와 분석을 위해 수사기관으로 이전된 데이터간의 동일성을 확인하는 것이 데이터의 무결성 보장에 있어서 필수적이다. 주로 이 단계에서는 해시값을 통한 무결성 입증이 행해지고 있다.

ⅱ) 데이터 분석단계에서의 무결성 확보이다. 즉 데이터를 분석한 도구와 변수가 무엇이고, 장소는 어디이며, 그 날짜와 시간은 언제이며, 누가 어떠한 방법론을 사용했으며, 누가 해당 데이터에 대한 서명을 하였는가 등에 관한 정보를 영구적이고 삭제할 수 없는 표지의 형태로 기록함으로써 데이터의 무결성을 확인해야 한다.

ⅲ) 데이터 처리 및 기록유지 단계에서의 무결성 확보이다. 엄격한 증거보존을 위해서는 정확하게 분석에 적합한 도구와 방법을 사용해야 하고, 분석과정에서 확인된 증거의 오염·손상·변경의 흔적을 그대로 보존해야 한다. 또한 권한이 있는 자 외에는 데이터에 대한 접근이 금지되어야 하며, 데이터에 접근한 사실은 모두 기록되어야 한다. 데이터 처리가 완료된 후 제출된 모든 보고서와 보관의 연속성에 관한 기록은 일괄 수집되어 접근이 제한된 저장 장치내에 보관되어야 하며, 더 이상 유효하지 않을 때까지 혹은 규정에 의해 요구될 때까지 그 저장장치 내에 있어야 한다."[26]

디지털 증거의 입증가치가 높아질수록 그리고 디지털 증거의 유형이 다양해질수록 디지털 포렌식 분석기법은 더욱 정확하고 신뢰성이 있어야 하며, 따라서 누구나 받아들일 수 있는 표준적인 프로세스에 기반을 둠으로써[27], 다양한 형태의 증거에 대한

차 및 증거능력 확보방안, 2006, 196면에서 재인용.

26) 탁희성/이상진, 앞의 보고서, 197-198면에서 재인용.

27) Gary L. Palmer, "Forensic Analysis in the Digital World", http://www.ijde.org/

일관된 방식의 보관의 연속성을 입증할 필요가 있다.[28] 하지만 현재까지는 디지털 증거의 보관의 연속성에 관하여 공식적으로 합의된 기준이나 규약이 존재하지 않기 때문에 각 기관별 실무 매뉴얼을 통해 보관의 연속성을 유지하고 있다.

2) 통합관리정책

디지털 포렌식 프로세스의 근본취지인 결과의 무결성과 신뢰성을 보장하기 위해서는 디지털 포렌식 업무 전체에 걸쳐 적절한 정책들이 시행되고 관리되어야만 한다. 이러한 관리정책은 디지털 포렌식이 일정한 수준의 품질기준을 충족하기 위해 어떻게 운영되어야 하는지에 대한 기관의 기본방침으로서 확립되어야 하는 것이다. 그리고 디지털 기술이 끊임없이 변화·발전하는데 따른 법률과 규제 그리고 기술의 변화를 지속적으로 정책에 반영함으로서만 디지털 포렌식 프로세스의 신뢰성이 담보될 수 있다는 점에서 통합적인 관리정책이 필요하다고 할 것이다. 따라서 디지털 포렌식 프로세스에 있어서는 전체적으로 각 단계별 프로세스에 적용되어야 하는 절차적 지침, 표준 및 인증 요건의 확보 및 유지, chain of custody 유지를 위한 단계별 관리 및 통제 정책의 수립 등을 총괄하여 운용할 수 있는 통합관리정책이 수립될 필요가 있다. 즉 기관내 디지털 포렌식 업무의 운용 측면에서 일관되게 적용되어야 하는 절차적·정책적 요구사항이 무엇인지 파악하여 디지털 포렌식 프로세스의 신뢰성을 뒷받침할 수 있는 통합적인 관리방침이 확립되어야 하는 것이다.

먼저 이와 같은 관리적 측면에서 고려되어야 하는 것으로는 디지털 포렌식 업무에 적용되고 있는 절차적 지침의 관리이다. 즉 디지털 포렌식 프로세스에 있어서는 각 단계별로 요구되는 절차적 지침 뿐만 아니라 디지털 포렌식 분야별, 분석매체의 유형별로 적용되어야 하는 절차적 지침들이 존재한다. 이는 국내외를 불문하고 거의 모든 디지털 포렌식 업무를 수행하는 기관내에 예외없이 존재하고 있는 것이다. 즉 동일한 기관내에서 운용되는 포렌식 업무라 할지라도 다양한 포렌식 전문가들이 다양한 방법으로 업무를 수행하기 때문에 일정한 표준운영지침이 제공되지 않으면 일관성 있는 결과를 확보하기가 어렵다고 할 수 있다. 최소한 동일한 업무영역 내에서는 누가 업무를 수행하든지간에 일정한 절차적 지침에 따라 업무가 공정하고 객관적으로 수행

---

archives/docs/IJDE_1.3.doc

28) 탁희성/이상진, 앞의 보고서, 196면에서 재인용.

될 수 있다는 것을 관리적인 측면에서 보장할 필요가 있다고 할 것이다. 그리고 디지털 포렌식에 있어서 절차적 지침은 기술의 변화에 따른 수정가능성을 항상 염두에 두어야 하기 때문에, 정기적인 리뷰를 통해 지침의 적합성 및 개선의 필요성을 지속적으로 점검해야 한다.

디지털 포렌식 프로세스의 관리적인 측면에서 중요하게 고려되어야 할 또 다른 사항은 각 프로세스에 적용되어야 하는 ISO 표준의 준수 및 유지이다. 디지털 포렌식 프로세스에 적용될 수 있는 ISO 표준들이 많이 있는데, 이 표준들은 약 5-10년 주기로 갱신하도록 되어 있다.[29] 따라서 포렌식 업무에 적용되어야 하는 관련 표준들이 정확하게 준수되고 있는지에 대한 관리와 함께, 관련 표준들을 점검하여 요구되는 수정사항들이 제대로 반영되고 있는지 여부 그리고 갱신주기의 누락으로 인한 표준의 신뢰성 배제 등의 문제가 발생하지 않도록 관리할 수 있는 시스템이 마련되어야 한다.

그리고 이와 함께 디지털 포렌식 프로세스의 관리정책에 있어서 중요하게 고려되어야 하는 것이 디지털 포렌식 관련 시설의 환경 적합성 유지와 시설내 장비의 기능점검 및 유효기간의 관리이다. 즉 디지털 증거의 특성상 온·습도의 변화에 취약하고, 자기장이나 전자파로 인한 증거의 훼손이 발생할 수 있기 때문에 디지털 증거를 보존하고 관리할 수 있는 환경적 조건이 유지되고 있는지를 지속적으로 점검해야 한다. 또한 디지털 포렌식 업무에 사용되는 장비의 기능들이 유효하게 작동하는지에 대한 정기적인 재검증과 함께 그 유효성이 담보될 수 있는 기간이 명확하게 준수될 수 있도록 관리방침을 설정해야 할 것이다.

다. 법률적 요소

1) 적법절차의 준수

디지털 포렌식 프로세스는 과학적 지식과 기술을 활용하여 수집된 디지털 증거가 유효하게 법정에서 그 입증가치를 인정받도록 하기 위한 일련의 절차라고 할 수 있다. 따라서 디지털 포렌식 프로세스에서 요구되는 법률적 요구사항을 준수하지 못하게

---

29) David Watson/Andrew Jones, Digital Forensics Processing and Procedures : Meeting the Requirements of ISO 17020, ISO 17025, ISO 27001 and Best Practice Requirements, 2013, p.14.

되면 아무리 중요한 입증가치를 지닌 증거라 할지라도 그 적법성에 흠결이 생기게 되고 결국 증거로서 활용되지 못하는 결과를 초래한다. 즉 디지털 포렌식 프로세스에 있어서 엄격히 요구되는 법률적 요소는 적법절차라고 할 수 있다.

디지털 포렌식에 있어서 요구되는 적법절차와 관련하여 논의되는 주된 문제로는 압수·수색의 권한과 그 허용범위를 들 수 있다. 각 나라마다 수집하고자 하는 디지털 증거의 유형 - 통신 데이터와 일반 데이터에 따라 - 에 따라 압수·수색의 권한 관련 법률을 달리 두고 있으며, 증거수집을 위한 합법적 권한을 확보한 경우라 하더라도 수집과정에서 그 권한에 의해 허용되는 범위의 적법성 여부 - 관련성과 plain view 문제 - 와 관련하여서는 끊임없이 소송의 쟁점이 되고 있을 만큼 압수·수색의 적법성 확보가 디지털 포렌식 프로세스의 유효성을 판단하는 핵심적 기준이 되고 있다고 할 수 있다.

특히 우리나라와 같이 디지털 증거의 압수·수색에 있어서 법률로서 "원칙적 선별압수, 예외적 매체압수"라고 하는 압수방법을 규정하고 있는 경우에 있어서는, 원칙과 예외에 대한 판단기준을 어떻게 해석하는가에 따라 위법수집증거가 될 수도 있다는 점을 고려하면, 디지털 포렌식 프로세스에 있어서 절차적 적법성 확보에 대한 사전적 검토가 필수적이라 할 것이다.

2) 증거법적 요구사항

법과학은 과학기술의 지식과 도구의 도움으로 그것이 없었더라면 밝혀질 수 없었던 실체적 진실을 판단할 수 있는 정보를 제공한다[30]는 점에서 오늘날 범죄수사에 있어서 없어서는 안되는 존재로서 인식되고 있다. 하지만 법과학적 판단의 기초가 되는 과학적 이론의 오류, 검사 및 분석도구의 오류, 분석대상의 오염 및 훼손, 전문가의 실수 등으로 인해 잘못된 결과 내지 부정확한 결과가 산출되는 경우에는 오히려 실체적 진실을 호도하는 결과를 초래할 수도 있다.[31] 따라서 법과학적 판단에 기초한 증거에 대해서는 그에 적용된 과학이론이나 응용기술의 타당성 및 신뢰성에 대한 법적 판단을 전제로 해서만 그 증거능력의 허부가 논의될 수 있다. 마찬가지로 법과학의 한 분야인 디지털 포렌식에 있어서도 활용되는 기술 및 도구, 전문가에 대한 신뢰성

30) 임종인, 경찰의 차세대 디지털 포렌식 기반 구축방안, 2008, 29면.
31) 임종인, 앞의 보고서, 29면.

판단을 전제로 해서만 그에 의해 산출된 디지털 증거의 증거능력을 논의할 수 있다고 할 것이다. 이와 같이 디지털 포렌식에 적용되는 기술과 지식 등의 신뢰성을 담보하기 위한 방법으로서 디지털 포렌식 품질표준에 따른 품질관리시스템이 현재 주로 논의되고 있다.

그리고 디지털 증거의 취약성으로 인해 디지털 포렌식에 있어서는 복제본에 대한 조사 및 분석을 원칙으로 하는데, 이로 인하여 원본과 복제본의 동일성 입증 역시 증거능력의 요건으로서 요구되고 있다. 이와 관련하여 디지털 포렌식에 있어서는 원본과 복제본의 동일성 입증방법으로서 기술적 요구사항인 해시값 함수를 산출해냄으로써 동일성 문제를 해결하고 있다. 이와 같이 디지털 포렌식 프로세스에 있어서는 증거법적 요구사항을 기술적 방식을 통해 충족시킬 수 있는 방안을 고려해야만 한다.

3. 디지털 포렌식의 기본원칙

디지털 포렌식의 기본원칙과 관련하여 미국 NIJ의 "Electronic Crime Scene Investigation : A Guide for first Responders", "Forensic Examination of Digital Evidence: A Guide for Law Enforcement"에서 다음의 3가지 원칙을 제시하고 있다.

"ⅰ) 디지털 증거를 수집하고 보존하기 위해 취해진 조치들이 증거의 무결성에 영향을 미쳐서는 안된다.
ⅱ) 디지털 증거의 조사를 행하는 사람은 그 목적을 위해 훈련을 받아야만 한다.
ⅲ) 압수·조사·저장 또는 디지털 증거의 이전과 관련한 활동들은 기록되고, 보존되고, 리뷰를 위해 활용가능해야 한다."[32]

그리고 영국의 Association of Chief Police Officer(ACPO)가 만든 "Good Practice Guide for Digital Evidence"에서도 다음과 같은 4가지 기본원칙을 제시하고 있다.

"ⅰ) 법집행기관, 그 기관에 채용된 사람 또는 그들의 소속직원 어느 누구도 차후에

32) U.S. Dept. of Justice, Electronic Crime Scene Investigation: A Guide for First Responders, 2nd.ed. 2008, p.vii.; U.S. Dept. of Justice, Forensic Examination of Digital Evidence: A Guide for Law Enforcement, NIJ Special Report, 2008, p.1.

법정에서 요구될 수 있는 데이터를 변경해서는 안된다.

ii) 어떤 사람이 원본 데이터에 접속할 필요가 있다는 것을 발견한 경우, 그 사람은 그렇게 할 수 있는 자격이 있어야 하고, 그러한 조치의 중요성과 함의를 설명하는 증거를 제공할 수 있어야 한다.

iii) 디지털 증거에 적용된 모든 프로세스에 대한 기록과 감사추적(audit trail)이 만들어져야 하고 보존되어야 한다. 독자적인 제3자가 그러한 프로세스를 조사할 수 있어야 하고 동일한 결론에 도달할 수 있어야 한다.

vi) 수사를 담당하는 사람은 법률과 원칙이 고수되도록 종합적인 책임을 진다."[33]

한편, 우리 대검찰청의 과학수사실무매뉴얼 내의 디지털 포렌식에 있어서 제시하고 있는 디지털 증거 취급원칙으로는 적법절차 준수, 동일성·무결성 유지, 신뢰성 확보 등이 있다.

이와 같이 미국와 영국 그리고 우리의 정부기관에서 디지털 포렌식의 기본원칙으로 제시하고 있는 내용을 정리해 보면, 무결성·적법절차·chain of custody·재현가능성이 디지털 포렌식에서 준수되어야 하는 기본원칙이라 할 것이다.

가. 무결성 원칙

디지털 포렌식 프로세스에 있어서 무결성 원칙에의 요구는 디지털 증거의 본래적 특성인 취약성에서 비롯된 것이라 할 수 있다. 즉 디지털 증거는 고의가 아니더라도 외부적 환경 - 온도, 습도, 자기장, 정전기 등 - 으로 인해 손상될 수 있고, 운영시스템의 설정방식에 따라 전자적으로 저장된 내용이 자동으로 변경·추가·삭제될 수도 있다. 또한 전원의 on/off 행위, 파일을 열거나 열린 파일을 닫는 단순한 행위로도 데이터 관련 정보가 변경될 수 있다. 따라서 증거로서 수집한 그 순간에 확보한 디지털 증거가 여러 가지 위험요인에 노출되지 않은 상태로 안전하게 이송 및 보존되었고, 분석되어 산출된 결과가 그와 같이 무결성이 보장된 프로세스를 통해 이루어졌다는 것이 법정에서 입증되어야만 한다.

---

33) Association of Chief Police Officers, ACPO Good Practice Guide for Digital Evidence, ver.5, 2012, p.6.

디지털 증거는 유체물과 같이 형상이 보존되는 것이 아니라서 그 내용을 본다고 해서 변경이나 훼손 여부를 확인할 수는 없기 때문에 그 무결성을 입증하기 위해서는 기술적·절차적 방법이 적용되어야 한다. 무결성을 입증하기 위한 기술적 방법으로는 디지털 데이터에 대한 이미지 파일을 생성하거나 압수한 디지털 데이터의 복사본에 대한 해시값을 산출하여 원본 데이터의 해시값과 비교함으로써 데이터 변경의 부재를 입증할 수 있다. 그리고 절차적 방법으로는 디지털 데이터가 압수 현장에서부터 법정에 제출될 때 까지 동일성을 유지한 상태에서 안전하게 수집·이송·분석되었고, 각 단계별 절차적 요구사항이 준수되었다는 것을 문서로 기록하여 입증함으로써 무결성을 담보할 수 있다.

나. 적법절차의 원칙

디지털 포렌식 프로세스는 수사기관에 의한 강제처분으로서 압수·수색으로부터 시작하기 때문에 형사소송의 기본원칙인 적법절차의 준수가 필수적으로 요구된다. 즉, 법률에 근거한 적법한 권한에 기하여 법에 정해진 절차에 따라 행해져야 하는 것이다. 따라서 만약 적법절차에 의하지 않고 수집된 증거는 위법한 증거로서 형사소송법 제308조의2 위법수집증거배제 규정에 의해 증거능력이 배제될 뿐만 아니라 이를 기초로 획득한 이차적인 증거도 유죄의 증거로 삼을 수 없다.

디지털 포렌식에 있어서 적법절차의 준수가 엄격히 요구되는 이유는 디지털 매체 등의 압수시 그 저장된 정보의 용량이 엄청나게 많을 뿐만 아니라, 그 내용에 있어서도 범죄와 무관한 정보, 프라이버시 보호의 대상 - 의료정보, 금융정보 등 - 이 되는 정보, 법적 보호의 대상 - 특허, 저작권, 산업기밀 등 - 이 되는 정보 등이 혼재되어 있기 때문이다. 즉 절차의 적법성을 준수하지 않음으로 인해 침해될 수 있는 권리의 범위가 기존의 물리적 증거와는 비교되지 않을 만큼 광범위하다고 할 수 있다. 따라서 디지털 포렌식에 있어서 적법절차 원칙은 국가를 불문하고 가장 기본적으로 엄격한 준수가 요구되는 원칙이라 할 것이다.

다. chain of custody 원칙

디지털 포렌식 프로세스에 있어서 chain of custody는 무결성의 원칙에 필연적으로 수반되는 원칙이라 할 수 있다. chain of custody는 증거의 수집, 이송, 분석, 제출, 보존, 폐기에 이르는 각 단계에서 디지털 증거에 적용된 무결성 보장을 위한 조치들이 깨어지지 않고 유지되었음을 의미하는 것으로, 일반적으로 보관의 연속성 또는 절차의 연속성으로 불리워진다. 이러한 보관 또는 절차의 연속성이 유지되기 위해서는 각 절차 사이에 단절이 발생하지 않았다는 것 뿐만 아니라, 각 절차별로 적절한 통제와 관리정책이 일관되게 적용되었다는 점, 각 절차에서 활용된 시스템의 정확성 및 오류가능성도 입증되어야 한다.

라. 재현의 원칙

재현의 원칙이란 제3자가 동일한 프로세스를 재현할 수 있으며, 법정에 제출된 것과 동일한 결론에 도달할 수 있어야 함을 의미한다. 즉 누가 하더라도 동일한 조건하에서 동일한 프로세스를 거쳤을 때는 동일한 결과가 산출되어야 한다는 것이다.

이는 다양한 디지털 포렌식 도구를 사용해도 동일한 대상 시스템을 조사하였을 경우 항상 같은 결과가 도출되어야 한다는 의미이다.[34] 즉 신뢰성 있는 도구를 전문가가 일반적으로 통용되는 기술과 지식을 사용하여 분석했을 경우 언제든지 동일한 결과가 나와야 한다는 의미로 이해되어야 하는 것이다.[35] 그리고 이러한 재현을 가능하게 하기 위해서는 디지털 포렌식 프로세스 전 과정에 걸쳐 당해 디지털 증거에 취해진 모든 조치들, 사용된 도구의 기술적 요구사항 및 버전, 분석방법 등이 기록되고 보존되어야 한다.

4. 디지털 포렌식 프로세스의 필요성

디지털 포렌식 업무를 수행하는 대부분의 기관들은 업무 관련 지침 및 도구 개발, 분석절차 등을 개별적으로 제작하여 운용하고 있다. 즉 디지털 포렌식 업무와 관련하

34) 정교일, "디지털 증거의 압수와 공판정에서의 제출방안", 형사법 신동향, 2010, 125면.
35) 김지홍, 디지털 포렌식 절차모델에 대한 새로운 접근, 서울대 석사논문 2015, 15면.

여 표준적인 요구사항이나 구조화되고 일관된 포렌식 절차가 제시된 바가 없기 때문이다. 이로 인해 기관내 포렌식 방식이나 절차의 신뢰성에 대하여 이의가 제기되는 경우에는 이를 뒷받침할 수 있는 객관적 기준을 제시하기 어렵게 되어 있다. 더욱이 디지털 증거와 관련되는 기술들이 엄청난 속도로 변화·발전하고 있는 상황에서 각 기관별로 독자적으로 절차와 도구를 운용하게 되면 그 변화를 따라가는데 한계가 있을 수 밖에 없다. 따라서 프로세스 단계별로 갖추어지고 준수되어야 할 표준적인 사항이 사전에 제시되어 있게 되면 기술적· 환경적 변화에 따른 프로세스의 수정이 보다 용이해질 수 있고, 동일한 프로세스를 적용하는 기관간 정보의 공유도 가능해지기 때문에 변화의 수용이 빨라질 수 있는 측면이 있다. 따라서 디지털 포렌식 프로세스는 수사에 있어서 디지털 포렌식의 중요성이 늘어남에 따라 함께 그 중요성이 높아져 가고 있는 추세라 할 것이다.[36]

디지털 포렌식 초기에는 포렌식 도구와 분석결과의 신뢰성에 주로 논의의 초점이 맞추어졌고, 그 다음에는 Chain of Custody, 즉 보관의 연속성을 통한 무결성의 입증에 초점이 맞추어졌으며, 이제는 전체적인 디지털 포렌식 프로세스 자체에 대한 신뢰성으로 논의의 중심이 옮겨가고 있다고 보여진다. 즉 기술수준이 고도화될수록 오히려 디지털 데이터의 입증가치를 확보할 수 있는 상황은 점점 더 취약해지고 있기 때문에, 디지털증거를 확보해서 폐기할 때까지의 각 단계별로 고도의 일관성과 검증가능성을 유지할 수 있는 과학적 입증방법이 요구되고 있고, 이를 뒷받침하기 위해 신뢰할 수 있는 프로세스 구축의 필요성과 중요성에 대한 인식이 높아져 가고 있다고 할 수 있다.

급속한 기술의 발전은 그것이 사용되고 있는 동안에도 끊임없는 변화를 가져오기 때문에 지속적으로 새로운 도구와 기법, 절차의 개발에 관한 필요성이 제기될 뿐만 아니라 그것들이 인증을 받고 검증될 필요성을 야기하는 측면이 있는데, 디지털 포렌식 프로세스는 이러한 필요성들을 일관되고 신뢰할 수 있는 프레임안에서 수용할 수 있도록 한다는 점에서 중요하다고 할 것이다.

---

36) Sean E.Goodison/Robert C.Davis/Brain A. Jackson, “Digital Evidence and the U.S. Criminal Justice System-Identifying technology and other needs to more effectively acquire and utilize digital evidence”, ; https://www.ncjrs.gov/pdffiles1/nij/grants/248770.pdf.; 2016.4.10.

가. 기관내 포렌식 업무품질의 질적 수준 유지

현재 국내외를 막론하고 디지털 포렌식 업무를 수행하는 대부분의 기관들에 있어서 디지털 데이터의 과잉으로 인한 디지털 포렌식 분석관의 업무부담이 중요한 문제로 제기되고 있다. 즉 디지털 정보에 대한 수사의 중요성이 증가할수록 디지털 포렌식의 필요성 역시 증가하고 있는 상황에서, 디지털 포렌식 업무에 종사하는 직원은 소수에 불과하여 업무부담이 점차 강화되어가는 추세에 있다는 것이다. 이러한 업무부담은 단순히 디지털 포렌식 분석관 개인의 문제에 그치는 것이 아니라, 포렌식 분석관의 재교육기회를 빼앗기 때문에 포렌식 프로세스내의 피드백회로에 문제를 발생시킬 뿐만 아니라, 불가피하게 디지털 포렌식에 비전문가인 수사관들로 하여금 수사초기단계에서 요구되는 포렌식적 조사를 분담케 함으로써 포렌식 업무의 신뢰성 확보에 문제를 발생시킬 수 있다는 점에서 중요한 문제라 할 수 있다.[37]

즉 디지털 포렌식 업무를 담당하는 분석관 등은 끊임없이 발전하는 디지털 기술을 습득할 수 있는 교육의 기회를 가져야 하고, 그 결과에 대한 검증을 통해 자신의 전문적 지식의 수준을 유지해야 하는 것이 필수적이다. 그런데 기관내 포렌식 업무부담으로 인해 이러한 교육과 재검증의 기회를 박탈당하게 되면 전문가로서의 신뢰성을 담보하기가 어려울 뿐만 아니라 내외부 기관의 디지털 포렌식 전문가 간에 심각한 수준의 격차가 발생할 수도 있다.

또한 업무부담을 줄이기 위한 한 방법으로, 수사중인 사건에 있어서 데이터를 식별할 수 있는 능력과 기본적인 논리적인 추출을 제공할 수 있도록 하기 위해 도구를 사용하는 방법에 대하여 기초적인 교육만을 시행한 상태에서 수사관이나 현장 조사관에게 디지털 포렌식 초기 업무를 맡기는 경우가 일반적이다. 하지만 이들은 전문가가 아니기 때문에 차후 법정에서 데이터 추출을 위해 사용된 방법에 대해 증언을 할 수 없을 뿐만 아니라, 그로 인하여 전체적인 디지털 포렌식 프로세스 자체의 신뢰성에 문제를 야기할 수도 있는 것이다.[38] 이와 같이 기관내에 디지털 포렌식 업무를 수행하

37) Sean E. Goodison/Robert C.Davis/Brain A.Jackson, "Digital Evidence and the U.S. Criminal Justice System:Identifying Technology and other needs to more effectively acquire and utilize digital evidence", https://www.ncjrs.gov/pdffiles1/nij/grants/248770.pdf; 2016.7.30.

38) Sean E. Goodison/Robert C.Davis/Brain A.Jackson, op.cit., https://www.ncjrs.gov/pdffiles1/nij/grants/248770.pdf; 2016.7.30.

는 사람의 전문성의 수준에 있어서 현실적인 편차가 존재한다는 것은 디지털 포렌식 자체의 신뢰성에 심각한 문제를 제기할 수 있다고 할 것이다.

그리고 디지털 매체 관련 기술들이 급속하게 발전함에 따라 그러한 장치로부터 데이터를 추출하고 분석하는 기술 또한 끊임없이 변화·발전할 수 밖에 없다. 하지만 디지털 포렌식 분야에 있어서 새로이 개발되는 기술들은 광범위한 리뷰 없이 그리고 관련 학계 내지 업계의 심사없이 업무의 필요성에 근거하여 개발되고 있고, 바로 업무에 활용되어 결과를 산출해내기 때문에 지속적으로 신뢰성의 문제가 제기될 수 밖에 없다. 특히 개발된 도구에 적용된 요구사항이 정확히 구현되는지, 그에 따라 정확한 결과가 도출되는지 여부를 확인할 수 있는 기술적 평가방법이 없는 상황에서 - 미국의 경우에는 CFTT에서 이러한 평가를 수행하지만 우리나라는 그러한 평가기구가 없다 -, 각 기관별로 개발된 도구와 지식을 활용하는 경우에 이것이 어느 정도의 정확성과 신뢰성을 갖는가에 대하여 확인할 방법이 없다고 할 수 있다.

이와 같이 기관별 디지털 포렌식 도구 및 전문가의 수준에 있어서 상당한 편차가 존재하기 때문에 최소한 그에 의해 산출된 결과의 품질을 통제할 수 있는 장치가 마련되어야 한다. 즉 디지털 포렌식의 업무품질을 담보할 수 있는 정책적 프레임이 존재해야만 법적인 문제에 있어서 디지털 증거에 대한 과학적 조사, 분석 및 평가의 결과에 대한 신뢰를 확보할 수 있기 때문이다. 이러한 디지털 포렌식의 품질표준을 확보하기 위한 정책적·절차적 프레임으로 제시될 수 있는 것이 디지털 포렌식 프로세스라 할 수 있고, 이러한 프로세스 전체에 걸쳐 공인된 표준의 적용, 유효한 통제 및 관리정책을 유지함으로써 디지털 포렌식 결과에 대한 고도의 신뢰를 제공할 수 있다고 할 것이다.

나. 법정 증거로서 디지털 데이터의 동일성 및 무결성 입증을 위한 절차적 수단

디지털 증거의 증거능력을 판단함에 있어서 요구되고 있는 일반적인 법적 판단기준은 동일성과 무결성에 대한 입증이라 할 수 있다. 이러한 디지털 증거의 동일성과 무결성에 대한 입증은 증거 자체에 대해 직접적으로 행해지는 것이 아니라 그 증거를 취급한 전문가, 도구, 관리절차 등의 검증을 통해 간접적으로 증명되어진다.[39] 즉 디지털 증거의 무결성을 담보하기 위해서는 디지털 증거에 적용되는 디지털 포렌식의

각 단계별 절차에서 요구되는 사항들이 일정한 수준의 신뢰척도에 부합한다는 것이 입증되어야 할 뿐만 아니라, 디지털 증거가 현장에서부터 법정까지 유효하게 관리 및 보존되어 왔다는 것이 입증되어야 하는 것이다.

이와 같이 디지털 증거를 신뢰가능한 방식과 절차를 통해 그 동일성과 무결성을 유지·관리할 수 있도록 하는 일관된 프레임을 제시할 수 있는 것이 디지털 포렌식 프로세스라 할 수 있다. 즉 일관된 디지털 포렌식 프로세스내에서 디지털 증거의 chain of custody를 유지할 수 있게 함으로써 절차의 단절에 따른 오류의 개입을 차단할 수 있다는 점에서 디지털 포렌식 프로세스는 디지털 증거의 동일성과 무결성을 보장할 수 있는 절차적 수단으로서 기능할 수 있다고 할 것이다.

다. 형사소송법 개정에 따른 포렌식 전문가 증언의 신뢰성 입증 자료

범죄수사를 함에 있어서 엄격한 적법절차와 기관의 정책적·기술적 표준절차에 따라 무결성과 동일성을 유지한 디지털 증거를 확보해도 그 증거가 법정에서 허용될 수 있는가 하는 문제는 법적인 판단의 문제로서 남게 된다. 그런데 기존의 증거방법인 인적·물적 증거 그리고 서증을 중심으로 마련된 현행 증거법상 규정들이 본질적으로 상이한 증거방법인 디지털 증거에는 적합하지 않음에도 불구하고 여전히 디지털 증거의 증거능력에 대해서 기존의 증거법상 규정들이 적용되고 있다.

공판중심주의 및 구두변론을 중심으로 하는 영미 형사절차에 있어서는 디지털 정보나 기록과 같은 2차적 자료에 의해 획득한 지식은 원칙적으로 전문증거로 간주하여 증거능력을 배제하고 있다. 우리 형사소송법 제310조2도 전문증거의 증거능력을 제한하고 있기 때문에 대법원 역시 그 내용의 진실성과 관련하여서는 디지털 증거에 대해 전문법칙이 적용된다고 보고 있다.[40] 따라서 형사소송법 제313조 제1항에 따라 그 작성자 또는 진술자의 진술에 의하여 성립의 진정함이 증명된 때에 한하여 증거로 사용할 수 있다. 하지만 기존의 진술증거와 달리 디지털 증거는 그 성립의 진정성을 기술적 방법을 통해 객관적으로 입증할 수 있음에도 불구하고, 작성자 등의 진술에

39) 박희일/윤종성/이상진, “디지털 포렌식 수준 평가지표 개발에 관한 연구”, 정보보호학회 논문지 Vol.24, no.5, 2015, 1154면.
40) 대법원 2013.2.15. 선고 2010도3504.

의해 인정되지 않으면 증거능력이 배제되는 불합리한 결과가 초래되어 왔다. 이러한 디지털 증거의 진정성립과 관련하여 제기되는 논란에 대하여 대법원은 "디지털 저장매체로부터 출력된 문서에 관하여는 저장매체의 사용자 및 소유자, 로그기록 등 저장매체에 남은 흔적, 초안 문서의 존재, 작성자만의 암호 사용 여부, 전자서명의 유무 등 여러 사정에 의하여 동일인이 작성하였다고 볼 수 있고 그 진정성을 탄핵할 다른 증거가 없는 한 그 작성자의 공판준비나 공판기일에서의 진술과 상관없이 성립의 진정을 인정하여야 한다는 견해가 유력하게 주장되고 있는 바, 그 나름 경청할 만한 가치가 있는 것은 사실이나, 입법을 통하여 해결하는 것은 몰라도 해석을 통하여 위와 같은 실정법의 명문조항을 달리 확장 적용할 수는 없다"[41]고 판시함으로써 디지털 증거의 진정성립과 관련해서는 별도의 입법적 해결이 필요하다는 입장을 나타냈다.

이러한 논의들이 뒷받침되어 2016년 5월 형사소송법 제313조 제2항을 개정하여 "제1항 본문에도 불구하고 진술서의 작성자가 공판준비나 공판기일에서 그 성립의 진정을 부인하는 경우에는 과학적 분석결과에 기초한 디지털 포렌식 자료, 감정 등 객관적 방법으로 성립의 진정함이 증명되는 때에는 증거로 할 수 있다. 다만, 피고인 아닌 자가 작성한 진술서는 피고인 또는 변호인이 공판준비 또는 공판기일에 그 기재 내용에 관하여 작성자를 신문할 수 있었을 것을 요한다"고 규정함으로써 디지털 증거의 진정성립의 입증방법으로서 과학적 분석결과에 기초한 디지털 포렌식 자료, 감정 등 객관적 방법을 활용할 수 있게 되었다.

디지털 증거의 진정성립을 기술적으로 입증할 수 있는 방법이 입법적으로 해결되었지만, 구체적으로 디지털 포렌식 자료를 통해 디지털 증거의 진정성립을 어떻게 입증할 것인가가, 그리고 디지털 포렌식 자료를 산출한 과학적 분석결과의 신뢰성은 어떻게 담보할 것인가가 앞으로 논의되어야 할 과제로 남아있다고 할 것이다. 먼저 디지털 포렌식 자료를 통한 디지털 증거의 진정성립의 입증은 고도의 신뢰성과 결과 품질을 담보할 수 있는 디지털 포렌식 프로세스를 통해 산출된 것임을 제시함으로써 충분히 가능하다고 볼 수 있다. 특히 디지털 포렌식 프로세스 각 단계별 요구사항에 부합하는 인증 및 평가시스템의 준수와 전체 프로세스에 적용된 통제 및 관리정책을 통한 무결

41) 대법원 2015.07.16. 선고 2015도2625 전원합의체 판결

성 유지 등의 입증을 통해 진정성립을 증명할 수 있다고 할 것이다. 이러한 디지털 포렌식 프로세스의 준수 및 유지에 대한 입증은 궁극적으로 포렌식 자료를 산출한 디지털 포렌식 전문가의 증언에 의해서 이루어질 것이므로, 디지털 포렌식 프로세스는 디지털 포렌식 전문가 증언의 신뢰성을 뒷받침할 수 있는 충분한 입증자료로서 역할을 하게 될 것이라 생각한다. 따라서 일관된 프레임을 갖춘 디지털 포렌식 프로세스를 구축하고 그러한 프로세스를 통해서 산출된 결과를 법정 증거로서 제시하는 것이 디지털 포렌식 업무를 수행하는 기관들에 있어서 앞으로의 과제라 할 것이다.

한편, 디지털 포렌식 자료를 산출한 과학적 분석의 신뢰성과 관련하여서는 Daubert test와 같은 과학적 증거에 대한 심사기준이 제시되어야 할 것으로 생각된다. 하지만 디지털 포렌식에 있어서 Daubert test 기준을 적용하는데는 그 기술적 특성으로 말미암아 일정한 한계가 있기 때문에, 디지털 포렌식 기술이 과학적 분석으로서 신뢰성을 확보할 수 있도록 일정한 법적 심사기준이 마련되어야 할 것이다.

5. 디지털 포렌식 프로세스 모델의 변화

1984년 초부터 FBI와 다른 사법기관들이 컴퓨터 증거를 조사하기 시작하면서 조사를 수행함에 있어서 채택된 프로세스나 절차가 조사의 결과에 직접적 영향력을 갖는다는 인식을 갖게 되었고, 따라서 공식화된 프로세스가 도입되기 시작했다. 즉 컴퓨터 포렌식에 있어서 부적절한 프로세스를 선택하는 경우 불완전하거나 실효성 없는 결과를 초래할 우려가 있을 뿐만 아니라, 임의적이거나 구조화되지 않은 방식으로 확보된 증거들이 법정에서 허용되지 않을 수 있는 위험이 있다고 보았던 것이다.[42]

이와 같이 구조화된 표준 프로세스의 존재는 컴퓨터 포렌식 조사관이 준수해야할 적절한 매카니즘을 제공하는 방식이 되기 때문에, 수년간에 걸쳐 다수의 컴퓨터 포렌식 조사 프로세스가 새롭게 개발되거나 기존모델에 대한 개선방안들이 제안되어왔다. 따라서 아래에서는 그동안 여러 논문들을 통해 제시되어온 디지털 포렌식 모델이 어떻게 변화되어오고 있는지 살펴보고자 한다.

---

42) Yunus Yusoff, Rosland Ismail and Zainuddin Hassan, “Common Phases of Computer Forensics Investigations Models”, International Journal of Computer Science & Information Technology, Vol.3, No.3, June 2011. p. 17.

가. 기존 디지털 포렌식 프로세스 모델

1) Computer Forensic Investigative Process(1984)

이 프로세스는 디지털 증거조사를 다루는 방법론을 제안한 것으로, 그 결과가 과학적으로 신뢰할 수 있고, 법적으로 허용될 수 있도록 하기 위한 것이었다.[43] 이 방법론을 제안한 Politt는 기존의 문서에 기반한 증거획득절차를 토대로 디지털 증거를 획득하는 경우 각 단계에 있어서의 제기되는 문제를 디지털 패러다임안에서 어떻게 해결할 것인가를 제시하고 있다.

즉, 이 프로세스는 획득(Acquisition) ⇒ 확인(Indentification) ⇒ 평가(evaluation) ⇒ 증거로서의 승인(Admission as evidence) 4단계로 구성되어 있는데, 먼저 획득단계에서는 수색을 할 수 있는 법률상 권한을 확보하기 위한 엄밀한 법해석적 토대와 실제 그 수색을 수행할 수 있는 기술적 능력을 요한다고 보았다. 다음으로 확인단계에서는 다시 3단계의 프로세스를 제시하는데, 첫째 디지털 증거가 매체의 특정한 부분에 존재한다는 것을 물리적인 형태로 설명할 수 있어야 하고, 둘째, 그것의 논리적인 위치에 관하여 확인할 수 있어야 하고, 마지막으로 그 의미를 사람이 이해할 수 있는 올바른 문맥으로 전환할 수 있어야 한다는 것이다. 그리고 이 각 단계는 기술적 능력을 요하며 차후에 법정에서 증언을 요할 수 있다고 한다.

평가단계에서는 데이터에 대한 기술적·법적 판단을 수반하는데, 이전단계에서 확인된 구성요소가 조사되고 있는 사건과 관련이 있는가, 그리고 합법적인 증거로서 고려될 수 있는가의 여부를 판단하며, 마지막 승인단계는 획득된 그리고 추출된 증거가 법정에 제출되는 것으로 설명하고 있다.

그리고 이러한 프로세스는 법률과 과학 양자를 모두 준수해야 하고, 어느 한 분야에서라도 실패하게 되면 그 결과물의 제출은 법률상 무의미하다고 결론짓고 있다.

2) DFRWS Model(2001)

디지털 포렌식 연구 워크숍(DFRWS:The Digital Forensic Research Workshop)은 학계와 실무계로 구성된 커뮤니티 포럼으로, 그 당시 디지털 포렌식 상황을 이끌어내

---

43) http://www.digitalevidencepro.com/Resources/Approach.pdf; 2016.5.3.

는 합의문을 만들어 내면서 디지털 포렌식은 몇가지 합의된 단계를 가진 절차라는 결론을 제시했으며, 7단계로 구성된 일반적인 목적의 디지털 포렌식 조사 프로세스를 제안했다.[44]

Identification	Presevation	Collection	Examination	Analysis	Presentation	Decision
Event/Crime Detection	Case Management	Preservation	Preservation	Preservation	Documentation	
Resolve Signature	Imaging Technologies	Approved Methods	Traceability	Traceability	Expert Testimonoy	
Profile Detection	Chain of Custody	Approved Software	Validation Techniques	Statistical	Clarification	
Anomalous Detection	Time Synch.	Approved Hardware	Filtering Techniques	Protocols	Mission Impact Statement	
Complaints		Legal Authority	Pattern Matching	Data Mining	Recommended Countermeasure	
System Monitoring		Lossless Compression	Hidden Data Discovery	Timeline	Statistical Interpretation	
Audit Analysis		Sampling	Hidden Data Extraction	Link		
Etc.		Data Reduction		Spacial		
		Recovery Techniques				

[그림 1] DFRWS Model[45]

즉 이 프로세스 모델은 확인→ 보존→수집→조사→분석→제출→판단 이라는 디지털 포렌식 조사 프로세스를 제시하고 있는데, 특히 두 번째 단계인 보존단계에서 적절한 사건관리를 확립하고 허용할 수 있는 Chain of Custody를 제시함으로써 수집된 데이터가 오염이 없도록 보장하는 것의 중요성을 강조했다. 그리고 조사단계와 분석단계에서는 증거추적, 증거확인, 숨겨진/암호화된 데이터의 복구, 데이터 마이닝, 타임라인 등과 같은 표준임무의 수행을 제시하고 있다. 특히 이 프로세스 모델은

44) G.Palmer, "DTR-T001-01 Technical Report. A Road Map for Digital Forensic Research", Digital Forensics Workshop(DFRWS), 2001, p.17.

45) DFRWS, "A Road Map for Digital Forensic Research by Collective work of all DFRWS attendes", The Digital Forensic Research Conference, DFRWS 2001 USA, p.17.; http://dfrws.org/sites/default/files/session-files/a_road_map_for_digital_forensic_research.pdf

이전 모델에서 포함되지 않았던 제출(presentation)을 포함함으로써 보다 포괄적이고 강화된 모델로 불리워진다.

이 모델의 장점은 사법기관 보다는 학계에 의해 주도됨으로 인해 디지털 포렌식에 대한 과학적 공동체의 방향을 정의하고 초점을 맞추는데 도움을 주었으며, 이 모델을 토대로 많은 다른 모델들이 제시되었다는 점에서 큰 의의가 있다고 할 수 있다.

3) Forensic Process Model(2001)

NIJ는 전자적 범죄현장 수사에 있어서 프로세스 모델을 제시하였는데, 이 모델이 제시된 문서는 최초 대응자를 위한 가이드라인[46]이었지만, 그 외에도 법집행 및 전자적 범죄현장을 보호할 책임이 있는 다른 대응자, 디지털 증거의 인지 및 수집과 보존에 책임이 있는 다른 대응자들에 의한 활용을 의도한 것이었다. 이 문서에서 제시하고 있는 포렌식 프로세스는 4단계로 구성되어 있는데, 수집→조사→분석→보고 로 되어 있다.

4) Abstract Digital Forensic Model(2002)

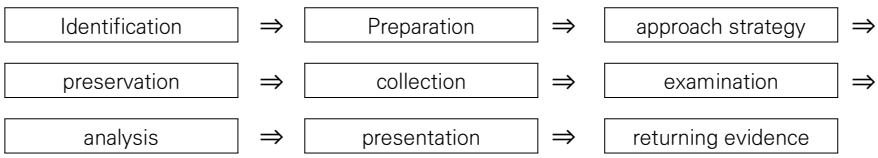
Reith, Carr & Gunsch가 디지털 포렌식에 관한 다수의 모델과 프레임워크를 조사하여 제시한 모델로, 법집행기관에 의해 실시되어온 전통적인 물리적 포렌식 증거수집전략으로부터 아이디어를 얻어 활용한 것이다. 이 모델은 대다수의 디지털 범죄수사에 있어서 포렌식 수행절차가 일관성도 없고 표준화되어 있지도 않으며, 그나마 기초적인 가이드라인을 만들고자 하는 시도가 된지는 얼마되지 않았는데 이것도 기술에 대한 상세한 설명에 초점을 맞추어 기술되어 있을 뿐 일반화된 프로세스에 대한 고려는 없었다고 하는 비판적 검토에 토대를 두었다.[47]

따라서 이 모델은 일관되고 표준화된 디지털 포렌식 도구 개발의 프레임워크, 미래 디지털 기술에 적용할 프레임워크를 위한 매카니즘, 사법기관 구성원들이 기술에 문외한인 사람들에게 기술을 설명하는데 이용할 수 있는 일반화된 방법론 등을 제공하고자 하는데 목적을 두고 있다.[48]

---

46) https://www.ncjrs.gov/pdffiles1/nij/219941.pdf:2016.10.30.
47) Mark Reith/Clint Carr/Gregg Gunsch, "An Examination of Digital Forensic Model", International Journal of Digital Evidence, Vol.1, Issue 3, 2002, p.3.
48) Mark Reith/Clint Carr/Gregg Gunsch,"An Examination of Digital Forensic Model",

저자는 이 모델이 기존의 DFRWS 모델로부터 영감을 받았기 때문에 강화된 DFRWS 모델이라고 기술하고 있으며, 저자가 제시한 모델은 9단계로 구성[49]되어 있다.



[그림 2] Abstract Digital Forensic Model[50]

이 프로세스 모델에서는 3가지의 중요한 단계가 도입되었는데, 준비, 접근전략 그리고 증거의 반환이 그것이다. 먼저 준비단계에서는 도구와 기술, 수색영장의 준비 그리고 권한과 관리지원 확보 등과 같은 활동이 행해지고, 접근전략단계는 오염되지 않은 증거의 확보를 최대화함과 동시에 피해자와 주변사람들에 대한 부정적 영향을 최소화하는데 목표를 두고 있다. 마지막으로 증거의 반환은 합법적인 소유자 또는 적절한 처분권한을 가진 자에게 증거가 안전하게 반환되는 것을 보장하기 위해 도입된 단계이다.

ADFM의 전체적인 프로세스를 간략히 정리하자면, 첫째는 확인단계로, 사고유형을 인지 및 확인하여 사고유형이 확인되면 다음단계인 준비단계가 행해지고 그 다음으로 접근전략단계가 뒤따른다. 다음의 보존단계에서는 획득된 물리적 데이터와 디지털 데이터를 적절히 분리하고 안전하게 보존해야 하기 때문에 Chain of Custody에 유념해야 하며, 다음의 수집단계에서는 데이터의 추출 및 복제가 행해진다. 그리고 조사단계에서는 수집된 데이터로부터 잠재적인 증거를 확인하고 정확한 위치를 찾아내기 위해 체계적인 접근방법을 활용해야 하며, 분석단계에서는 증거의 중요성을 판단하고 발견된 증거에 기반한 결론을 이끌어내야 한다. 제출단계에서는 분석한 결과물을 요약하여 제출하고 마지막으로 증거를 반환하는 것으로 프로세스는 완료되는 것으로

International Journal of Digital Evidence, Vol.1, Issue 3, 2002, p.1.

49) Mark Reith/Clint Carr/Gregg Gunsch, "An Examination of Digital Forensic Model", International Journal of Digital Evidence, Vol.1, Issue 3, 2002, pp.6-7.

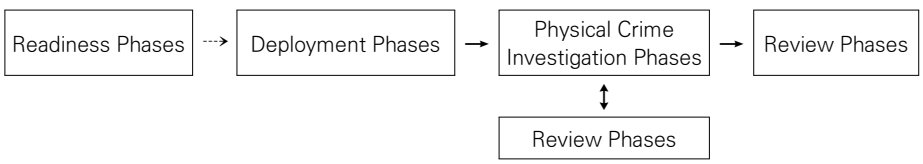
50) ibid.

설명하고 있다.[51]

저자는 이 모델의 단점으로 각 유형이 실제 사용함에 있어서는 지나치게 일반적인 것으로 정의될 수 있으며, 모델을 검증하기 위한 용이하고도 명확한 방법이 없다는 점, 그리고 이 모델에 추가된 하위 유형들이 이 모델을 이용하기 번거롭게 만들 수 있다는 점을 제시하고 있다.[52]

5) IDIP(The Integrated Digital Investigation Process) Model(2003)

Carrier, Spafford가 제안한 모델로, 다양한 활용가능한 조사 프로세스를 하나의 통합된 모델로 결합시키고자 하는 의도를 가진 것이었다. 이 모델은 컴퓨터는 그 자체가 범죄현장, 즉 디지털 범죄현장이라는 이론을 이용해서 물리적인 범죄현장에 관한 조사기법을 디지털 조사에 적용하고 있다. 디지털 범죄현장조사는 물리적 범죄현장과 통합되며 따라서 수집될 수 있는 물리적 증거가 어떤 사람에 대한 디지털 활동과 결부되며, 따라서 디지털 범죄현장은 물리적 범죄현장에 대한 부차적인 범죄현장으로 고려될 수 있다[53]고 설명하고 있다.



[그림 3] IDIP Model[54]

51) Mark Reith/Clint Carr/Gregg Gunsch, “An Examination of Digital Forensic Model”, International Journal of Digital Evidence, Vol.1, Issue 3, 2002, pp.6-7.; Yunus Yusoff, Roslan Ismail. Zainuddin hassan, “Common phases of computer forensics investigation models”, International Journal of Computer Science & Information Technology, vol.3. no.3., p.20.

52) Mark Reith/Clint Carr/Gregg Gunsch, “An Examination of Digital Forensic Model”, International Journal of Digital Evidence, Vol.1, Issue 3, 2002, p.10.

53) Brian Carrier/Eugene H.Spafford, “Getting Physical with the Digital Investigation Process”, International Journal of Digital Evidence, Vol.2, Issue 2, 2003, p. 6. ; https://www.utica.edu/academic/institutes/ecii/publications/articles/A0AC5A7A-FB6C-325D-BF515A44FDEE7459.pdf; 2016.5.20.

54) Brian Carrier/Eugene H.Spafford, op.cit.,p.7.; Venansius Baryamureeba/Florence Tushabe, “The Enhanced Digital Investigation Process Model”, The Digital Forensic Research Conference, DFRWS 2004 USA, p.3.

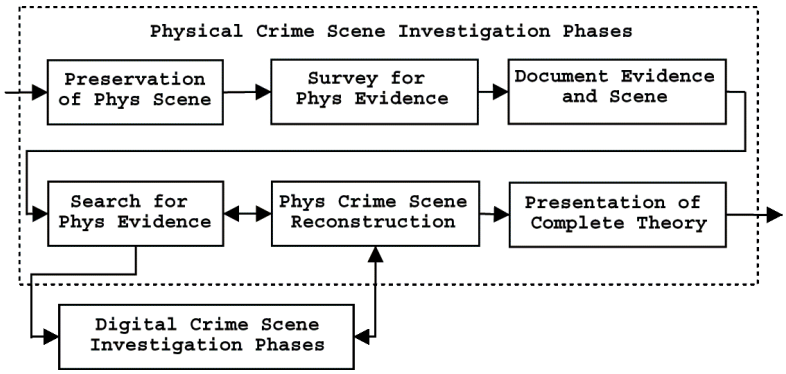
이 모델은 디지털 수사 조직의 라이프사이클 전반에 적용되는 절차를 제시하고 있다. 즉 전체적으로는 17단계로 이루어져 있지만 이를 5개의 그룹으로 유형화하여 구조화하는 방식을 택하고 있다. 이 프로세스는 앞으로의 조사를 뒷받침하기 위해 준비되어야 할 물리적 기반시설과 운영상의 기반시설을 요구하는 단계에서 시작하는데, 이 준비단계에서 필요한 장비들이 준비되고 직원들이 그것을 효율적으로 사용할 능력이 있어야 한다고 설명하고 있다. 준비단계는 특정한 사건이나 범죄와 결부되지 않으며 현재 진행형이다. 이 준비단계는 다시 2개의 하위 단계, 즉 운영상의 준비(Operations Readiness Phase)와 인프라 준비(Infrastructure Readiness Phase)로 구성되는데, 직원에 대한 훈련과 현장 장비 및 실험실내 장비의 기능성, 최신성 및 유지 등을 기술하고 있다.

준비단계 다음은 배치단계인데, 이 단계는 범죄(사고)를 발견하고 확인하는 매카니즘을 제공하는 것으로 2개의 하위단계가 소개되어 있는데, Detection&Notification Phase와 Confirmation&Authorization Phase가 그것이다. Detection&Notification 단계는 조사 프로세스의 시작을 규정하는 것이며, Confirmation&Authorization 단계는 특히 법집행의 상황에 있어서 범죄를 충분히 조사할 수 있는 권한 - 전형적으로 수색영장 또는 다른 법률상의 승인 - 을 취득하는 것이다.[55]

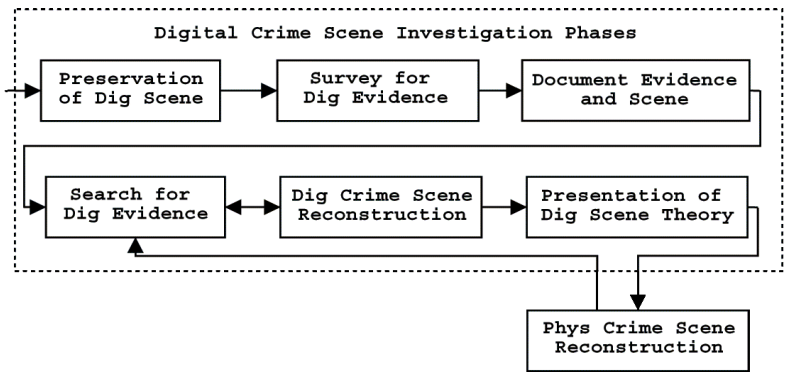
다음으로 물리적 범죄현장 조사단계에서는 물리적인 증거의 수집과 분석이 이루어지는데, 여기에는 보존, 조사, 문서화, 수색, 재구성과 제출이 하위단계를 구성하고 있다. 디지털 범죄현장조사단계는 디지털 환경에서 디지털 증거에 초점을 맞춘다는 것을 제외하고는 물리적 범죄현장 조사단계와 동일하게 구성되어 있다.

---

55) Brian Carrier/Eugene H.Spafford, op.cit., p. 7.



[그림 4] six phases in the physical crime scene investigation[56)]



[그림 5] six phases in the digital crime scene investigation[57)]

이 모델의 마지막 단계는 검토단계로, 물리적 조사와 디지털 조사가 얼마나 잘 운용되었는지, 물리적 조사와 디지털 조사가 얼마나 잘 협력되었는지, 사건을 해결하는데 충분한 물리적 증거와 디지털 증거가 존재했는지의 여부 등을 포함해서 새로운 절차 또는 새로운 훈련요구사항을 초래할 수 있는 개선분야를 확인하기 위해 전체 조사프로세스를 검토하는 것이다.[58)]

이 모델에 대해서는 몇가지 비판이 제기되는데, 첫째, 사전조사가 이루어지기 전까지는 디지털범죄를 확인하는 것이 불가능하며, 둘째, 피해자의 현장과 피의자의 현장

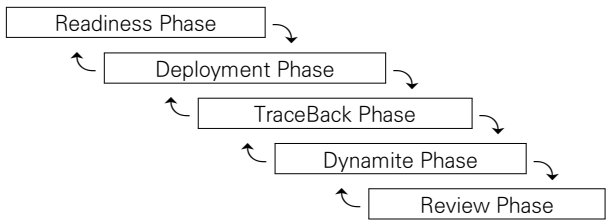
56) Brian Carrier/Eugene H.Spafford, op.cit., p.8.
57) Brian Carrier/Eugene H.Spafford, op.cit., p.10.
58) Brian Carrier/Eugene H.Spafford, op.cit., p. 12.

간의 명확한 구분을 제공하지 못하며, 셋째, 보다 큰 네트워크와 인터넷을 취급하는 경우 그것을 역추적하는 프로세스에 문제가 제기될 수 있다는 것이다.

6) Enhanced Digital Investigation Process Model(EDIP) (2004)

Barayamueeba/Tushaba가 Carrier/Spafford가 제시한 Integrated Digital Investigation Model에 대한 수정안을 제시한 모델로, 역추적 단계와 다이너마이트 단계를 추가적으로 기술하여 1차 주요범죄 현장(컴퓨터)와 2차 범죄현장(물리적 범죄현장)을 명확하게 구분하고자 하였다. 특히 역추적 단계는 조사관으로 하여금 범죄를 실행하기 위해 범죄자가 사용한 실제 장비/컴퓨터를 온전하게 역추적하는 것을 가능하게 할 수 있다.

이러한 구분 목적은 두 개의 범죄현장을 동시에 재구성하는 과정에서 생겨나는 불일치를 최소화하고자 하는데 있었다. 이 모델은 5단계를 제안하고 있는데, 준비단계→배치단계→역추적단계→다이너마이트 단계→검토단계로 되어있다.



[그림 6] EDIP Model[59]

조사 프로세스는 준비단계로 시작하는데 이는 IDIP 모델과 동일한 임무를 수행하는 것으로 되어 있으며, 두 번째 배치단계는 범죄(사고)를 발견하고 확인하는 매카니즘을 제공하는데, 하위 5단계로 구성되어 있다. Detection and Notification Phase, Physical Crime Scene Investigation Phase(보존, 조사, 수색과 수집, 문서화, 제출), Digital Crime Scene Investigation Phase(보존, 조사, 수색과 수집, 문서화),

59) Venansius Baryamureeba/Florence Tushabe, "The Enhanced Digital Investigation Process Model", The Digital Forensic Research Conference, DFRWS 2004 USA, p.6.; https://www.dfrws.org/sites/default/files/session-files/pres-the_enhanced_digital_investigation_process_model.pdf; 2016.5.20.

Confirmation Phase, Submission Phase(물리적 증거와 디지털 증거를 사법기관에 재출하는 것)가 그것이다.[60]

추적단계에서는 주요 목표인 장소와 장비를 포함해서 범죄현장 출처를 추적하는 것으로 하위 2단계로 구성되어 있는데, 디지털 범죄현장 조사와 권한 확보가 그것이다. 디지털 범죄현장으로서 IP 주소는 DNS서버로부터 nslookup, dig, tracert를 활용하여 쉽게 추적되며, 권한확보는 조사를 수행하고 정보에 접근할 수 있는 승인을 관할기관으로 부터 확보하는 것이다.[61]

Dynamite 단계에서는 범인을 확인할 목적을 가지고 주요한 범죄현장에 대한 조사가 수행된다. 이 단계는 4개의 하위단계로 구성되는데, 물리적 범죄현장 조사(보존, 조사, 수색과 수집, 문서화, 제출), 디지털 범죄현장 조사(보존, 조사, 수색과 수집, 문서화), 재구성(수집된 증거를 활용하여 최선의 조사가설을 확인하는 것), 의사소통(최종적인 해석과 결론을 사법기관에 제출)이 그것이다.[62]

이 모델의 마지막 단계는 검토단계로 IDIP 모델과 동일하며, 이 단계에서 전체적인 조사가 검토되고 개선분야가 확인되어진다.

7) Computer Forensics Field Triage Process Model(CFFTPM)(2006)

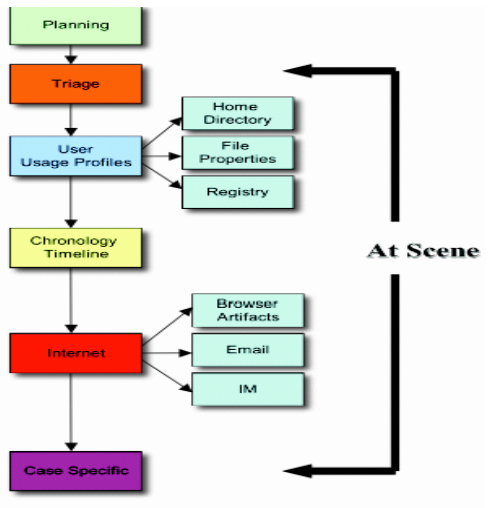
CFFTPM은 매체나 장치를 실험실로 가져올 필요 없이 비교적 짧은 시간안에 디지털 증거에 대한 확인, 분석, 해석을 제공하기 위한 현장 접근방식이다. 초기 몇시간 동안의 조사과정에서 행해지는 이러한 조사 프로세스는 피의자 심문단계와 수색집행 단계에서 활용되는 정보를 제공하기 위한 것이다. 이와 같이 비교적 짧은 시간에 정보를 확보할 필요성으로 인하여 이 모델은 당해 컴퓨터 시스템에 대한 현장분석을 수반한다. 따라서 이 모델은 즉시 활용가능한 증거를 발견하고, 극히 위험한 상태의 피해를 확인하고, 지속적인 조사를 가이드하고, 기소 가능성을 확인하고, 사회에 대한 범죄자의 위험을 정확히 평가하는 것에 초점을 맞추고 있다.

CFFTPM은 2002년 IDIP 모델, 2006년 DCSA 모델로부터 파생된 단계를 활용하고

---

60) Venansius Baryamureeba/Florence Tushabe, op.cit., p.7.
61) https://www.dfrws.org/sites/default/files/session-files/pres-the_enhanced_digital_investigation_process_model.pdf; 2016.5.20.
62) ibid.

있는데, 계획, 분류, 사용자 프로파일/이용행태, 연대순/시간대, 인터넷 활동, 구체적 이 사건 증거가 그것이다.



[그림 7] CFFTPM Phase[63]

즉 이 모델은 전통적인 조사와 실험실에서의 분석단계 이전에 적용되는 것이기 때문에 모든 조사 상황에 적절한 것은 아니지만, 원본증거의 오염을 최소화하고, 디지털 증거의 무결성을 유지하며, 증거의 Chain of Custody를 유지하며, 연방과 주 차원에서의 허용가능성에 대한 증거법칙을 준수하는 포렌식의 기본원칙들을 고수한다고 설명하고 있다.[64]

이 모델 역시 계획단계로 시작하는데, 이는 조사를 시작하기 이전의 적절한 계획이 조사의 성공률을 확실히 개선할 수 있다고 설명한다. 다음으로 분류단계에서는 중요성 또는 우선순위의 면에서 증거를 확인하고 순서를 매기는 것인데, 이는 가장 중요한 증거와 취약한 증거가 우선하여 처리될 필요가 있기 때문이다.[65] 다음으로 이용자

63) http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.169.1878&rep=rep1&type=pdf; 2016.5.20.
64) http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.169.1878&rep=rep1&type=pdf: 2016.5.20.
65) http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.169.1878&rep=rep1&type=pdf; p.26. 2016.5.20.

프로파일/이용행태 단계는 용의자와 관련한 증거를 목표로 이용자 활동과 프로파일을 분석하는데 초점을 맞추며,[66] 이러한 이용자 프로파일은 대략적으로 이용자 고유계정과 배타적으로 결합되어 있는 파일, 폴더, 레지스트리 키, 파일 속성을 수집한 것이다. 그리고 범죄활동을 순서대로 하기 위해 MAC 타임을 작성함으로써 연대기적 관점에서 범죄를 구축하는 것이 Chronology/Timeline 단계이다. 연대기를 통해 사건을 밝힘에 있어서는 정보의 출처를 밝힐 필요가 있으며, 물리적 증거의 일부에 의해 판단된 절대적 시간에 기반한 사건들과 연관성을 보여줄 필요가 있다.

인터넷 단계에서는 인터넷 관련 서비스의 가공물을 조사하는 임무가 수행된다. 이 단계에서 포렌식 조사관은 용의자(또는 피해자)가 관련되어 있다고 생각하는 인터넷 활동의 유형을 평가하고, 그러한 활동들이 사건과 관련되어 있는지, 관련되어 있다면 어떻게 관련되어 있는지를 평가하는 것이 효율적이다.[67] 마지막으로 Case Specific Evidence 단계에서는 조사관들이 사건의 특성에 대한 조사의 초점을 조정하는데, 이는 사건에 따라 요구되는 능력·시간·지식 등에 있어서 서로 다를 수 있기 때문이다.

이 모델의 핵심은 일정한 조사는 극단적으로 시간에 민감하다는 것이며, 디지털 증거는 핵심적인 정보의 최우선적인 출처이며, 처음 몇 시간 동안의 조사에 있어서 요구되는 수사상의 단서라는 것이다. CFFTPM의 가장 큰 장점은 이 분야에 있어서 대부분의 다른 모델들과 반대로 개발된 모델이라는 사실 때문에 대단히 실제적이고 실용적인 것이라는 것이다. 하지만 CFFTPM가 모든 경우에 맞는 해법은 아니기 때문에 적절한 경우에만 그리고 법적·기술적 고려사항을 조심스럽게 따져본 후에만 활용되어야 한다고 설명하고 있다.[68]

---

66) Yunus Yusoff/Roslan Ismail/Zainuddin Hassan, "Common Phsases of Computer Forensics Investigation Models", International Journal of Computer Science & Information Technology, Vol.3., no.3., 2011, p.22.

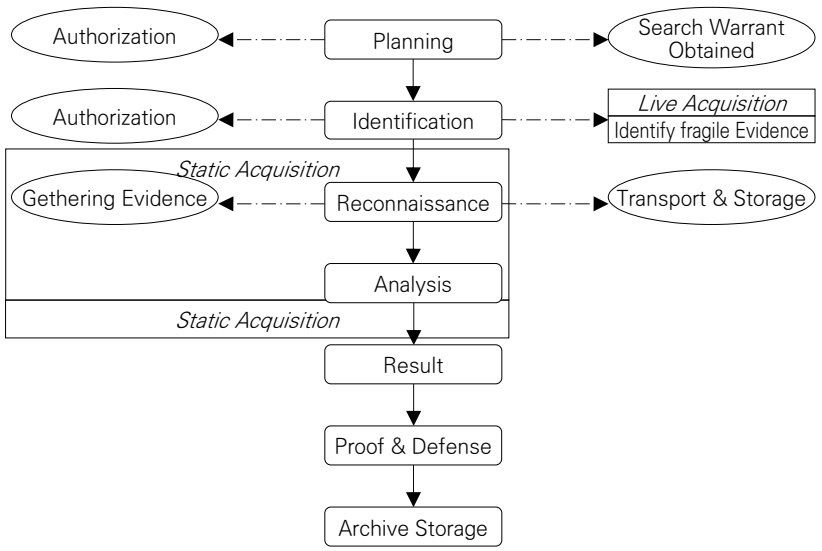
67) http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.169.1878&rep=rep1&type=pdf; p.30. 2016.5.20.

68) http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.169.1878&rep=rep1&type=pdf; pp.35-36. 2016.5.20.

8) Digital Forensic Model based on Malaysian Investigation Process (DFMMIP)(2009)

2009년에 Perumal에 의해 제안된 또 다른 디지털 포렌식 조사 모델로서 말레이시아 수사절차에 기반을 두고 있다. 말레이시아에 있어서 컴퓨터 포렌식은 새로운 규정이기 때문에 법원이나 산업분야에 있어서 디지털 포렌식에 관한 일관성이나 표준화가 거의 존재하지 않는다. 즉 말레이시아에서 디지털 포렌식은 여전히 공식적인 과학분야로서 인정되고 있지 못하기 때문에, 이 모델은 말레지아 컴퓨터 형사사법에 있어서 디지털 포렌식 조사를 행하는 방식을 향상시키고 안전하게 하기 위한 모델을 보여주는데 목적이 있다고 저자는 설명하고 있다.[69]

저자는 기존의 모델들이 주로 디지털 증거의 처리에만 초점을 맞추고 있으며, Chain of Custody와 같은 문제에 초점을 맞춘 정보 처리 플로우를 보여주지 못하고 있다고 비판하면서, 따라서 기존의 모델들이 사이버범죄 수사에 활용하기에 충분할 정도로 안정적이지 못하다는 점을 지적하고 있다. 따라서 저자가 제안한 모델은 7단계로 구성되어 있는데 이를 그림으로 제시하면 다음과 같다.



[그림 8] DFMMIP Model[70]

69) Sundresan Perumal, "Digital Forensic Model Based On Malaysian Investigation Process", International Journal of Computer Science and Network Security, Vol.9, No.8, 2009, p.40.

제1단계는 계획단계로 하위 2단계로 구성되는데 권한확보와 수색영장 확보가 그것이며, 이는 모든 사이버범죄수사에 있어서 필수적인 단계이다. 다음단계는 확인단계로 하위 2단계로 구성되는데 압수된 물품의 확인과 취약한 증거의 확인이 그것이다. 세 번째 단계는 식별단계인데, 여기서 식별은 정보를 얻기 위해 행해지는 탐색을 의미한다. 이 단계는 라이브 포렌식을 수행하는 것과 유사한 것으로 매체가 작동중인 동안에 조사를 수행하는 방식을 다룬다. 저자는 취약한 증거에 초점을 맞춘 라이브 데이터 획득의 제시는 긍정적인 기소가능성을 높인다고 주장하며, 따라서 데이터를 분석하기 전에 조사 장소로 안전하게 이전해야 하고 적절히 저장되어야 한다고 설명하고 있다[71]. 따라서 식별단계의 하위단계는 증거수집과 이전 및 저장으로 구성되어 있다. 네 번째 분석단계에서 요청되는 것은 적절한 도구와 기술을 활용하여 데이터를 분석하고 검토하는 것이다. 다음으로 입증과 방어의 단계는 이전 모델들의 제출단계와 유사한 것으로 조사관들은 제출된 사건을 뒷받침할 증거를 제시할 것을 요구받게 된다.

이 단계에서 분석관은 자신의 결과물로서 사건의 유효성을 입증해야만 하며, 만약 성공적이지 못할 경우에는 포렌식 분석관은 전체 분석절차를 역행해야만 한다.[72] 마지막으로 정보저장단계에서는 관련증거가 차후의 참고를 위해 적절히 저장되며 훈련목적으로 사용될 수도 있다. 데이터 마이닝으로 알려진 이러한 개념을 적용함으로써, 그 사건이 다른 조사와 관련이 있는 경우에 다른 국가의 분석관이나 기관에게 이익이 될 수 있을 뿐만 아니라 유죄판결을 받은 피고인이 재심을 청구하는 사건들에 있어서도 활용되어질 수 있다고 기술하고 있다.

---

70) Sundresan Perumal, "Digital Forensic Model Based On Malaysian Investigation Process", International Journal of Computer Science and Network Security, Vol.9, No.8, 2009, p.42.

71) Yunus Yusoff/Roslan Ismail/Zainuddin Hassan, "Common Phsases of Computer Forensics Investigation Models", International Journal of Computer Science & Information Technology, Vol.3., no.3., 2011, p.23.

72) Sundresan Perumal, "Digital Forensic Model Based On Malaysian Investigation Process", International Journal of Computer Science and Network Security, Vol.9, No.8, 2009, p.42.

9) Systematic Digital Forensic Investigation Model(2011)

이 모델의 저자는 디지털 포렌식 과학이 수행되는 방식은 ⅰ) 의도했던 목표에 대하여 발생하는 차후의 악의적인 사건들의 예방 ⅱ) 범죄로 이어졌던 발생한 사건을 성공적으로 추적하고, 관련된 범죄자를 알아내는 것, ⅲ) 범죄자를 재판에 회부하는 것, ⅳ) 그러한 사건이 다시 일어나는 것을 방지하기 위해 준비된 현행 예방 매카니즘의 개선, ⅴ) 각자의 기업 네트워크를 보호하기 위해 기업의 보안전문가에 의해 사용되는 표준을 개선하는 것, ⅵ) 이러한 디지털 환경에 접속한 모든 사람들이 현재의 취약점들과 예방수단에 대한 인식을 높일 수 있는 방법 등에 직접적인 영향을 미친다[73]고 전제하고 있다. 따라서 모든 디지털 포렌식 조사에서 사용되는 표준적인 방법론에 대한 필요성이 존재한다고 기술하고 있다. 그리고 현재 과학 공동체내에서 행해진 대다수의 연구들이 실행가능한 good model을 제시하고 있지만, 대부분이 당면한 문제에 한해서 적용되는 것이고 보다 더 완성될 필요가 있는 것들이라고 기술하고 있다.

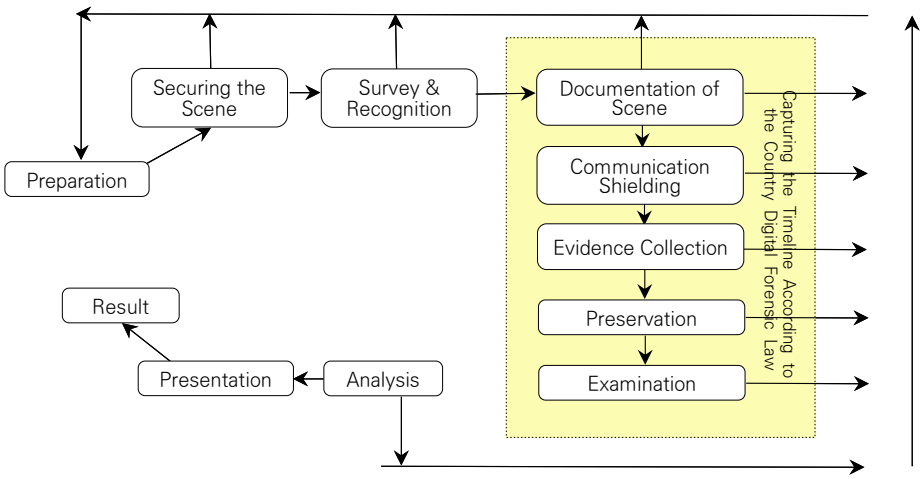
저자는 이 모델이 포렌식 실무자와 관련 기관들이 적절한 전략이나 절차를 고안하는데 도움을 줄 수 있는 체계적인 모델을 제시하고자 한 것이라고 기술하고 있다. 즉 이 모델은 특히 사이버범죄와 사이버사기의 수사에 초점[74]을 맞추어 각기 서로 다른 11단계의 절차를 개발하였다. 따라서 이 모델은 사이버 사기와 사이버 범죄에 제한되어 적용된다.

저자가 제안한 모델을 그림으로 보면 다음과 같다.

---

73) Ankit Agarwal/Megha Gupta/Saurabh Gupta/Subhash Chandra Gupta, "Systematic Digital Forensic Investigation Model", International Journal of Computer Science and Security, Vol.5, Issue1, 2011, p. 122.

74) Ankit Agarwal/Megha Gupta/Saurabh Gupta/Subhash Chandra Gupta, "Systematic Digital Forensic Investigation Model", International Journal of Computer Science and Security, Vol.5, Issue1, 2011, p. 129.



[그림 9] SRDFIM 모델[75]

제1단계는 준비단계로 실제 조사가 행해지기 이전단계로, 이 단계에서는 범죄와 관련한 정황들에 대한 완전한 평가를 확보하는 것이 중요하며, 이와 함께 다양한 법률상의 제한과 관할권 문제, 피의자의 프라이버시 권리에 대한 고려가 행해져야 한다고 기술하고 있다. 이와 같이 철저한 준비단계는 증거의 품질을 향상시키고 조사와 관련한 위험과 위협을 최소화할 수 있다는 것이다.[76]

제2단계는 현장확보(Securing the Scene)로, 이 단계는 우선 권한 없는 접근으로부터 범죄현장을 확보하고 증거가 오염되지 않도록 보존하는 문제를 다룬다. 따라서 이 단계에서는 chain of custody가 적절히 수행될 수 있도록 범죄현장 취급에 관한 공식적인 프로토콜이 있어야만 한다. 즉, 이 단계의 목표는 현장에서 모든 사람의 안전을 확보하고 모든 증거의 무결성을 보호하는데 있기 때문에 영국 하이테크범죄대책단(National Hi-Tech Crime Unit)의 가이드라인과 함께 ACPO(Association of Chief Police Officers)를 준수해야 한다고 기술하고 있다.[77]

---

75) Ankit Agarwal/Megha Gupta/Saurabh Gupta/Subhash Chandra Gupta, "Systematic Digital Forensic Investigation Model", International Journal of Computer Science and Security, Vol.5, Issue1, 2011, p. 124.

76) Ankit Agarwal/Megha Gupta/Saurabh Gupta/Subhash Chandra Gupta, "Systematic Digital Forensic Investigation Model", International Journal of Computer Science and Security, Vol.5, Issue1, 2011, p. 124.

77) Ankit Agarwal/Megha Gupta/Saurabh Gupta/Subhash Chandra Gupta, "Systematic Digital Forensic Investigation Model", International Journal of Computer Science

제3단계는 조사와 인지(Survery and Recognition)로, 현장평가, 증거의 잠재적 출처 확인, 적절한 수색계획 확립 등이 행해진다. 조사환경이 복잡한 경우에는 이러한 것들이 확실히 행해지지 않을 수 있지만 현장평가를 통해 전문가의 지원여부를 결정하고, 현장에 있는 다양한 사람들로부터 최대한의 정보 - 보안시스템, 다양한 어플리케이션, 패스워드, 사용자 이름, 암호에 관한 사항 등 -를 확보해야 한다고 기술하고 있다. 증거의 수집 및 분석을 위한 초기 계획은 이 단계가 마무리되는 시점에서 개발되어야 한다고 본다.[78]

제4단계는 현장기록(Documenting the Scene)으로, 이 단계에서는 사진, 스케치, 범죄현장 지도와 함께 범죄현장을 적절하게 기록해야 한다고 기술하고 있다. 그리고 장치가 작동중인 경우에는 스크린에 나타난 것을 기록해야 하고, 볼 수 있는 모든 데이터에 대한 기록이 만들어져야 한다고 되어 있다. 이러한 현장기록은 언제든지 현장을 재구성하고 재검토하는데 도움을 될 뿐만 아니라 포렌식 전문가가 법정에서 증언을 해야 할 때 특히 중요하다고 볼 수 있다. 이러한 기록은 조사의 모든 단계에서 요구되고, 그리고 적절한 chain of custody를 유지하기 위해 요구되는 지속적인 loopback 활동이라 할 수 있다.[79]

제5단계는 통신차단(Communication Shielding)으로, 증거수집 이전에 이루어지는 단계로서 디지털 장치의 모든 가능한 통신옵션을 차단해야만 한다. 이는 기존의 정보를 덮어쓸 수 있기 때문에 그러한 가능성을 피해야만 한다.[80]

제6단계는 증거수집(Evidence Collection)으로 가장 중요한 단계이며, 이를 위해서는 적절한 절차 또는 가이드라인이 요구된다고 본다. 증거수집단계는 휘발성 증거수집과 비휘발성 수집으로 나누어서 고려되어야 한다. 모바일 장치와 관련한 증거의 대부분이 휘발성 증거이며, 비휘발성 증거는 외부적인 저장장치로부터 수집되는 증거

---

and Security, Vol.5, Issue1, 2011, pp. 124-125.

78) Ankit Agarwal/Megha Gupta/Saurabh Gupta/Subhash Chandra Gupta, "Systematic Digital Forensic Investigation Model", International Journal of Computer Science and Security, Vol.5, Issue1, 2011, p. 125.

79) Ankit Agarwal/Megha Gupta/Saurabh Gupta/Subhash Chandra Gupta, "Systematic Digital Forensic Investigation Model", International Journal of Computer Science and Security, Vol.5, Issue1, 2011, p. 125.

80) Ankit Agarwal/Megha Gupta/Saurabh Gupta/Subhash Chandra Gupta, "Systematic Digital Forensic Investigation Model", International Journal of Computer Science and Security, Vol.5, Issue1, 2011, p. 125.

와 관련이 된다.[81]

제7단계는 보존(Preservation)으로 포장·이전·저장을 포함하는데, 수집된 증거가 변경되거나 파괴되지 않도록 적절한 절차를 따라야 한다. 이와 같이 적절한 Chain of Custody를 유지하기 위해 National Institute of Standards and Technology 가이드라인이 적절한 이송과 저장절차의 필요성을 강조하고 있다.[82]

제8단계는 조사(Examination) 단계로, 포렌식 전문가에 의해 수집된 증거의 내용을 조사하여 정보를 추출하는 것이다. 이 단계의 목적은 증거의 원본성과 중요성을 설명하면서 그 증거를 가독적인 상태로 만드는데 있다. 이 단계에서는 조사관에 의해 사용되는 포렌식 도구의 능력이 중요한 역할을 담당하며, 포렌식 전문가에 의해 처리된 후 증거가 변경되지 않았다는 것을 입증하도록 요구받는 경우에는 데이터의 진정성을 수학적으로 입증하기 위해 MD5와 같은 해쉬값이 활용되어야 한다.

제9단계는 분석(Analysis)으로, 증거의 조사결과를 토대로 조사팀에 의한 기술적 검토가 행해지는 단계로서 NIJ 가이드라인은 시간대 분석, 숨겨진 데이터 분석, 추출된 데이터에 대한 파일분석 등을 제안하고 있다. 분석결과는 완벽하고 정확하게 기록되어야 한다.

제10단계는 제출(Presentation)로, 수집된 증거를 추출하고 분석한 후 그 결과가 경찰관, 기술 전문가, 법률 전문가, 기업의 관리자 등 다양한 사람들에게 제출될 수 있다. 이 단계에서 포렌식 전문가는 법정에 전문가 증언을 제공할 수 있으며, 여러 단계의 조사절차와 관련한 복잡한 용어들이 비전문가의 수준에서 설명될 필요가 있다. 그리고 포렌식 조사관의 능력과 지식·채택된 방법론·사용된 도구와 기법 등은 모두 배심원 앞에서 이의가 제기될 수 있기 때문에, 보고서와 함께 디지털 증거의 복사본·chain of custody 기록·다양한 항목의 증거에 관한 출력물과 같은 뒷받침자료들이 제출되어야 한다.[83]

---

81) Ankit Agarwal/Megha Gupta/Saurabh Gupta/Subhash Chandra Gupta, "Systematic Digital Forensic Investigation Model", International Journal of Computer Science and Security, Vol.5, Issue1, 2011, p. 126.

82) Ankit Agarwal/Megha Gupta/Saurabh Gupta/Subhash Chandra Gupta, "Systematic Digital Forensic Investigation Model", International Journal of Computer Science and Security, Vol.5, Issue1, 2011, p. 126면.

83) Ankit Agarwal/Megha Gupta/Saurabh Gupta/Subhash Chandra Gupta, "Systematic Digital Forensic Investigation Model", International Journal of Computer Science

마지막 단계는 결과와 검토(Result&Review)로, 조사의 모든 단계를 검토하고 개선 분야를 확인하는 것이다. 검토단계의 일부로서 결과와 그 결과에 대한 해석은 앞으로의 조사에 있어서 증거의 수집, 조사, 분석을 보다 개선하는데 활용될 수 있다.[84]

이 모델이 다른 모델들과의 차이를 나타내는 것은 통신차단과 증거수집의 구분(휘발성, 비휘발성)을 두고 있다는 것이며, 특히 컴퓨터 사기와 사이버범죄의 분석에 있어서 품질과 표준·확장성·시험가능성·신뢰성·반복성의 특성을 실현함으로써 사건의 재구성과 증거의 역학관계에 도움을 줄 수 있을 것이라고 결론짓고 있다. 그리고 급속히 변화하며 고도의 휘발성을 지닌 디지털 기술에 관한 시나리오의 요구에 부응할 수 있는 일반화된 솔루션을 개발하는데도 도움이 될 것이라고 기술하고 있다.[85]

10) Harmonized Digital Forensic Investigation Process Model(2012, 2014)

Valjarevic와 Venter가 제안한 모델로, 기존 모델들을 조화시키는데 목적을 두고 있으며, 서로 다른 유형의 디지털 증거와 디지털 포렌식 조사에 활용하기에 충분한 포괄적인 모델을 제안하고자 한 것이라고 기술하고 있다.[86] 각 단계를 기존 모델과 다르게 배치하고 포렌식 원리의 실행에 평행작용이라는 개념을 제시하고 있다. 즉 각 단계가 병행하는 6개의 조치를 제시하고 있는데, 이러한 병행적 조치들은 디지털 증거의 허용가능성과 최고의 효율성을 가진 조사를 확보하는데 목적을 두고 있다고 되어 있다.

이 모델은 사건탐지→초기대응→계획→준비→사건현장 기록→잠재적 증거의 확인→잠재적 증거의 수집→잠재적 증거의 이동→잠재적 증거의 저장→잠재적 증거의 분석→발표→결론의 12단계로 구성되어 있다.

---

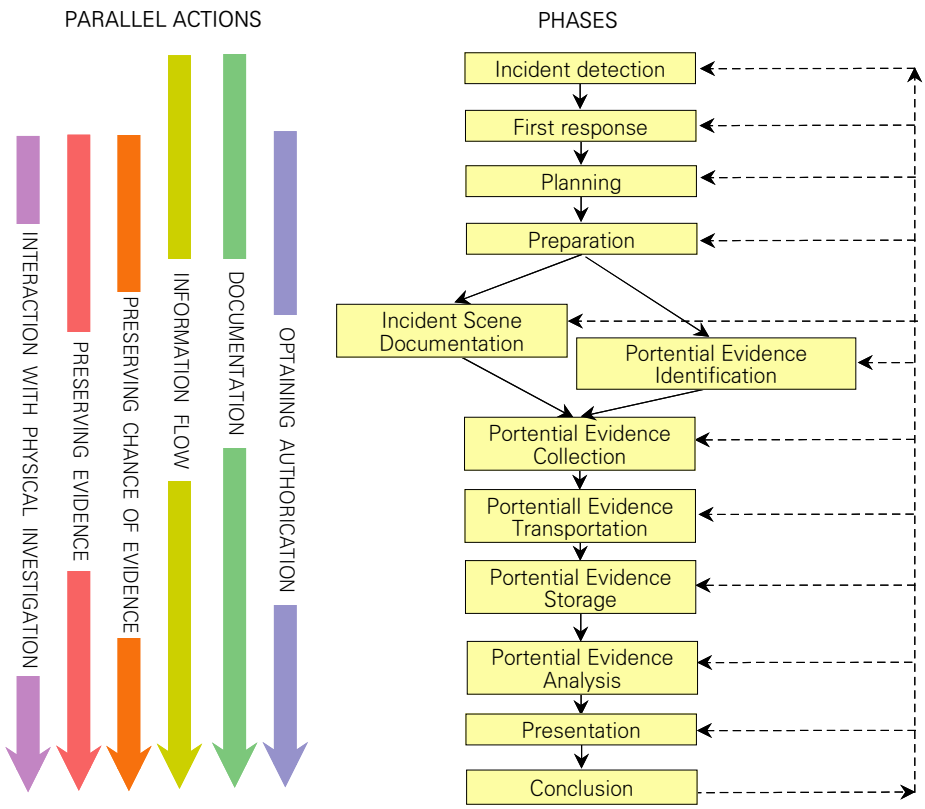
and Security, Vol.5, Issue1, 2011, p. 127.

84) Ankit Agarwal/Megha Gupta/Saurabh Gupta/Subhash Chandra Gupta, "Systematic Digital Forensic Investigation Model", International Journal of Computer Science and Security, Vol.5, Issue1, 2011, p. 127.

85) Ankit Agarwal/Megha Gupta/Saurabh Gupta/Subhash Chandra Gupta, "Systematic Digital Forensic Investigation Model", International Journal of Computer Science and Security, Vol.5, Issue1, 2011, p. 130.

86) Aleksandar Valjarevic/Hein S. Venter, "Harmonised Digital Forensic Investigation Process Model", IFIP Advances in Information and Communication Technology, Vol.410, 2012; https://pdfs.semanticscholar.org/bde1/bf7c149434639a938dd04b6883208d6c51ef.pdf.

이 모델을 그림으로 보면 다음과 같다.



[그림 10] HDFIP 모델[87]

제1단계는 사고탐지 단계(Incident Detection Phase)로, 사고탐지 뿐만 아니라 나머지 절차에 중요한 영향력을 갖는 사고의 유형과 설명을 포함한다. 여기서 중요한 것은 사고 유형과 설명은 사고탐지 이전에 수집된 정보를 토대로 수행되어야만 하며, 그것이 목표시스템에서 데이터를 변경할 수 있는 어떠한 조치도 포함해서는 안된다는 것이다. 다른 모델들이 준비단계를 포렌식 조사프로세스의 시작단계로 하고 있는데 반해 이 모델은 사고탐지단계를 시작단계로 하고 있는 이유는 디지털 포렌식 실무자들이 자신들이 작업하게 될 각각의 시스템이 디지털 포렌식 준비활동을 실행할 수

87) Aleksandar Valjarevic/Hein S. Venter, op.cit.,p.8.

있을지 확신할 수 없기 때문이라고 설명하고 있다.[88]

제2단계는 첫 번째 대응단계(First Response Phase)로, 탐지된 사고에 대한 첫 번째 대응을 포함해야 하는데, 이러한 첫 번째 대응은 디지털 포렌식을 수행할 가능성에 부정적 영향 - 장치의 전원을 끄거나 파일을 열어보거나 변경하는 것 등 -을 미치지 않는 것이 바람직하다고 기술하고 있다.[89]

제3단계는 계획단계(Planning Phase)로, 이 단계의 과정에서 누군가는 나중에 디지털 포렌식 조사 프로세스에서 필요한 모든 계획들을 이행해야만 한다고 기술하고 있다. 그리고 계획에는 관련 절차의 개발, 활용할 도구와 방법에 대한 정의, 적절한 인적자원의 활용계획, 다른 단계에서의 모든 활동들에 대한 계획 등이 포함되어야 한다고 되어 있다.[90] 저자가 제시한 모델은 두가지 프로세스 간의 인터페이스를 정의할 필요성을 강조하는 것이기 때문에, 다른 단계의 효율성과 성공을 결정하는 계획단계가 대단히 중요하다고 기술되어 있다.[91]

제4단계는 준비단계(Preparation Phase)로, 다른 디지털 포렌식 조사 프로세스 단계의 활동들을 수행하기 위한 조직을 준비하고자 하는 것이기 때문에 관련 장비의 준비(하드웨어와 소프트웨어)·기반시설·인적자원·인식제고·훈련과 기록 등을 포함한다.[92]

제5단계는 사고현장기록(Incident Scene Documentation)으로, 사고현장에서 행해진 조치에 대한 서면기록·스케치·사진·비디오·잠재적 증거의 라벨링 등을 포함한다. 즉 디지털 포렌식 조사 프로세스와 관련하여 수행된 모든 조치들은 사고가 발생한 정보시스템의 구조와 구성요소에 대한 구체적인 사항과 함께 모두 기록되어야만 한다고 되어 있다.[93]

제6단계는 잠재적 증거확인 단계(Potential Evidence Identification Phase)로, 이는 사고현장에서 수행되는 두 번째 단계인데, 현장에서 이와 같이 잠재적 증거를 확인하는 것은 만약 이 시점에서 증거가 확인되지 않으면 나중에는 그것이 존재하지 않을

88) Aleksandar Valjarevic/Hein S. Venter, op.cit.,p.4.
89) ibid.
90) Aleksandar Valjarevic/Hein S. Venter, op.cit., p.4.
91) ibid.
92) Aleksandar Valjarevic/Hein S. Venter, op.cit., p.5.
93) ibid.

수도 있기 때문에 나머지 프로세스에서 결정적인 중요성을 갖고 있다고 설명한다.[94]

제7단계는 잠재적인 증거수집 단계(Potential Evidence Collection Phase)로, 이 단계에서는 일단 증거로 확인되면 무결성을 보존하는 방식으로 수집되어야만 하고, 엄격한 법률상의 규정들을 준수하는 것이 나중에 법정에서 공식적인 결론을 이끌어내는데 중요한 역할을 한다고 기술하고 있다.[95]

제8단계는 잠재적인 증거이전 단계(Potential Evidence Transportation Phase)로, 저장과 차후 분석을 위한 장소로 이전하는 것을 말한다. 이전은 물리적으로 행해질 수도 있고, 전자적으로 행해질 수도 있는데, 전자적으로 이전되는 경우에는 증거의 연결과 무결성을 보존하기 위한 특별한 조치가 취해져야만 한다고 지적하고 있다.[96]

제9단계는 잠재적 증거저장 단계(Potential Evidence Storage Phase)로, 바로 분석이 수행될 수 없거나 일정기간 디지털 증거를 보관하도록 하는 법률상 요건이 존재하는 경우에 필요한 단계로서, 이 단계에서는 증거의 무결성에 대한 보존과 chain of custody가 가장 중요하며, 디지털 증거를 포함하고 있는 매체에 손상이 가해지지 않도록 주의조치가 취해져야 한다고 지적하고 있다.[97]

제10단계는 잠재적 증거분석 단계(Potential Evidence Analysis Phase)로, 이 단계에서는 사고가 어떻게 발생했고 그것의 정확한 특징은 무엇이며, 누가 책임을 지는지에 대한 가설을 만들기 위해서 디지털 증거를 확인하고, 필요한 증거를 재구성하고, 그것을 해석할 수많은 기술의 활용이 수반된다.[98]

제11단계는 제출단계(Presentation Phase)로, 서면 보고서·멀티미디어의 제출, 전문가 증인의 증언의 형식으로 행해질 수 있는데, 만약 가설에 대한 이의가 제기되는 경우에는 가설의 유효성을 입증하는 내용이 포함되어야 하고, 그 가설을 제시한 사람이 준비해야만 한다고 기술하고 있다.[99]

마지막 제12단계는 결론단계(Conclusion Phase)로, 이 모델은 반복적인 성격을 갖기 때문에 이 단계를 완료한 후에 다시 이전단계로 되돌아갈 수도 있다고 설명한다.

---

94) ibid.
95) ibid.
96) Aleksandar Valjarevic/Hein S. Venter, op.cit., p.5.
97) Aleksandar Valjarevic/Hein S. Venter, op.cit., p.6.
98) ibid.
99) ibid.

그리고 결론단계에서는 가설의 승인 또는 거부, 증거의 반환, 증거의 파기, 모든 이해관계자에 대한 관련정보의 배포 등의 조치가 포함되어야 한다고 기술하고 있다.[100]

이 모델은 앞서 기술한 12단계와 함께 병행적으로 취해져야 하는 조치(Parallel Actions)를 두고 있는데, 물리적 조사와 상호작용(Interaction with the physical investigation), 증거의 연계성 보존(Preserving the chain of evidence), 증거의 보존(Preserving evidence), 정보의 흐름(Information flow), 기록(Documentation), 권한확보(obtaining authorisation)가 그것이다. 이러한 병행적 조치는 보다 높은 조사의 효율성과 디지털 증거의 허용가능성을 확보하는 것이라고 설명하고 있다.[101]

저자는 이 모델이 갖는 장점으로 첫째, 표준화된 절차를 활용했다는 사실로 인하여 법정에서 디지털 증거의 허용가능성을 보다 높일 수 있다는 것이며, 둘째, 이와 같이 조화된 프로세스를 채용하게 되면 디지털 포렌식 조사 프로세스에 있어서 사람에 의한 오류와 누락이 최소화될 수 있으며, 셋째, 이 모델을 활용하게 되면 사이버범죄에 보다 효율적으로 대응할 수 있고 사인과 정부기관간의 상호작용이 보다 용이하고 효율적이 될 수 있으며, 마지막으로 무엇보다도 디지털 포렌식 조사의 효율성을 향상시킬 수 있다는 점을 제시하고 있다.[102]

한편 2014년에 이 HDFIP 모델을 검증하고자 하는 연구가 2014년 Emilio Raymond Mumba 그리고 H.S. Venter에 의해 행해졌다. 이 연구는 HDFIP 모델이 디지털 포렌식 조사에 관한 국제표준(ISO/IEC 27043)이 되고자 하는 방향으로 초안을 제출함에 따라 이를 시험할 필요가 있다는 이유로 연구를 수행했고, 그 모델이 구조화되고 정확한 논리적 흐름을 유지하는지를 입증하기 위해 시험과 평가절차는 익명화된 현실사례를 활용하였다.[103]

즉, HDFIP 모델은 ISO/IEC 27035[104], 27037[105], 27040[106], 27041[107], 27042[108]

---

100) ibid.
101) Aleksandar Valjarevic/Hein S. Venter, op.cit., pp.6-7.
102) Aleksandar Valjarevic/Hein S. Venter, op.cit., p.8.
103) Emilio Raymond Mumba/H.S.Venter, "Testing and Evaluating the Harmonized Digital Forensic Investigation Process in Post Mortem Digital Investigation", ADFSL Conference on Digital Forensics, Security and Law, 2014, p. 83.
104) Part 1:사고탐지 관리에 관한 원칙, Part 2: 사고대응 계획과 준비에 관한 가이드라인, Part 3: 사고대응활동에 관한 가이드라인
105) 디지털 증거의 확인, 수집, 획득, 보존에 관한 가이드라인 제공

표준을 모두 고려한 것으로, 이는 HDFIP 모델이 조사과정에서 추출된 잠재적인 증거의 무결성을 유지하도록 하고자 한 것이며, 따라서 이 표준들은 디지털 조사과정에서 조사관들이 HDFIP 모델안에 정의된 각각의 하위 프로세스를 활용하도록 가이드라인을 제공한다고 설명되어 있다.[109] 이러한 HDFIP 모델의 효과성에 대하여 테스트 절차와 평가절차를 하는 과정에서, 저자는 HDFIP 모델이 조사관들로 하여금 반복적인 구조의 조사 프로세스를 통해서 행해지는 모든 조치를 해명할 수 있게끔 하기 때문에 효율적인 것으로 판단되었다고 기술하고 있다.[110] 즉 HDFIP모델이 제시하는 병행적인 프로세스는 조사의 과정에서 행해지는 각각의 단계들이 기록되고, 각각의 상호작용이 포렌식적으로 유효한 조사를 행하는 것에 대한 규칙과 규범들을 명확하게 준수함으로써 설명되어진다는 것을 보장할 뿐만 아니라, 무결성·신뢰성·유효성과 같은 디지털 포렌식 과정에서 중요한 특성들을 성공적으로 유지하고 있다는 의견을 제시했다. 다만 HDFIP 모델은 표준초안이기 때문에 앞으로 국제적으로 채택되어 디지털 조사의 결과를 비교 대조하는 것을 용이하게 하고, 더 나아가 서로 다른 관할권에 있는 서로 다른 조사관이나 기관들에 의해 수행되기를 바란다고 결론짓고 있다.[111]

11) Integrated Digital Forensic Process Model

이 모델은 기존의 모델들을 통합하고 용어를 정제하여 모두 통합하는 표준화된 디지털 포렌식 절차모델을 제시하고자 한 것이었다.[112] 이 모델은 기록(Documentation)을 가장 중요한 것으로 보고 있으며, 따라서 전체 프로세스에 걸쳐서 지속되어야 하는 것으로 보고 있다. 즉 기록의 주요한 목적은 많은 경우에 있어서 사건이 일어나고 오랜 뒤에 최종적인 디지털 증거를 허용하기 위해 활용된 절차와 조사 기법이 무엇인가에 대해 최종적으로 증언을 해야할 조사관들에게 조사의 기록으로서 역할을 하기 때문이라고 설명하고 있다.[113] 따라서 기록은 최소한 다른 조사관에 의해 동일한

106) 저장장치보안에 관한 세부방안 제공
107) 디지털 증거 조사방법의 확보에 관한 가이드라인 제공
108) 디지털 증거의 분석과 해석에 관한 가이드라인 제공
109) Emilio Raymond Mumba/H.S.Venter, "Testing and Evaluating the Harmonized Digital Forensic Investigation Process in Post Mortem Digital Investigation", ADFSL Conference on Digital Forensics, Security and Law, 2014, p.88.
110) Emilio Raymond Mumba/H.S.Venter, op.cit., p.94.
111) Emilio Raymond Mumba/H.S.Venter, op.cit., p.95
112) Michael Donovan Kohn, Integrated Digital Forensic Process Model, 2012, p.76

결론에 이르게 할 수 있을 정도의 조사관의 기록을 포함해야 하고, 따라서 조사관들은 chain of custody와 chain of evidence가 충분히 그리고 정확히 기록되도록 해야만 한다.[114] 그리고 이러한 기록은 궁극적으로 법원에 제출된 디지털 증거의 기초를 형성하는 것이기 때문에 조사과정중에 사용된 방법과 기술, 기록된 디지털 증거, 증거의 연계성 및 보관의 연계성, 조사관의 전문가 증언 등이 보고서 안에 포함되어야 한다고 기술하고 있다.[115]

이 모델의 첫 번째 단계는 준비단계(Preparation)로, 이러한 포렌식 준비는 사고현장으로 부터 신뢰할만한 디지털 증거의 수집을 최대화하고, 포렌식 사고대응비용을 최소화하는 것을 그 목적으로 한다고 설명하고 있다. 저자는 준비의 순차적 논리표기를 다음과 같이 제시하고 있다. "Prepartion= {Policy/Procedure⇒Operational Readiness ‖ Infrastructure Readiness} "[116]

다음으로 사고(Incident)는 정보시스템의 무결성, 효용성, 기밀성을 손상시키기 위해 행해지는 모든 행위가 될 수 있으며, 사고범위는 행해지는 조사의 유형에 의해 판단되어져야 할 것이라고 기술하고 있다. 사고의 순차적 위치는 다음과 같다. "Incident= {Detect⇒Assess ‖ Confirm⇒Notify⇒Authorise⇒Deploy} "[117]

사고대응(Incident Response)은 사고단계의 하위 프로세스가 완료되면 시작되는 것으로, 대응프로세스 항목은 다음과 같이 제시되어 있다. "Incident Response= {Approach Strategy⇒Search⇒Recover ‖ {Seize⇒Preserve}⇒Transport⇒Store}∧ {Preserve⇒Digital Foresic Investigation}[118]

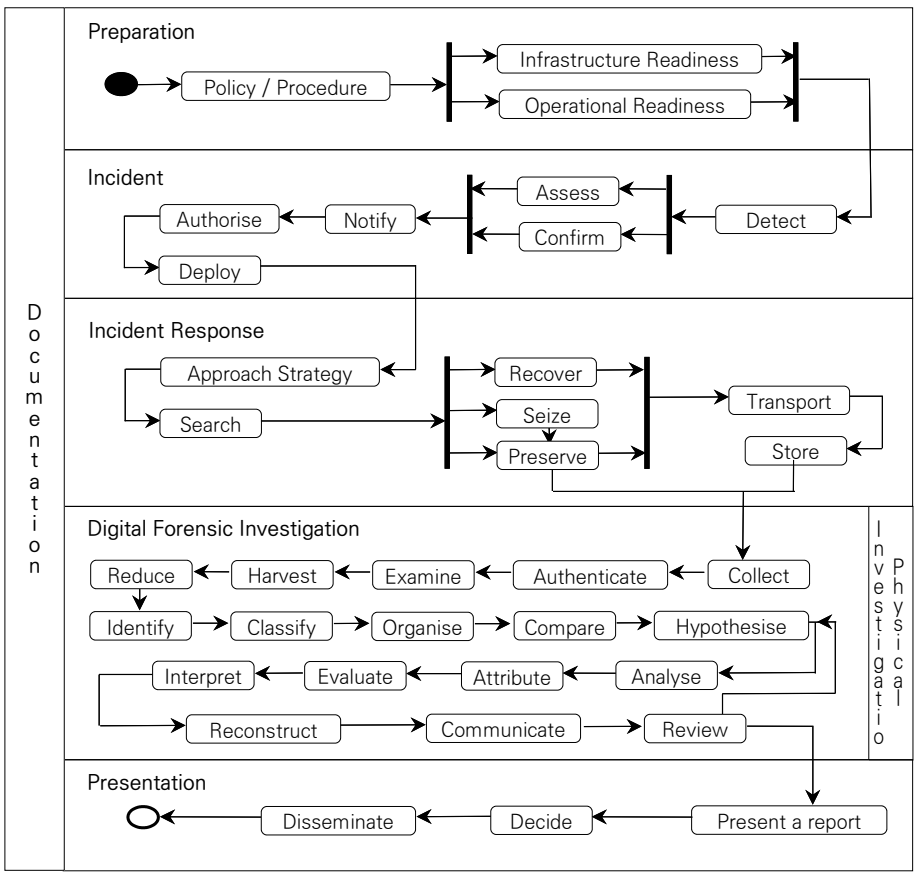
디지털 포렌식 조사(Digital Forensic Investigation)는 IDEPM의 핵심으로, 이 단계에서 열거된 항목들은 궁극적으로 법원에 제출되는 조사관의 결과의 성공여부를 판단하게 된다. 이 프로세스에서는 물리적인 조사 프로세스가 디지털 조사와 병행하여 행해지게 된다고 되어 있다. 이 단계에서 저자가 제시한 하위 프로세스 항목을 순차적으로 표기하면 다음과 같다. "Digital Forensic Investigation={Collect⇒Authenticate⇒

113) Michael Donovan Kohn, op.cit.,p.89.
114) ibid.
115) ibid.
116) Michael Donovan Kohn, op.cit., p.90.
117) Michael Donovan Kohn, op.cit., p.92.
118) Michael Donovan Kohn, op.cit., p.94.

Examine⇒Harvest⇒Reduce⇒Identify⇒Calssify⇒Organise⇒Compare⇒Hypothesise⇒Analyse⇒Attribute⇒Evaluate⇒Interpret⇒Reconstruct⇒Communicate⇒Review}∧{Reconstruct⇒Hypothesis}[119]

마지막은 제출(Presentation)인데, 제출은 가설이 조사관 이외의 다른 사람 즉 배심원 또는 관리자에게 제시될 때 행해지는데 판단은 결과물을 토대로 행해지게 된다. 이 단계의 순차적 논리표기는 다음과 같다. "Presentation={Report/Present⇒Decide⇒Disseminate}[120]

위에서 설명된 IDFPM의 순차적 논리표기를 그림으로 표시하면 다음과 같다.



[그림 11] IDFPM 모델[121]

119) Michael Donovan Kohn, op.cit., p.97.
120) Michael Donovan Kohn, op.cit., p.102.

저자는 이러한 단계별 구성요소와 함께 이 모델을 뒷받침하는 3가지 중요한 역할을 하는 것으로 법률과 원칙 그리고 경험을 제시하고 있다. 이 3가지는 제출되는 보고서가 법적인 심사를 견뎌낼 수 있는 방식으로 행해지게 되는 디지털 포렌식 조사를 위해 요구되는 것이라 할 것이다.

IDFPM에 있어서 요구되는 법률상 원칙과 표준들은 조사가 행해지는 나라에 따라 다르기 때문에 디지털 포렌식 기관의 정책과 절차를 개발함에 있어서 법률적 조언을 구해야만 한다고 기술하고 있다. 그리고 IDFPM은 특정한 원칙에 의존하고 있는데, ACPO 원칙, Best Practice, Standard Operating Procedure 등이 그것이며, 마지막으로 경험은 다양한 전문가의 경험으로이를 측정할 수 있는 기존의 기준은 없지만 찾아내기 어려운 문제를 어떻게 다룰 것인가에 대한 하나의 해법이 될 수 있다고 기술하고 있다.[122]

하지만 이 모델은 각 단계를 지나치게 세부적으로 설명함으로써 인해 복잡해졌고, 세부단계에서의 예외적 상황 발생시에 적용하기 어려운 단점을 갖고 있다는 비판을 받는다.[123]

나. 기존 디지털 포렌식 프로세스 모델의 변화 경향 분석

앞서 기술했던 디지털 포렌식 모델들은 디지털 증거가 법정에서 허용될 수 있도록 하기 위하여 단계별로 구조화된 프로세스를 제시하는 방식을 취하고 있다. 이러한 구조화된 포렌식 프로세스는 디지털 기술의 발전과 함께 복잡·다양해진 디지털 증거를 그 대상으로 함에 따라 초기의 단순한 단선적·일방향 진행 구조에서 점차 병행적·복합적·상호 반복형 진행 구조로 절차의 단계가 늘어나고 있음을 볼 수 있다. 그리고 초기에는 사법기관 또는 법집행관련 실무기관들이 포렌식 프로세스 모델을 제시한데 비해서, 최근 들어서는 학계를 중심으로 포렌식 프로세스 모델에 대한 연구들이 증가하고 있는 것으로 나타났다. 따라서 디지털 포렌식 프로세스 모델이 범죄수사를 중심으로 하는 사법분야 뿐만 아니라 일반 기업의 영역에서도 활용할 수 있는 방향으로

121) Michael Donovan Kohn,op.cit., p.86.
122) Michael Donovan Kohn, op.cit., pp.105-106
123) 김지홍, 디지털 포렌식 절차모델에 대한 새로운 접근, 서울대 석사논문, 2015, 28면.

변화되었다. 또한 초기 모델들은 디지털 조사 그 자체에만 초점을 맞추어 포렌식 프로세스를 구성하는 단계들을 제안한데 비해서, 2000년 중반 이후부터는 디지털 조사 프로세스와 물리적 조사 프로세스가 서로 조화될 수 있는 구성단계들을 제시하고자 하는 경향을 볼 수 있다.

그동안 제안되어온 디지털 포렌식 프로세스 모델들이 절차적 프레임을 제시하는 방식의 변화를 보면, 이전 모델이 제시한 결과를 분석한 후 이를 토대로 새로운 단계를 추가하거나 기존 단계를 보다 구체적으로 세분화하여 새로운 프로세스의 프레임을 제시하는 방식, 기존 모델들이 제시한 유효한 단계들을 서로 통합하거나 조화시키는 방식으로 프로세스 프레임을 제시하는 방식을 취하고 있다. 특히 최근으로 올수록 디지털 포렌식 프로세스 모델은 통합과 조화라는 개념을 사용하고 있으며, 그와 함께 절차상 표준의 준수를 중요한 기준으로 삼고 있다고 할 수 있다. 즉 표준화된 절차의 활용이 디지털 증거의 허용가능성을 높일 수 있을 뿐만 아니라 전체적인 포렌식 조사 프로세스에 있어서의 사람에 의한 오류를 최소화할 수 있다는 인식이 높아져가고 있다고 볼 수 있다.

하지만 기존의 모델들이 제시하는 단계별 절차가 많아지고 구체화될수록 디지털 포렌식 업무의 분야별 정확성과 일관성은 확보될 수 있다는 장점이 있지만, 그와 함께 절차의 반복에 따른 시간적 소모로 인한 비효율성이라는 단점도 동시에 갖고 있다고 할 수 있다.

제2장

KOREAN INSTITUTE OF CRIMINOLOGY

현행 디지털 포렌식 시스템 및 프로세스 비교

탁 희 성

제2장

현행 디지털 포렌식 시스템 및 프로세스 비교

제1절 형사사법기관별 디지털 포렌식 시스템 및 프로세스

1. 검찰의 디지털 포렌식 시스템(DFIS)

가. 디지털 포렌식 업무 현황

대검찰청은 국가 디지털 포렌식 센터를 두고 있으며, 그 안에 디지털 수사담당관실에서 디지털 포렌식 업무를 수행하고 있다. 하지만 폭증하는 디지털 증거분석 업무로 말미암아 압수수색 및 증거분석 지원을 위해 7개의 지검내에 디지털 포렌식 수사팀을 확대하여 설치·운영중에 있다.

검찰은 디지털 포렌식을 위하여 D-NET 시스템을 두고 있는데, 이는 디지털수사팀을 온라인으로 연계하여 신속한 수사지원시스템을 제공하고, 디지털 증거분석 업무의 편의성 및 증거 관리의 엄격성을 향상시키기 위한 디지털수사 네트워크[124]라고 할 수 있다. D-NET은 디지털 수사 통합업무관리시스템(DFIS II), 디지털 증거관리시스템, 통합디지털 증거분석 시스템(IDEAS), 원격디지털수사공조시스템 등으로 구성[125] 되어 있다.

먼저 DFIS II는 디지털 포렌식 프로세스를 정립하고, 각 단계별 필요한 정보를 관리하며, 디지털 포렌식 수사관이 사용하는 내부 시스템과 일선 수사팀이 사용하는 외부시스템의 연계를 통해 데이터를 확보하는 기능을 담당한다. 그리고 디지털 증거

124) 검찰, 국가 디지털 포렌식 센터 Brochure, 21면.
125) 검찰, 국가 디지털 포렌식 센터 Brochure, 20면.

관리시스템은 디지털 압수물의 생명주기 전체를 관리하고, 디지털 압수물 관련자료를 사건별로 관리함으로써 chain of custody를 확보하고 있다. 또한 사건단위로 압수한 디지털 정보에 대한 포렌식 조사관 및 수사팀의 접근권한을 설정하여 권한 없는 자의 접근 및 변경을 엄격히 차단함으로써 디지털 압수물의 안정성 및 보안을 강화하고 있다.[126] 그리고 이를 통해 디지털 압수물의 접근이력이 관리되기 때문에 압수된 디지털 정보가 시스템에 등록되는 순간부터의 이전, 변경 등의 전체적인 흐름에 대한 추적이 가능하도록 되어 있다.[127] 즉, 디지털증거관리시스템은 대검내의 디지털수사 담당관실을 중심으로 모든 디지털 압수물을 관리할 수 있도록 함으로써 디지털 증거의 관리 및 보관의 안정성과 효율성을 담보하고 있는 것이다. 통합 디지털증거분석시스템(IDEAS)는 디지털 포렌식 수사관이 수행한 분석결과를 SBC(Server Based Computing)과 GPKI(Government Public Key Infrastructure) 두 단계 인증을 거쳐 안전하게 제공할 수 있게 하며, 분석결과를 사건단위로 통합조회하거나 분석하는 것을 가능하게 한다.[128] 또한 분석요원에게 실시간 수사상황에 필요한 다양한 분석을 요청할 수 있고, 분석결과를 온라인을 통해 신속하게 전달받아 수사에 활용할 수 있도록 되어 있다.[129] 즉 검찰의 경우 디지털 포렌식 지원요청단계에서 부터 DFIS II를 통해 등록하고, 최종 분석완료된 이미지파일을 증거관리시스템을 통해 보관하는 단계까지 통합된 시스템내에서 전체적인 프로세스가 진행되도록 구성되어 있다.

검찰은 디지털 포렌식 업무와 함께 디지털 포렌식 도구의 개발 및 다른 정부기관의 디지털 포렌식 담당관에 대한 교육훈련을 지원하는 기능도 수행하고 있다. 즉 국방부, 국세청, 식품의약품안전청 등 12개 기관이 참여하는 디지털 포렌식 관련 기관 협의회를 만들어 연구 성과와 정보를 공유하고 있으며, 국가정보원, 해양경찰청 등 다른 수사기관의 디지털 증거분석 분야의 위탁 교육도 맡고 있다.

나. 디지털 포렌식 절차

검찰은 디지털 포렌식 업무의 적법성 확보를 위한 규정 및 내부 지침, 실무매뉴얼

126) 김지홍, 디지털 포렌식 절차모델에 대한 새로운 접근, 서울대 석사논문, 2015, 48면.
127) 김지홍, 앞의 논문, 49면.
128) 김지홍, 앞의 논문, 49면.
129) http://cpuu.postype.com/post/220456/; 2016.8.20.

등을 두고 있는데, 디지털 포렌식 수사관의 증거 수집 및 분석 규정(2015.7.16.개정), 디지털 포렌식 압수지원 절차에 관한 지침 (2015.7.16.개정), 전국 디지털수사망 운영 지침 개정(2015.7.16.개정), 과학수사 실무매뉴얼 등이 그것이다.

1) 디지털 포렌식 수사관의 증거수집 및 분석 규정

동 규정은 디지털 증거를 수집, 분석, 현출하는 과정에서 준수해야 할 기본적 사항을 규정한 것이며,[130] 이 과정에서 준수해야할 기본원칙으로서 압수시 부터 법정제출 시까지의 무결성 원칙과 수집·분석도구와 방법의 신뢰성 원칙을 제시하고 있다. 그리고 동 규정의 전체적인 체계는 디지털 증거의 압수·수색 전단계에서 부터 분석단계에 이르기까지 수사를 담당하는 검사와 디지털 포렌식 수사관이 준수해야 할 일련의 조치들로 이루어져 있다.

가) 압수·수색 준비단계

동 규정 제9조부터 제11조는 압수·수색을 위한 준비를 위한 규정으로, 디지털 증거에 대한 압수·수색·검증의 필요성이 인정되는 경우 수사를 담당하는 검사 등이 디지털 포렌식 수사관에게 지원요청[131]을 하도록 하고 있다. 그리고 이러한 지원요청은 디지털수사 통합업무관리시스템에 등록하도록 함으로써 준비단계에서 부터 chain of custody가 유지될 수 있도록 하고 있다.

이러한 준비단계에서 수사담당 검사 등은 정보저장매체의 무결성 확보를 위한 조치의무와 포렌식 수사관에 대한 정보제공의무를 부담하도록 하고 있다.[132]

디지털 증거에 관한 구체적인 압수지원절차와 관련하여서는 대검찰청 예규 제807호 '디지털 포렌식 압수지원절차에 관한 지침'을 마련해 두고 있다.

나) 압수·수색·검증 단계

디지털 증거의 압수·수색·검증은 원칙적으로 디지털 포렌식 수사관 또는 디지털 증거 압수·수색 실무교육을 받은 수사관이 하도록 하고 있다.[133] 즉 디지털 증거의 압수·수색 등에 요구되는 전문적인 지식과 기술을 갖춘 사람으로 하여금 해당 업무를

130) 디지털 포렌식 수사관의 증거수집 및 분석규정, 대검찰청 예규 제805호, 제1조.
131) 디지털 포렌식 수사관의 증거수집 및 분석규정, 대검찰청 예규 제805호, 제9조 제1항
132) 디지털 포렌식 수사관의 증거수집 및 분석규정, 대검찰청 예규 제805호, 제9조 제4항, 제10조.
133) 디지털 포렌식 수사관의 증거수집 및 분석규정, 대검찰청 예규 제805호, 제13조.

수행하도록 함으로써 디지털 증거의 본질적인 취약성으로 인한 증거의 훼손을 방지하고자 하는 것이다.

그리고 압수·수색 등의 절차는 국가의 공권력에 의한 강제처분으로서 기본권 침해적 행위이기 때문에 법률에 규정된 요건과 절차를 준수해야만 하며, 이를 위반한 경우에는 위법수집배제원칙에 의해 증거로서의 허용되지 않는다. 이는 디지털 증거의 압수·수색 등에 한정된 것이 아니라 모든 압수·수색에 있어서 준수되어야 할 원칙이기 때문에, 동 규정 역시 적법절차원칙을 준수해야 함을 명시하고 있다.[134]

동 규정은 디지털 증거의 압수·수색·검증의 단계와 관련하여 형사소송법 제106조 제3항에 따른 압수의 방법과 범위의 준수, 네트워크 수색방법, 압수한 디지털 증거의 무결성 입증방법, 정보저장매체 운반시 손상방지 조치의무 등을 명시하고 있다.

다) 등록 및 분석단계

디지털 증거의 분석시 압수된 디지털 증거는 복제된 이미지 파일로 디지털수사 통합업무관리시스템에 등록해야 하며, 등록된 이미지 파일로 분석하는 것이 원칙이다.[135] 따라서 원본 매체에 대한 직접분석은 예외적으로 이미지파일 복제가 불가능한 경우에 한해서만 가능하도록 규정하고 있다. 이 경우 원본 동일성에 대한 입증에 있어서 문제가 생길 수 있으므로 훼손 및 변경 방지를 위한 적절한 조치를 취하도록 하고 있다. 이와 함께 동 규정은 분석단계에서 준수해야 할 기본원칙인 신뢰성 원칙과 관련하여 장비와 프로그램의 적합성을 명시하고 있다.

분석이 종료되면 분석보고서를 작성하여 디지털수사 통합업무관리시스템에 등록해야 하고, 분석과정에서 생성된 자료는 지체 없이 폐기하도록 하고 있다. 즉 동 규정은 대검찰청의 디지털 포렌식 업무가 디지털수사 통합업무관리시스템을 통해 압수·수색 준비단계에서의 지원요청에서부터 최종 분석결과까지 일관된 프로세스내에서 관리될 수 있는 체계를 마련하고 있다고 할 것이다.

2) 과학수사 실무매뉴얼

과학수사 실무매뉴얼은 DFC내의 법과학 수사실무를 분야별로 기술하고 있는데,

---

134) 디지털 포렌식 수사관의 증거수집 및 분석규정, 대검찰청 예규 제805호, 제12조.
135) 디지털 포렌식 수사관의 증거수집 및 분석규정, 대검찰청 예규 제805호, 제22조.

디지털 포렌식 실무매뉴얼도 그 가운데 하나로 포함되어 있다.

가) 디지털 증거 취급원칙

디지털 포렌식 실무매뉴얼은 디지털 증거 취급원칙으로서 적법절차 원칙, 동일성·무결성 원칙, 신뢰성 원칙을 제시하고 있다. 적법절차 원칙은 형사소송의 기본원칙이므로 당연히 디지털 증거의 압수·수색에도 적용되는 것이라 할 것이다. 그리고 무결성 원칙에 있어서는 이미징 기술과 해시값을 통한 무결성 검증이 요구되며, 신뢰성 원칙에 있어서는 디지털 포렌식 절차의 타당성·사용한 도구의 신뢰성·수사관의 전문성·활용된 지식과 기술의 검증가능성 등이 요구된다고 기술하고 있다.

나) 압수·수색 절차의 준비

디지털 증거에 대한 압수·수색 준비단계에서는 대상 매체나 시스템, 사용자 등 관련 정보의 수집, 영장청구시 요구되는 필요성 및 관련성 요건 입증을 위한 소명자료 준비, 디지털 포렌식 수사지원요청을 위한 디지털 포렌식 수사관과의 사전협의 및 DFIS II를 통한 지원요청 사항 등록 등이 행해져야 한다.[136]

이러한 준비절차는 전문가의 사전적 판단을 토대로 압수수색 현장에서 부딪치는 다양하고 방대한 분량의 디지털 증거에 효과적으로 대응하는데 필요한 것일 뿐만 아니라, 디지털 포렌식 절차의 시작단계에서 부터 chain of custody를 유지하여 절차의 신뢰성을 확보하는데 필요한 것이라 할 것이다.

다) 압수·수색 현장에서의 준비

압수·수색 현장에서 대상 정보저장매체 및 기기 등에 대한 압수·수색을 하기전에 디지털 증거를 훼손 없이 온전하게 확보하고 은닉 정보의 누락 위험을 배제하기 위해 취해져야할 사전조치로서, 현장 상황의 촬영, 현장 및 시스템에 대한 통제, 현장분석을 통한 압수·수색 대상 특정, 관련자의 협조, 이동식 저장매체 및 백업시스템의 확인, 디지털 증거 압수·수색을 보완할 수 있는 관련 유체물의 확보 등이 기술되어 있다.[137] 이 가운데 특히 시스템 통제와 관련하여서는 원격지 접속을 통한 데이터 삭제 등의 위험 방지를 위해 네트워크 차단 및 시스템 전원 차단여부에 대한 판단이 행해져야

136) 대검찰청, 과학수사 실무매뉴얼, 155면-163면 참조.
137) 대검찰청, 과학수사 실무매뉴얼, 164면-167면 참조.

함을 강조하고 있다.

라) 정보저장매체의 압수·수색

형사소송법 제106조 제3항의 규정에 따라 디지털 데이터에 대한 압수 방법은 원칙적으로 선별 후 복제하는 것이며, 선별복제가 불가능한 경우에 한하여 예외적으로 매체자체를 압수할 수 있다. 따라서 현장에서 사건과 관련된 데이터를 포렌식 도구를 사용하여 선별하고, 논리 이미지 파일을 생성한 후 해시값 계산 등의 무결성 담보 조치를 취해야 한다.[138] 이때 디지털 데이터에 대한 사건관련성 여부는 기술적 방법 - 파일명, 파일시간, 파일종류, 파일내용, 파일 시그니처 검색 -을 통해 확인할 수 있다.[139]

이와 같이 선별복제 압수가 불가능하거나 디지털매체에 저장된 데이터 전체에 대한 분석이 필요한 경우에는, 해당 저장매체를 컴퓨터에서 분리한 후 쓰기방지 조치후 이미지 파일 또는 복제본 디스크를 생성하도록 하고 있다.[140]

하지만 현장에서 디지털 데이터의 압수·수색이 불가능한 경우에는 형사소송법 제106조 제3항의 예외규정에 따라 저장매체 자체를 압수·수색할 수 있는데, 이 경우 디지털 증거의 동일성 및 무결성 확보를 위해 압수시간 특정후 대상 컴퓨터 전원을 차단한 후 압수대상 정보저장매체를 분리해야 한다. 저장매체/정보시스템 압수 확인서에 분리된 저장매체의 정보, 압수·수색 일시 및 장소를 기재하여 피압수자나 참여인으로부터 확인을 받은 후 봉인해야 한다.

동 매뉴얼은 이러한 컴퓨터 등 정보저장매체에 대한 압수절차 외에 네트워크에 연결된 서버시스템에 대한 압수·수색절차, 휴대폰 등 모바일 기기의 압수·수색 절차, CCTV 압수·수색 절차에 대해서도 별도로 기술하고 있다.

마) 압수 후 등록 및 피압수자의 참관

압수한 저장매체를 디지털증거분석실로 운반한 후에는 봉인을 해제하고 절차에 따라 이미지 파일을 생성하여 DFIS II에 등록해야 한다.[141] 이 경우 개봉의 전과정을

---

138) 대검찰청, 과학수사 실무매뉴얼, 168면.
139) 대검찰청, 과학수사 실무매뉴얼, 170-171면.
140) 대검찰청, 과학수사 실무매뉴얼, 173면.
141) 대검찰청, 과학수사 실무매뉴얼, 179-180면.

촬영함으로써 chain of custody를 유지해야 한다.

정보저장매체 압수 후 법원은 피압수자의 참여 하에 관련 정보의 선별압수를 요구하고 있기 때문에, 검찰은 저장매체를 분석실로 운반한 후 이미지파일 생성 및 관련 데이터 선별 출력 및 복사과정에 피압수자 참여를 보장하고 추출파일에 대한 목록을 교부하고 있다.[142)]

바) 압수 데이터의 관리 및 보관

DFIS II에 등록된 이미지 파일은 무결성 보장을 위해 정당한 권한을 가진 사람에 의한 인증절차를 거쳐야만 접근이 가능하도록 통제하고 있다. 이미지 파일은 사건담당 디지털 포렌식 수사관만 접근이 가능하고, 분석결과자료에 대해서는 지원요청을 한 검사와 수사관만 열람이 가능하도록 되어 있으며, 해당 데이터에 대한 접근 및 작업내용은 모두 시스템에 자동으로 기록된다.

디지털 포렌식 수사관이 등록된 이미지 파일에 대한 분석을 거쳐 추출한 데이터를 통합디지털증거분석시스템에 업로드하면, 수사팀은 두 번의 인증과정을 거쳐 통합디지털증거분석시스템에 접속하여 업로드한 데이터와 분석결과자료를 열람하며, 이를 출력하여 법원에 증거로 제출하게 된다.[143)]

분석이 종료된 이미지파일은 이미지 파일 보관용 저장서버에 보존되고, 보존되는 동안 접근로그를 생성·관리함으로써 권한없는 접근시 추적가능하도록 보존절차를 강화하였다.[144)]

2. 경찰의 디지털 포렌식 절차

가. 디지털 포렌식 업무 현황

경찰청 디지털 포렌식센터는 사이버테러대응센터 기술지원팀으로 시작되었다가 2010년 디지털 포렌식팀으로 변경되었으며, 2014년 사이버안전국이 출범하면서 디지털 포렌식센터로 개편되었다. 경찰청 사무분장규칙 제27조의4에 규정된 디지털

142) 대검찰청, 과학수사 실무매뉴얼, 191-193면.
143) 대검찰청, 과학수사 실무매뉴얼, 194면.
144) 대검찰청, 과학수사 실무매뉴얼, 194면.

포렌식센터의 분장업무의 내용을 보면, 디지털 포렌식 기획, 첨단기법개발, 모바일포렌식, 컴퓨터포렌식으로 구분되어 있으며, 정책기획 및 지원, IT 환경 분석 및 신규 추적기법, 도구 개발, 스마트폰 등 모바일기기 분석기법 개발, 악성코드 등 디지털기기 증거분석기법 개발 등 의 업무를 수행하는 것으로 규정되어 있다.[145]

경찰은 본청의 디지털 포렌식센터 외에 지방 17개청에 디지털 포렌식계(팀/반)가 설치되어 있는데, 본청은 지방청에서 분석이 곤란한 고난이도 매체분석 및 연구 개발 활동을 중심으로 하고 있으며, 지방청의 디지털 포렌식계는 각 수사관서에서 실제 분석 의뢰되는 분석매체에 대해서 증거분석 업무를 처리하는 조직이라 할 수 있다. 즉 디지털 포렌식계가 경찰에서 담당하는 대부분의 디지털 포렌식 분석업무 및 현장 지원을 수행하고 있다고 할 수 있다. 통상 각 지방경찰청별로 2~10명 내외의 증거분석관이 배치되어 있는데, 2016년 현재 61명의 증거분석관이 전국 지방경찰청에 배치되어 있는 것으로 나타나 있다.[146]

경찰의 디지털 포렌식 업무 운용에 있어서 가장 큰 문제는 국내에서 발생하는 형사사건의 대부분을 인지하는 상황하에서 디지털 포렌식을 통한 증거분석 요청은 지속적으로 증가하고 있는데 비해서 증거분석을 담당할 수 있는 인력수요가 뒷받침되지 못하고 있다는 것이다. 실제 2016년 국감자료에서 나타난 바에 따르면, 2015년에 경찰의 디지털매체 증거분석건수는 24,295건이었던데 비해 증거분석관수는 61명으로, 전국 평균 1인당 398건이었으며, 청별로는 충남청의 경우 1인당 912건, 대구청 1인당 777건이었던 것으로 나타났다.[147]

원칙적으로 디지털 증거에 대한 현장 압수·수색 단계에서부터 포렌식 전문가의 지원이 뒷받침되어야 증거의 무결성 및 신뢰성을 담보할 수 있지만, 경찰은 디지털 증거 분석을 담당하기에도 절대적으로 부족한 인력구조이기 때문에, 일선 수사관에게 디지털 증거의 압수·수색에 관한 기본적인 지식과 기술을 훈련시켜 수사관이 직접 디지털 증거에 대한 압수·수색을 수행하고, 분석만 증거분석관들이 담당하는 방식으로 운영되고 있다.

---

145) 신지호/최낙범, "경찰 디지털 포렌식 조직구조와 업무과정 개선방안에 관한 연구 - 거점분석실과 전문상담관 제도를 중심으로", 경찰학 연구 제16권 제3호, 2016, 240면.
146) http://biz.heraldcorp.com/view.php?ud=20161006000913; 2016.10.6.
147) http://biz.heraldcorp.com/view.php?ud=20161006000913; 2016.10.6.

검찰이 DFIS II를 통해 디지털 포렌식 프로세스를 운영하는 것과 유사하게 경찰은 '디지털 포렌식 포털'이라는 내부 온라인 시스템을 운영하고 있다. 다만 약간의 차이는 경찰의 온라인 시스템은 증거분석 요청 그리고 결과보고서 및 결과 파일의 회신의 용도로 활용되기 때문에 전체적인 포렌식 프로세스를 통합관리하는데는 한계가 있다는 점이라 할 것이다.

경찰의 디지털 포렌식 절차에 있어서는 일선수사관이 직접 디지털 증거에 대한 압수·수색업무를 수행하기 때문에, 수사관이 압수한 디지털저장매체 등에 대한 분석 필요성이 있다고 판단되면 디지털 포렌식 포털시스템을 통해 증거분석관에게 사건의 내용, 분석매체의 정보, 분석요구사항 등의 정보를 입력하여 분석을 요청하게 된다.[148] 이 단계는 시스템 접수로서 아직 분석대상이 되는 디지털 저장매체가 분석관에게 전달되지 않은 상태이기 때문에 분석관 또는 디지털 포렌식 팀장이 시스템상으로 분석요청 접수여부를 확인해도 분석업무를 진행할 수는 없다. 즉, 수사관이 분석대상이 되는 디지털 저장매체를 지방 경찰청 디지털 포렌식팀에 직접 전달하면 비로소 시스템 입력내용을 기반으로 실제 접수가 진행되고 분석업무를 수행하게 되는 것이다.[149] 분석관은 분석이 완료되면 분석결과보고서를 팀장에게 완료보고를 하고 분석을 의뢰한 수사관에게 결과를 회신하고, 수사관이 온라인 시스템에서 분석사건에 대한 완료처리를 하면 해당 사건에 대한 분석절차는 종료하게 된다. 즉 경찰의 디지털 포렌식 프로세스는 온라인과 오프라인이 연계되어 있는 시스템이고 비전문가에 의한 압수를 전제로 하기 때문에, chain of custody를 유지할 수 있는 실무표준매뉴얼과 디지털 증거처리기준이 마련될 필요가 있다고 할 것이다.

나. 디지털 포렌식 절차

경찰은 디지털 포렌식 절차와 관련한 근거규정으로 '디지털 증거 수집 및 처리 등에 관한 규칙'[150]을 두고 있으며, 실무매뉴얼로는 '현장수사관을 위한 디지털 증거 압수·수색 길라잡이'와 '디지털 증거처리 표준 가이드라인'이 있다.

---

148) 신지호/최낙범, 앞의 논문, 242면.
149) 신지호/최낙범, 앞의 논문, 242면.
150) 경찰청 훈령 제766호, 2015.5.22. 제정.

1) 디지털 증거수집 및 처리 등에 관한 규칙

동 규칙은 디지털 증거의 수집·운반·분석·보관 등 전 과정에서 증거분석관과 수사관이 준수해야 할 기본원칙과 업무처리절차를 규정하고 있다. 즉 경찰이 수행하는 디지털 포렌식 업무의 기본이 되는 절차적인 준수사항을 규정하고 있는 것이라 할 수 있다.

가) 디지털 증거의 수집

동 규칙은 디지털 증거의 수집에 있어 기본원칙으로서 동일성 원칙, 무결성 원칙 그리고 과잉금지원칙을 규정하고 있다.[151]

디지털 증거수집 절차에 있어서는 디지털 데이터의 압수·수색·검증 필요시 디지털 포렌식 센터 또는 지방경찰청 수사과장에게 지원요청을 하면 증거분석관이 기술적 지원을 제공할 수 있도록 규정하고 있다.[152] 그리고 디지털 데이터 또는 저장매체를 압수함에 있어서 동일성 및 무결성 확보를 위하여 피압수자 등의 참여권 보장, 해시값 생성 후 서명날인, 원본 보존, 압수·수색과정의 촬영, 저장매체의 봉인 등의 조치를 취하도록 규정하고 있다.[153]

나) 디지털 증거의 분석

디지털 증거의 분석에 있어서는 신뢰성이 확보되어야 하므로, 동 규정은 분석관의 자격과 정확성과 신뢰성 있는 과학적 기법, 장비 및 프로그램의 사용을 요구하고 있다.[154] 또한 원본과의 동일성이 유지를 위해 분석에 있어서는 복제본을 생성하여 분석함을 원칙으로 하고, 복제본 생성이 불가능한 예외적인 경우에 한해 원본 압수물로 분석할 수 있도록 규정하고 있다.[155]

분석절차의 신뢰성을 확보함에 있어서는 접근통제가 중요하므로 분석실 및 증거보관실에 대한 출입제한 규정을 두고 있다.[156]

---

151) 디지털 증거 수집 및 처리 등에 관한 규칙 제4조, 제8조.
152) 디지털 증거 수집 및 처리 등에 관한 규칙 제9조.
153) 디지털 증거 수집 및 처리 등에 관한 규칙 제12조.
154) 디지털 증거 수집 및 처리 등에 관한 규칙 제16조.
155) 디지털 증거 수집 및 처리 등에 관한 규칙 제17조.
156) 디지털 증거 수집 및 처리 등에 관한 규칙 제18조.

다) 분석결과의 제출 및 보관

증거분석관은 분석이 종료되면 지체 없이 증거분석결과 보고서를 작성한 후 분석의뢰자에게 통보해야 한다.[157] 증거분석이 완료되면 디지털 압수물, 복제본, 증거분석을 통해 획득한 디지털 증거는 분석의뢰자에게 반환하도록 규정하고 있으며, 반환후 지체없이 분석관에게 남겨져 있는 복제본이나 분석으로 획득한 증거는 지체없이 삭제하도록 되어 있다.[158] 즉 디지털 증거의 보관 및 관리에 대한 기본적인 책임은 분석관에게 있는 것이 아니라 수사관에게 있음을 분명히 함으로써 분석업무와 관리업무를 명확히 구분짓고 있다.

2) 현장 수사관을 위한 디지털 증거 압수·수색 가이드라인

앞서 기술한 바와 같이 경찰의 경우 수사관이 디지털 증거의 압수·수색을 하는 것이 일반적이므로, 현장수사관이 디지털 포렌식에 대한 기본적인 지식과 규정 그리고 기술적 방법 등을 숙지하고 있어야 한다. 현장수사관을 위한 디지털 증거 압수·수색 가이드라인은 그러한 목적하에서 디지털 증거의 개념 및 특징, 디지털 증거 압수와 관련한 용어 및 디지털 포렌식 관련 프로그램에 대한 설명, 디지털 증거의 증거능력과 관련한 형법상 규정에 대한 개념설명 및 증거능력 인정 요건 등을 기술하고 있다. 그리고 디지털 증거의 압수방법과 분석의뢰 방법 등을 기술하고 있다.

이 매뉴얼은 디지털 포렌식에서 준수해야 할 전체적인 프로세스를 기술하고 있는 것이 아니라, 프로세스 가운데 현장 수사관이 숙지하고 있어야 할 사항만을 세부적으로 열거하고 있는 것이며, 디지털 데이터 유형별· 매체별 구체적인 분석업무와 관련하여서는 별도의 세부적인 매뉴얼을 두고 있다.

가) 디지털 증거 압수 방법

형사소송법 제106조 제3항에 따라 디지털 증거의 압수는 현장에서 범위를 정하여 출력·복제하는 것이 원칙이고, 예외적으로 현장에서 선별 출력 및 복제가 불가능한 경우에는 전체 복제, 복제본 획득이 불가능하거나 현저히 곤란한 경우에는 원본반출 후 선별 출력복제를 하도록 기술하고 있다. 다만, 압수 대상이 몰수물이거나 범죄의

157) 디지털 증거 수집 및 처리 등에 관한 규칙 제19조.
158) 디지털 증거 수집 및 처리 등에 관한 규칙 제22조.

반복 방지 및 범죄로 인한 이익취득을 금지하기 위한 경우에는 원본압수의 필요성을 소명하여 압수하도록 하고 있다.[159]

디지털 증거 압수에 있어서는 동일성 및 무결성 확보조치로서 해시값 생성·봉인·현장 촬영 등을 이행해야 하고, 피압수자의 참여권을 보장하도록 하고 있다.[160] 특히 스마트폰의 경우에는 압수 즉시 전원차단을 실시하여 원격삭제 및 데이터 변경 위험을 방지하도록 요구하고 있다.[161]

나) 디지털 증거 분석의뢰 방법

디지털 증거 분석의뢰 방법은 앞서 기술했던 통합포털시스템인 '디지털 포렌식 포털'을 활용하는 방법을 기술하고 있다. 즉 포털 내의 사건관리시스템을 통해 사건정보·의뢰자 정보·분석의뢰 요구사항·증거물 정보 등을 기입하여 사건을 등록하도록 하고 있으며, 등록된 사건에 대한 디지털 증거분석 의뢰서를 생성하고 이첩을 요청함으로써 증거분석 의뢰를 가능하도록 하고 있다.[162]

다) 디지털 증거의 송부방법

디지털 증거는 본질적으로 취약하기 때문에 분석을 위해 현장에서 이동하는 경우 충격·자기장·습기·먼지 등으로 인한 손상이 유발되지 않는 용기에 담아 송부해야 하며, 분석을 의뢰한 사람이 직접 운반하거나 기타 신뢰할 수 있는 방법으로 송부하도록 하고 있다.[163]

3) 디지털 포렌식 표준 가이드라인

경찰청은 정보통신·교수·민간 IT전문가, 수사기관 등이 참여한 한국 디지털 포렌식 학회와 공동연구를 수행하여 2006년 12월에 「디지털증거 처리 표준 가이드라인」을 제작하여 배포한 바 있다. 이 표준 가이드라인은 기술적 표준절차를 기술한 것으로, 신뢰성·무결성·정확성·지속성이라고 하는 증거분석의 기본원칙을 준수하는 범주내에서 분석계획·수행절차·기록 및 보고서 제출 등의 일련의 과정을 상세히 기술한

159) 사이버안전국 디지털 포렌식 센터, 현장수사관을 위한 디지털 증거 압수수색 길라잡이, 2016, 20면.
160) 사이버안전국 디지털 포렌식 센터, 앞의 책, 21-22면.
161) 사이버안전국 디지털 포렌식 센터, 앞의 책, 23면.
162) 사이버안전국 디지털 포렌식 센터, 앞의 책, 40-45면.
163) 사이버안전국 디지털 포렌식 센터, 앞의 책, 50면.

실용 매뉴얼이라 할 수 있다.[164] 즉 발생가능한 대부분의 상황에 빠르게 대응할 수 있는 운영절차의 형태로 구성되어 있으며, 다양한 유형별 증거분석 명세서를 기술함으로써 단계별로 기술된 절차대로 분석을 수행할 수 있도록 되어 있다.[165] 따라서 디지털 증거를 수집, 분석, 보관함에 있어서 수사관 및 디지털 증거 분석관이 보다 용이하게 활용할 수 있는 절차와 준수사항으로 활용될 수 있는 표준업무지침이라 할 수 있다.

디지털증거 처리 표준 가이드라인은 사전준비, 증거수집, 조사, 분석의뢰·접수·운반, 증거분석, 결과보고서, 보존 및 증거관리 등 7개 절차로 구성되어 있다. 다만 이 가이드라인은 2006년에 만들어진 이후로 업데이트 되지 않은 관계로 그동안 급속히 발전된 디지털 기술을 반영하지 못하는 한계가 있다. 따라서 경찰은 현재 이를 새롭게 개정하여 디지털 포렌식 표준절차를 마련하고자 TF를 운영중에 있다.

가) 사전준비 프로세스

가이드라인은 사전준비 프로세스의 기본원칙으로서 최소한의 증거수집원칙·적법절차 원칙·무결성 원칙 등을 제시[166]하고 있으며, 사전준비 프로세스의 준비사항으로서 증거수집계획의 수립·증거수집팀 구성·수집장비 등[167]을 요구하고 있다.

나) 증거수집 프로세스

디지털 증거 수집절차에 있어서는 현장 촬영 및 스케치, 휘발성 증거 수집, 전원확인, 본체수집원칙, 증거물 포장 및 피압수자의 확인 등을 제시하고 있다.[168] 그리고 수집단계에서의 주의사항으로 압수시스템의 시간 확인, 소프트웨어 유형 및 네트워크 확인, 압수시스템 확인 및 원본손상 방지[169] 등이 기술되어 있다.

증거수집 프로세스에 있어서 수집, 분석의뢰, 접수, 운반에 관한 절차적 표준사항은 분석의뢰자와 증거분석관 간의 증거이송에 따른 chain of custody를 유지하기 위한 절차로서, 증거의 무결성과 신뢰성을 담보하기 위한 필수적인 사항이라 할 것이다.

---

164) 변정수, "한국형 디지털 증거분석 표준화: 경찰청 디지털 증거처리 표준가이드라인 및 증거분석 전문매뉴얼의 고찰", 디지털 포렌식 연구, 2007, 166-167면.
165) 변정수, 앞의 논문, 173면.
166) 경찰청, 디지털증거처리 표준가이드라인, 2006, 10면.
167) 경찰청, 앞의 책, 11-13면.
168) 경찰청, 앞의 책, 13-14면.
169) 경찰청, 앞의 책, 16-20면.

다) 증거분석 프로세스

가이드라인은 증거분석 프로세스의 기본원칙으로서 증거 원본의 안전한 보존 및 무결성 확보, 증거기법과 도구의 신뢰성 확보, 증거분석과정의 기록, 증거분석결과의 신뢰성 확보 등을 정의하고 있다.[170] 그리고 분석을 실행하기 전 준비사항으로서 분석에 필요한 장비 준비, 분석담당자 지정, 복제본 생성, 분석대상 및 범위결정을 제시하고 있다. 또한 증거분석 프로세스에 있어서 유형별로 - 디스크 포렌식, 네트워크 포렌식, 웹 포렌식, 전자우편 및 메신저 포렌식, 해킹 및 악성코드 포렌식, 데이터베이스 포렌식, 멀티미디어 포렌식, 암호 포렌식, 스테가노그래피 포렌식, 휴대폰 포렌식 - 증거분석 표준절차를 제시[171]하고 있다.

라) 결과보고 프로세스

결과보고 프로세스에는 결과보고서의 작성과 증거자료의 관리에 관한 기본원칙을 기술하고 있다. 먼저 결과보고서의 작성에 있어서는 사실관계 중심, 객관적 사실과 설명 및 의견의 명확한 구분, 증거발견 방법 및 증거물에 대한 작업내용의 문서화, 분석 및 처리과정에 대한 기록 유지, 사용된 하드웨어와 소프트웨어 기록 등이 포함되어야 하며, 분석관은 이에 대한 책임을 지도록 하고 있다.[172] 다음으로 증거자료 관리에 있어서는 디지털 증거에 적합한 증거보관실 설치, 증거물 데이터베이스 구축, 분석에 사용된 도구 및 프로그램의 지속적 관리보관, 증거보관실 및 증거물에 대한 접근통제 등이 포함되어 있다.[173]

제2절 디지털 포렌식에 대한 판례 경향

1. 디지털 포렌식 절차에 대한 법원의 태도

디지털 증거와 관련한 우리의 판례에 있어서 디지털 포렌식은 단지 디지털 포렌식

---

170) 경찰청, 앞의 책, 26면.
171) 경찰청, 앞의 책, 28-45면 참조.
172) 경찰청, 앞의 책, 48면.
173) 경찰청, 앞의 책, 48면.

센터 또는 디지털 포렌식 전문가라고 지칭하거나 디지털 증거 분석절차를 말할 때 사용되는 용어일 뿐이며, 디지털 데이터가 유효한 법정 증거로서 기능할 수 있도록 무결성과 신뢰성을 담보할 수 있는 디지털 증거의 압수 준비단계에서부터 전문가 보고서 제출 또는 전문가 증언에 이르는 일련의 절차를 일컫는 개념으로는 사용되고 있지 않다. 따라서 아직까지 우리 판례는 디지털 증거의 증거능력과 관련하여 디지털 포렌식의 신뢰성 여부에 대한 판단을 하는 경우가 많지 않다고 보여진다. 다만 일부 판례에 있어서는 판시내용에 디지털 증거의 수집에서부터 분석, 제출에 이르는 각각의 절차상의 요건들을 제시하는 방식을 취하고 있는 경우를 볼 수 있다.

아래에서는 디지털 포렌식과 관련하여 검토할 의미가 있는 판례들에 있어서 법원이 어떠한 판단기준을 적용하고 있는지에 대해서 살펴보고자 한다.

가. 서울중앙지법 2007.4.16. 선고 2006고합1365 등, 서울고등법원 2007.08.16. 선고 2007노929 판결

이 판결은 정보저장매체의 수집 및 제출단계에서부터 분석처리과정, 그리고 법정에서의 전문가 증언에 이르는 일련의 디지털 포렌식 프로세스의 신뢰성을 토대로 디지털 증거의 증거능력을 문제삼은 최초의 판결이라 할 수 있다. 또한 디지털 증거의 증거능력 판단에 있어서 무결성, 신뢰성, chain of custody - 직접적으로 이와 같은 용어를 기술하지는 않았지만 그 내용적 의미에 비추어 볼 때 -를 그 요건으로 기술하고 있는 바, 이것이 디지털 포렌식의 기본원칙에 해당하는 요건이라는 점을 처음으로 명시한 판결이라 할 것이다.

이 판결에서 피고측은 “검찰이 위 저장매체의 데이터가 본래 존재하였던 상태와 전혀 다름이 없이 수집·제출되었다는 사실과 위 전자적 정보의 분석처리과정에 대한 신뢰성에 대하여 그 입증책임을 다하지 못하였고, 이 법원의 검증절차에 참여하여 이를 주도적으로 진행한 증인의 전자적 정보 분석능력과 그 증언은 신뢰할 수 없으므로 위 문건들은 독립적인 증거로 사용할 수 없다”고 주장했다. 즉 디지털 포렌식 절차와 전문가 증인의 신뢰성에 대하여 이의를 제기하였다.

이에 대하여 법원은 컴퓨터 기록의 증거능력이 인정되기 위한 요건을 다음과 같이 제시하고 있다.

ⅰ) 컴퓨터 기록이 입력된 후 법원의 검증절차에 이르기까지 변경되지 않았음이 인정되어야 한다(무결성, chain of custody)

ⅱ) 컴퓨터 기록의 보관상황에 대한 신뢰성이 담보되어야 한다(chain of custody)

ⅲ) 디지털 저장매체 원본과 하드카피 또는 이미징한 매체 사이의 데이터의 동일성이 증명되어야 한다.(동일성)

ⅳ) 검증과정에 이용된 컴퓨터의 기계적 정확성, 프로그램의 신뢰성, 입력, 처리, 출력의 각 단계에서의 컴퓨터 처리과정의 정확성, 조작자의 전문적 기술능력이 갖추어져야 한다.(신뢰성)

그리고 본 사건과 관련하여 법원은 법정에 제출된 디지털 증거가 적법한 증거능력을 부여받기 위해서 어떤 절차를 거쳐야 하고, 그리고 그 절차들이 신뢰성을 갖기 위해서는 각 단계별로 어떤 방법으로 수행되어야 하는지를 분석적으로 기술하고 있다.

"ⅰ) 압수·수색영장을 통해 압수된 원본 디지털 저장매체는 그 자리에서 봉인되었다.

ⅱ) 수사기관에서 압수된 원본 디지털 저장매체에 대한 카피작업 또는 이미징작업을 위해 압수물의 봉인해제 및 작업후 재봉인 과정에 피고인이 참여했으며, 봉인 및 봉인해제, 재봉인 전과정을 녹화했다.

ⅲ) 이미징 작업시 디지털 저장매체 원본에 쓰기방지장치를 사용하고 이미징 장비를 통해 작업을 했다.

ⅳ) 법원의 검증절차시 피고인, 검사, 변호인이 모두 참여하였고, 법원의 전자법정 시설내의 규격에 적합한 컴퓨터와 EnCase 프로그램을 이용하여 적절한 방법으로 검증절차가 이루어졌다.

ⅴ) 컴퓨터의 기계적 정확성, 프로그램의 신뢰성, 컴퓨터 처리과정의 정확성, 조작자의 전문적 기술능력 등의 요건이 구비되었다"

따라서 피고인들의 주거지 또는 사무실 등에서 압수된 이후 법원에서의 검증절차에 이르기까지 보관과정의 신뢰성이 인정되며, 디지털 저장매체 원본을 이미징한 파일에

수록된 파일내용과 압수물인 디지털 저장매체로부터 출력한 문건의 동일성이 인정되므로 적법한 증거능력이 인정된다고 판시하였다.

법원이 이와 같이 분석적인 논리구조로 디지털 증거의 증거능력을 허용하기 위한 절차적 요건을 제시한 것은, 앞으로 점점 더 복잡해질 다양한 유형의 디지털 증거의 증거능력을 판단함에 있어서 법원이 고려해야 할 디지털 포렌식 절차별 준수요건이 무엇인가에 대한 논의를 제공했다는 점에서 중요한 의미를 갖는 판결이라 할 것이다.

다만 아쉬운 것은 디지털 포렌식 도구인 EnCase의 신뢰성에 대한 구체적인 판단기준을 제시함이 없이 단순히 '전 세계적으로 많이 사용되고 있는'이라는 표현으로 그쳤다는 점이다. EnCase에 대해서는 미국 법원에서 Frye test 뿐만 아니라 Daubert test에 의한 적합성 여부에 대한 법적 판단이 행해지고 있다. 따라서 본 판결에서도 EnCase의 신뢰성에 대한 판단기준을 제시했더라면 다른 디지털 포렌식 도구의 신뢰성을 판단함에 있어서도 중요한 선례가 되었을 것이다.

한편, 이 원심판결에 대하여 항소한 피고인측은 좀더 치밀하게 디지털 포렌식의 각 단계별 절차의 신뢰성에 이의를 제기함으로써 디지털 증거의 증거능력에 대한 배제를 요구하고 있다. 즉 항소심 판결인 "서울고등법원 2007.08.16. 선고 2007노929 판결"에서 피고인측은 다음과 같은 논지를 내세워 디지털 증거의 증거능력을 반박하고 있다.

ⅰ) 최초 이미징시 해시값 미작성은 디지털 포렌식 과정에서의 원본매체의 변경가능성을 추론할 수 있다.(동일성)

ⅱ) 국가정보원에서의 최초 압수에서부터 포렌식 복구절차와 검찰의 포렌식 복구절차사이에 chain of custody가 유지되었다는 것이 입증되지 않는 이상, 원본매체의 무결성을 절차적으로 그리고 기술적으로 보장했다고 볼 수 없다.(chain of custody)

ⅲ) 검찰 수사관 1인이 혼자서 이 사건 디지털 증거를 분석처리작업을 한 결과에 대해서는 신뢰성을 배척해야 한다.(포렌식 결과에 대한 재검증)

이에 대하여 항소법원은 다음과 같이 판단하고 있다.

ⅰ) 국가정보원에서 디지털 저장매체의 압수·봉인·해제 및 복제시 피고인측에서 입회하여 과정을 확인한 이상, 해시값 미작성으로 인해 디지털 저장매체의 내용이 변경될 가능성은 없다.

ⅱ) 디지털 저장매체내 원본자료의 내용과 출력문건의 동일성에 대하여는 원심의 검증절차를 거쳐 동일성이 확인되었다.

그런데 항소법원은 피고인측이 주장했던 디지털 증거의 분석을 담당한 디지털 포렌식 전문가와 그에 의해 작성된 결과에 대한 신뢰성에 대해서는 별도의 판단을 하지 않았다. 즉 디지털 포렌식 전문가의 증언 및 분석결과의 입증가치에 대해서는, 검찰 수사관이 해당 분석작업을 할 수 있는 전문지식과 기술을 보유한 사람인가의 여부와 그에 의해 작성된 결과가 제3자에 의해 검증되었는가 아니면 검증가능성이 있는가의 여부에 대한 판단이 이루어질 필요가 있음에도 이에 대한 판단을 배제한 것은 아쉬운 측면이 있다고 할 것이다.

나. 대법원 2013.7.26. 선고 2013도2511, 서울고등법원 2013.02.08. 선고 2012노805 판결

대법원 판결은 앞에 기술한 판결의 판시내용을 거의 동일하게 따르고 있는 판결로서, 디지털 증거의 증거능력 허용여부에 있어서 준수해야 할 절차적인 요건들을 기술함과 아울러 무결성 원칙이 요구됨을 명시적으로 기술하고 있다.

다만 차이는 디지털 저장매체로부터 출력한 문건의 증거능력과 관련하여 무결성 또는 동일성을 입증하는 방법에 있어서 이전 판결은 원본과 이미징 사본간의 해시값의 동일성 증명을 제시한 반면에, 동 판결은 해시값 증명이 원칙이지만 그러한 증명이 불가능한 경우에는 수사관이나 전문가의 증언 또는 법원이 원본과 출력문건을 대조하는 방법 등을 제시하고 있다는 점이다.

동 판결이 디지털 증거의 증거능력을 인정하기 위한 요건으로 제시한 사항은 다음과 같다.

ⅰ) 정보저장매체 원본이 압수시부터 문건 출력시까지 변경되지 않았다는 사정

즉 무결성이 담보되어야 한다.

ii) 정보저장매체의 원본과 하드카피 또는 이미징한 매체 사이에 자료의 동일성이 인정되어야 한다

iii) 컴퓨터의 기계적 정확성, 프로그램의 신뢰성, 조작자의 전문적 기술능력과 정확성이 담보되어야 한다.

iv) 출력문건과 정보저장매체에 저장된 자료의 동일성과 무결성 입증은 정보저장매체원본과 하드카피 또는 이미징한 매체의 해시값의 동일성에 대한 확인서면에 의한 증명이 원칙이지만, 그 증명이 곤란하거나 불가능한 경우에는 일련의 압수절차에 참여한 수사관이나 전문가 등의 증언 또는 법원이 원본저장 자료와 출력문건을 대조하는 방법으로 증명할 수 있다.

이 대법원 판결의 판시이유를 좀더 구체적으로 설명하고 있는 것이 항소심 판결인 "서울고등법원 2013.02.08. 선고 2012노805 판결"이라 할 수 있다.

동 항소심 판결에서 항소인인 피고인은 디지털 저장매체에 대한 압수·수색 집행과정을 촬영한 동영상에 대한 검증을 통하여 무결성이 입증되지 못하였다는 점, 이미징 파일에 대한 해시값을 법정에서 새로 산출한 것이 아니라는 점, 원본 디지털 정보저장매체상의 편집양식과 출력문건의 현출방식이 상이하다는 점, 그리고 검증절차에만 참여한 증인의 증언만으로 매체의 무결성과 출력문건의 동일성이 입증될 수 없으므로 매체로부터 출력한 문건의 증거능력은 없다고 주장하였다.

이에 대하여 법원은 앞서 기술한 대법원 2007. 12. 13. 선고 2007도7257 판결(원심 서울지법 2007.4.16. 2006고합1365 판결)에서 제시한 디지털 증거를 증거로서 허용하기 위한 절차적 요건으로서 무결성과 동일성이 인정되어야 한다고 판시하고 있다. 그리고 동 판결은 무결성과 동일성의 개념에 대하여, 무결성(보관의 연속성)이란 디지털 증거에 대한 압수·수색에서부터 법정에 증거로 현출되기까지 일련의 절차에서 그 증거가 변개, 훼손 등 인위적 개작이 없는 것을 의미하며, 동일성이란 원본과 복제본 혹은 출력물 간 또는 같은 저장매체의 압수·수색 당시와 증거로 제출될 때 동일해야 한다고 설명하고 있다. 그리고 무결성과 동일성의 입증에 대한 판단기준으로서, 먼저 무결성 입증은 압수절차 또는 복제 및 분석절차에 참여한 수사관이나 디지털

포렌식 전문가 등 관련자 진술, 봉인 내지 재봉인 상태에 대한 검증결과 등 제반사정을 종합하여 객관적이고 합리적으로 판단하면 족하고, 동일성 입증은 기본적으로 원본과 복제본의 해시값 비교를 통하여 원본과 복제본의 동일성을 확인한 후 복제본과 출력문건의 동일성을 검증하는 방법 등으로 판단하면 되지만, 위 동일성과 표리(표리)의 관계에 있는 무결성(보관의 연속성)이 담보되는 한, 반드시 동일성 입증을 위하여 해시값을 비교 확인하는 절차가 요구된다고 할 수 없고, 법정에 제출된 원본과 출력문건을 직접 비교한 검증결과 등 제반사정을 종합하여 판단하면 된다고 기술하고 있다.

위의 항소심 판결과 대법원 판결은 모두 디지털 증거의 무결성 또는 동일성 입증방법으로서 수사관 또는 조사관의 증언이나 입회인의 증언에 의한 증명을 허용하고 있기 때문에, 향후 디지털 포렌식 절차에 참여하는 전문가 증언의 유효성 판단을 위하여 전문가 자격에 대한 검증기준도 제시될 필요가 있다고 할 것이다.

2. 디지털 증거의 압수·수색과 관련한 판례의 경향

디지털 증거의 압수·수색과 관련한 판례들에 있어서 다투어지고 있는 가장 일반적인 쟁점은 압수·수색의 방법, 참여권의 보장 그리고 plain view에 관한 것이라 할 수 있다.

가. 압수·수색의 방법에 관한 법원의 태도

1) 디지털 증거에 대한 법원의 압수 대상 및 방법의 제한

현행 형사소송법 제106조 제3항은 디지털 증거를 압수함에 있어서 관련 있는 정보의 범위를 정하여 출력하거나 복제함을 원칙으로 하고, 예외적으로 출력 또는 복제가 불가능하거나 압수목적 달성이 현저히 곤란한 경우에 정보저장매체 자체를 압수할 수 있도록 규정하고 있다. 이에 따라 법원은 디지털 증거에 대한 압수방법을 구체적으로 규정하여 영장발부시 별지형태로 붙이고 있다. 별지의 내용을 보면 정보저장매체 자체를 압수할 수 있는 예외적인 경우를 다시 두 가지 경우 즉, 저장매체 소재지에서 하드카피·이미징 등의 복제본 형태로 반출할 수 있는 경우와 저장매체의 원본 반출이 허용되는 경우로 나누어 기술하고 있다.

먼저 하드카피나 이미징 등 복제본 형태로 반출할 수 있는 경우로는 ⅰ) 피압수자 등이 협조하지 않거나 협조를 기대할 수 없는 경우, ⅱ) 혐의사실과 관련될 개연성이 있는 전자정보가 삭제·폐기된 정황이 발견되는 경우, ⅲ) 출력·복제에 의한 집행이 피압수자 등의 영업활동이나 사생활의 평온을 침해하는 경우, ⅳ) 그 밖에 위 각호에 준하는 경우 등이 기재되어 있다. 그리고 원본저장매체의 반출이 허용되는 경우로는 ⅰ) 집행현장에서의 하드카피·이미징이 물리적·기술적으로 불가능하거나 극히 곤란한 경우, ⅱ) 하드카피·이미징에 의한 집행이 피압수자 등의 영업활동이나 사생활의 평온을 현저히 침해하는 경우, ⅲ) 그 밖에 위 각호에 준하는 경우로 기재되어 있다. 그리고 원본 저장매체 자체를 반출한 경우에는 이에 더하여 피압수자 등의 참여권을 보장한 가운데 원본을 개봉하여 복제본을 획득할 수 있고, 그 경우 원본은 지체없이 반환하되 특별한 사정이 없는 한 원본 반출일로부터 10일을 도과해서는 안된다고 되어 있다.

2) 대법원 2011.5.26. 자 2009모1190 결정(원심 서울중앙지방법원 2009. 9. 11.자 2009보5 결정)

본 결정의 항고인은 “이 사건 영장은 컴퓨터 저장장치에 저장된 정보의 경우 원칙적으로 수사기관이 휴대한 저장장치에 하드카피, 이미징하거나 출력물을 수집하는 방법으로 압수하되 이를 할 수 없는 불가피한 경우에만 그 저장장치 자체를 압수할 수 있도록 하는 등 압수의 방법을 제한하고 있음에도 피준항고인들은 이에 위반하여 단지 “빨리 집행을 마쳐야 하므로 카피할 시간적 여유가 없다”는 이유로 저장장치 자체를 압수하였으므로 이 사건 영장집행은 위법하다“고 주장하였다. 이에 대하여 법원은 다음과 같은 이유로 항고인의 청구를 기각하였다.

ⅰ) 압수대상 대부분의 컴퓨터에서 하드디스크가 제거된 점 등 증거인멸의 정황이 있었다.
ⅱ) 피압수자의 수가 7만명이고, 피의사실과 관련된 사람도 1만7천명이었다.
ⅲ) 피압수자들이 압수집행 현장에서 적대적으로 대했다.
ⅳ) 전원공급 장애로 하드카피가 물리적으로 불가능했다.
ⅴ) 저장매체에 저장된 파일크기를 고려하면 현장에서의 복제 및 출력은 원천적으

로 불가능했다. 따라서 컴퓨터 및 서버의 저장장치 자체를 압수한 것은 영장내용에 부합하는 집행이다"라고 판단했다.

이에 대해 재항고가 제기되었고 이 재항고에 대한 대법원의 결정은 디지털 증거에 대한 압수·수색 영장 집행시 정보저장매체 자체를 수사기관 등 외부로 반출할 수 있는 예외적인 경우 및 영장집행이 적법성을 갖추기 위한 요건을 구체적으로 명시하고 있다. 그리고 이 결정에 의하여 형사소송법 제106조 제3항이 입법되었으며, 현재 디지털 증거의 압수·수색방법에 대한 기준이 되고 있다.

본 대법원 결정은 디지털 증거의 압수·수색의 방법에 있어서의 원칙과 예외를 명확히 하고 있다. 즉 "원칙적으로 디지털 증거에 대한 압수·수색 영장집행은 혐의사실과 관련부분만 출력하거나 복사하는 방식으로 행해져야 한다. 그리고 이 원칙에 대한 예외로서 저장매체 자체 또는 하드카피나 이미징 복제본의 형태로 반출이 허용되는 경우로는 출력 또는 복사방식에 의한 집행이 불가능하거나 현저히 곤란한 부득이한 사정이 있어야 한다"는 것을 명확히 기술하고 있다.

그리고 영장집행의 적법성 요건과 관련하여서는 수사기관의 사무실 등으로 옮겨진 저장매체 자체 또는 하드카피나 이미징 등 복제본에에서 관련 정보를 탐색하는 것도 영장집행의 일환에 포함되므로, 범죄혐의와 관련성 없는 내용의 자료나 파일을 출력내지 복사하는 행위는 영장주의 원칙에 반하다고 판시하였다.

이에 따르면 수사기관은 현장에서건 기관내 분석실에서건 간에 범죄혐의와 관련이 있는 내용에 한해서만 출력 및 복제해야 위법수집증거배제법칙의 적용을 피할 수 있다고 할 것이다.

3) 서울중앙지방법원 2012.02.23. 선고 2011고합1131 판결

이 판결은 디지털 증거의 압수·수색에 있어서 원칙인 관련 범위내 출력 및 복사에 대한 예외로서 그것이 불가능하거나 현저히 곤란한 경우, 그리고 압수의 목적을 달성하기 어려운 경우가 현실적인 집행에 있어서 구체적으로 어떠한 경우인가를 적시하고 있다는 점에서 검토할 의미가 있다고 보여진다.

이 사건에서 피고인측은 영장이 허용하지 않는 방식으로 압수·수색 영장을 집행했으므로 위법하다고 주장하였다. 즉, "디지털 저장매체에 대한 압수·수색은 원칙적으

로 혐의 사실과 관련된 부분만을 그 자리에서 문서 출력물로 수집하거나 수사기관이 휴대한 저장매체에 해당 파일을 복사하는 형식으로 이루어져야 함에도, 모든 디지털 저장매체에 대하여 그 자체를 압수하거나 혹은 복제·이미징 등의 형태로 외부에 반출하였으므로 이는 위법한 집행이고, 위 매체 자체 또는 복제·이미징된 것을 외부로 반출한 이후 국가정보원 등 수사기관의 사무실에서 혐의 사실과 관련된 파일들을 압수·수색한 것은 영장이 허용하지 않는 위법한 집행"이라고 주장했다. 이에 대하여 법원은 다음과 같은 사유를 근거로 하여 원본 저장매체 자체의 반출 및 하드카피나 이미징 형태의 복제본 반출이 허용된다고 판단하고 있다.

"ⅰ) 현장에서 범죄사실과 관련성이 있는 전자정보만을 구분해내는 것은 현실적으로 불가능했다.
ⅱ) 암호가 설정되어 있어서 현장에서 그 내용을 지득할 수 없었다.
ⅲ) 삭제파일의 복구 등 추가적 분석이 필요했다."

즉, 본 판결은 압수·수색 현장에서 합법적 강제처분의 목적을 달성할 수 없는 불가피한 상황으로서 현장에서 압수한 매체 분량의 과다, 압수대상 매체에 설정된 암호해독의 필요성, 삭제파일의 복구필요성 등이 있음을 인정한 것이고, 이러한 경우에는 디지털 증거의 압수·수색 집행방법에 대한 예외로서 허용된다고 보고 있는 것이다.

4) 대법원 2015.7.16. 자 2011모1839 전원합의체 결정

본 결정은 정보저장매체 원본 또는 복제본을 수사기관 사무실 등 외부로 반출이 허용되는 예외적인 경우에 대한 판단과 반출된 저장매체 또는 복제본에서 관련성에 대한 구분 없이 정보를 출력하거나 복제하는 행위의 위법성여부에 대하여 판단을 하고 있다.

먼저 디지털 증거의 압수·수색방법의 예외로서 저장매체 원본 또는 복제본의 반출이 허용되는 경우에 대하여, 대법원은 "ⅰ) 현장의 사정이나 전자정보의 대량성으로 관련정보 획득에 긴 시간이 소용되는 경우, ⅱ) 전문인력에 의한 기술적 조치가 필요한 경우"를 그 예외적 사유로 제시하고 있다.

그리고 예외적으로 반출이 허용된 저장매체 원본 또는 복제본에서 영장기재사실과

의 관련성에 대한 구분 없이 전자정보를 출력하거나 복제하는 행위의 위법성과 관련해서, 대법원은 " ⅰ) 저장매체 자체 또는 복제본을 탐색하여 혐의사실과 관련된 전자정보를 출력 또는 복제하는 일련의 과정은 하나의 영장에 기한 압수·수색의 일환이며, ⅱ) 따라서 저장매체 자체 또는 복제본에서 출력 또는 복제할 대상 역시 혐의사실과 관련된 부분으로 한정하는 것은 적법절차, 영장주의 원칙, 비례원칙에 비추어 당연하다. ⅲ) 반출된 저장매체 또는 복제본에서 혐의사실 관련성에 대한 구분없이 저장된 전자정보를 출력 또는 복제하는 행위는 영장주의원칙에 반하는 위법한 압수"라고 판단하고 있다.

나. 참여권 보장에 관한 법원의 태도

법원은 디지털 증거의 압수·수색 과정에 있어서 피압수자 등의 참여권이 보장되어야 함을 명확히 하고 있다. 즉 법원의 영장별지에 의하면 "압수·수색의 전체과정(복제본의 획득, 저장매체 또는 복제본에 대한 탐색·복제·출력 과정 포함)에 걸쳐 피압수자 등의 참여권이 보장되어야 하며, 참여를 거부하는 경우에는 신뢰성과 전문성을 담보할 수 있는 상당한 방법으로 압수·수색이 이루어져야 함"이라고 기재되어 있다. 즉 법원은 압수·수색과정에서 참여권보장을 통해 절차의 적정성과 공정성을 확보하고자 하는 것이며, 이는 형사소송의 기본원칙인 적법절차원칙 - 실체적 적법성과 절차적 적법성 -에 따른 것이라 할 것이다.

1) 대법원 2011.5.26. 자 2009모1190 결정

대법원은 본 결정에서 전자정보에 대한 압수·수색 영장집행이 적법성을 갖추기 위한 요건과 관련하여 피고인 등의 참여권이 영장집행의 적법성을 담보할 수 있는 요건이라는 점을 명확히 하고 있다. 즉 "...저장매체에 대한 압수·수색영장을 집행할 때 영장이 명시적으로 규정한 위 예외적인 사정이 인정되어 전자정보가 담긴 저장매체 자체를 수사기관 사무실 등으로 옮겨 이를 열람 혹은 복사하게 되는 경우에도, 전체 과정을 통하여 피압수·수색 당사자나 변호인의 계속적인 참여권 보장, 피압수·수색 당사자가 배제된 상태의 저장매체에 대한 열람·복사 금지, 복사대상 전자정보 목록의 작성·교부 등 압수·수색 대상인 저장매체 내 전자정보의 왜곡이나 훼손과

오·남용 및 임의적인 복제나 복사 등을 막기 위한 적절한 조치가 이루어져야만 집행절차가 적법하게 된다."고 판시하고 있다.

2) 대법원 2015.1.22. 선고 2014도10978 전원합의체 판결

본 판결에서 피고인은 검사제출 증거는 전자정보의 복호화 과정 등에 대한 참여권이 보장되지 않아 증거로 사용할 수 없다고 주장하였다. 이에 대한 대법원은 압수·수색과정에서 수집된 디지털 관련 증거들은 유죄 인정의 증거로 사용할 수 있는 예외적인 경우에 해당한다는 이유로 위 증거들의 증거능력을 인정한 원심의 판단이 옳다고 보아 피고인의 주장을 기각하였다.

대법원이 제시한 논거는 다음과 같다.

"ⅰ) 절차를 준수하지 않은 압수 증거물의 증거능력 인정여부는 전체적·종합적 사정을 고려하여 볼 때, 수사기관의 절차 위반행위가 적법절차의 실질적 내용을 침해하지 않고, 오히려 그 증거의 증거능력을 배제하는 것이 헌법과 형사소송법이 형사소송에 관한 절차 조항을 마련하여 적법절차의 원칙과 실체적 진실의 발견을 통해 형사사법의 정의를 실현하려는 취지에 반하는 것으로 평가되는 예외적인 경우에는 그 증거를 유죄 인정의 증거로 사용할 수 있다.

ⅱ) 압수한 디지털 저장매체 원본 또는 복제본을 국가정보원의 사무실로 옮긴 후 …삭제된 파일을 복구하고 암호화된 파일을 복호화하는 과정도 압수·수색의 일환이므로 피고인 등에게 압수·수색 일시와 장소를 통지해야 함에도 하지 않은 것은 형사소송법 제219조, 제122조 본문, 제121조에 위배된다.

ⅲ) 하지만, 피고인들은 일부 현장 압수·수색과정에는 직접 참여하기도 하였고, 직접 참여하지 아니한 압수·수색절차에도 피고인들과 관련된 참여인들의 참여가 있었던 점

ⅳ) 현장에서 압수된 디지털 저장매체들은 제3자의 서명하에 봉인되고 그 해시(Hash)값도 보존되어 있었다는 점에 비추어 볼 때, 절차를 위반하여 압수된 디지털 증거를 유죄의 증거로 할 수 있는 예외적인 경우에 해당한다"고 판시하였다.

본 판결에서 대법원은 디지털 포렌식 분석과정에서 피고인 등의 참여권의 배제는 영장주의 원칙을 침해하는 것이지만, 참여권의 흠결을 보완 내지 대체할 수 있는 방법에 의하여 참여권에 의해 보장하고자 한 본래의 취지 즉 절차의 공정성과 적정성이 실현되었다면, 그리고 그것이 형사사법의 정의실현에 부합하는 것이라면 절차상의 하자는 어느 정도 치유될 수 있다고 본 것이라 할 것이다.

3) 대법원 2015. 7.16. 자 2011모1839 전원합의체 결정

대법원은 본 결정에서 저장매체 원본 또는 복제본을 수사기관의 사무실 등으로 옮겨 복제·탐색·출력하는 일련의 과정에서, 영장주의 원칙과 적법절차를 준수하기 위해서는 변호인에게 피압수·수색 당사자나 변호인 등에게 참여의 기회를 보장하고 혐의사실과 무관한 전자정보의 임의적 복제를 막기 위한 적절한 조치가 취해져야 한다고 명시하고 있다.

하지만 ⅰ) 피압수자측이 참여하지 아니한다는 의사를 명시적으로 표시한 경우, ⅱ) 참여 배제 등의 절차위반행위가 이루어진 과정의 성질과 내용에 비추어 참여권보장의 취지가 실질적으로 침해되지 않았다고 볼 수 있는 특별한 사정이 있는 경우라면 적법하다고 평가할 수 있다고 보고 있다.

위의 판례들에 비추어 볼 때, 디지털 증거의 압수·수색 집행과정에서의 피압수자 등의 참여권과 관련하여 법원의 태도는 참여권보장은 영장집행의 적법성 요건이지만, ⅰ) 피압수자가 명시적으로 참여하지 아니한다는 표시를 한 경우, ⅱ) 참여권을 보완 내지 대체할 수 있는 다른 방법으로 본래의 취지가 실현된 경우, ⅲ) 참여권 보장의 취지를 실질적으로 침해하지 않은 경우에는 피압수자 등이 집행절차에 참여하지 않은 경우라 하더라도 그로 인하여 취득한 디지털 증거의 증거능력이 배제되지 않는다고 보고 있음을 알 수 있다.

다. Plain View 관련 법원의 태도

Plain View 원칙은 미국법원에 의해 확립된 영장주의에 대한 예외로서, 수정헌법 제4조에 따라 수색권한을 가진 수사관이 일견 명백한 범죄의 증거를 발견하고 그

발견이 우연한 것일 때에는 영장없이 압수할 수 있다는 것이다. 다만 다른 영장주의 예외와 달리 영장없는 압수수색을 허용한다는 의미가 아니라 이미 육안으로 발견된 물건의 압수만을 허용한다는 것을 의미한다.[174]

디지털 증거의 압수수색에 있어서 대표적인 plain view 관련 판결은 U.S. v. Carey[175] 판결이다. 이 판결에서 미 연방대법원은 수사관이 처음 우연히 찾은 jpg 파일을 제외한 나머지 파일은 수색영장의 범위 밖에 있는 증거로서 증거능력이 없다고 판시하였다. 한편 U.S. v. Walser 판결에서는 수사관이 영장범위 밖에 있는 증거를 발견하자 수색을 중단하고 새로이 발견한 증거에 대한 수색영장을 추가로 발부받은 후에 수색을 했기 때문에 증거능력이 인정되었다. 이에 반해 U.S. v. Slanina[176] 사건에서 법원은 컴퓨터나 저장장치의 일부분의 무영장수색이 정당했다면 해당 장치내의 내용물에 대한 프라이버시에의 정당한 기대를 할 수 없다고 판결함으로써 우연히 발견한 영장범위 밖의 범죄사실에 대한 압수·수색이 수정헌법 제4조에 위배되지 않는다고 보았다. 또한 U.S. v. Comprehensive Drug Testing, Inc. 판결에서는 디지털 증거의 수색에 있어서 Plain View의 적용을 일률적으로 배제하고자 시도하기도 했다. 즉 미국 법원들이 디지털 증거에 대한 Plain View 원칙의 적용에 있어서 일관된 태도를 보이고 있지는 않다.

디지털 증거의 압수·수색에 있어서 Plain View 원칙을 그대로 적용할 수 있는가에 대해서는 논란의 여지가 있다. 일반적으로 정보저장매체내에는 방대한 양의 범죄 관련정보와 범죄무관 정보가 혼재되어 있어서 범죄관련 정보를 추출하기 위해 전체 파일을 열어보거나, 경우에 따라서는 특정 프로그램을 실행시켜야 할 뿐만 아니라 파일에 걸려있는 암호를 해제해야만 볼 수 있는 것들이기 때문에 비록 적법한 압수·수색현장에서 범죄와의 관련성이 인정될 수 있는 정보가 발견된 경우라 해도 이를 본래적 의미의 플레인 뷰라고 보기 어려운 측면이 있기 때문이다.

---

174) Robert M.and Bloom/Mark S. Brodin, Criminal Procedure(The Constitution and the Police), 5th ed. 2006, p. 171.; 대검찰청, "압수수색 관련 판례의 태도 및 외국 증거법제 도입가능성 연구, 2014. 66면에서 재인용.

175) U.S. v. Carey, 172 F.3d 1268(10th Cir.1999); U.S. v. Walser, 275 F.3d. 981(10th Cir.2001)

176) U.S. v. Slanina, 283 F.3d 670,680(5th Cir.2002); 경찰청, 한국형 디지털증거 표준 관리 모델에 관한 연구, 2015, 48면.

디지털 증거의 압수·수색에 있어서 Plain View와 관련한 우리 대법원의 입장은 2015.7.26. 2011모1839 전원합의체 결정에 의해 명확해졌다고 할 수 있다.

이 사건은 강력부 검사가 영장에 의하여 적법하게 압수한 정보저장매체 원본을 이미징 하여 대검 DFISII에 등록한 후 피압수자의 참여 없이 자신의 외장하드에 재복제를 하여 탐색한 결과 영장내 혐의사실과 무관한 정보를 출력하여 특수부 검사에게 통보하였고, 특수부 검사는 별건정보를 토대로 압수·수색영장을 받아 강력부 검사가 보관중인 복제본 중 본건 범죄사실 관련 데이터를 강력부 검사실에서 압수하였다. 이에 대하여 대법원은 수사기관의 별건정보에 기한 압수·수색의 적법성에 대하여 다음과 같이 판단하고 있다. 즉,

"ⅰ) 전자정보에 대한 압수·수색이 종료되기전 혐의사실과 관련된 전자정보를 적법하게 탐색하는 과정인 경우
ⅱ) 별도의 범죄혐의와 관련된 전자정보를 우연히 발견한 경우
ⅲ) 수사기관으로서 추가 탐색을 중단하고 별도 범죄혐의에 대한 법원의 압수·수색영장을 받은 경우
ⅳ) 별도의 압수·수색절차에 있어서 특별한 사정이 없는 한 피압수자에 대한 참여권 보장 및 압수목록 교부 등 적절한 이익보호조치가 취해진 경우"에는 적법한 압수·수색이라고 보고 있다.

제3절 현행 디지털 포렌식 프로세스의 문제와 한계

1. 디지털 포렌식 운영 현황에 대한 전문가 면접조사

가. 조사 목적 및 방법

현재 정부업무의 상당부분이 디지털화되어감에 따라 디지털 포렌식이 요구되는 분야가 점차 늘어가고 있다. 범죄수사를 담당하는 검찰과 경찰은 물론이고, 국방 및 국가안전을 담당하는 국방부, 기무사, 국정원, 저작권 침해조사를 담당하는 한국 저작권위원회, 그리고 관세청, 공정거래위원회, 선거관리위원회 등에서 디지털 포렌식

업무를 수행하고 있다. 즉 정부업무 가운데 수사 또는 조사업무를 담당하는 기관들에 있어서 디지털 포렌식은 필수적인 업무분야가 되고 있다고 할 수 있다.

이와 같이 다양한 정부기관에서 디지털 포렌식이 행해지고 있음에도 현재까지 어느 정도 공신력 있는 디지털 포렌식 절차 가이드라인이나 표준업무지침 등이 제시된 적이 없다. 각 기관의 업무의 필요에 따른 디지털 포렌식 업무 매뉴얼은 있지만 대부분 외부에 공개하지 않고 있기 때문에 그것이 얼마나 신뢰성을 담보할 수 있는 지침으로서의 역할을 하고 있는가에 대해서는 거의 논의되지 않고 있다.

따라서 본 연구의 일환으로 디지털 포렌식 업무를 수행함에 있어서 전문가들이 인식하고 있는 현행 디지털 포렌식의 문제점과 한계가 무엇이고, 디지털 포렌식 프로세스에 대한 인식은 어떠한지 살펴보고자 디지털 포렌식 전문가들을 대상으로 개별 또는 집단 인터뷰를 실시하였다.

인터뷰 방법은 개별 인터뷰의 경우에는 해당 기관을 직접 방문하여 디지털 포렌식 담당자를 대상으로 하였고, 집단 인터뷰의 경우에는 정부기관, 대학 그리고 민간영역(로펌, 디지털 포렌식 업체 등)에서 디지털 포렌식 업무를 직접 수행하거나 지원하고 있는 전문가들을 대상으로 하였다. 개별 인터뷰는 3개 정부기관에서 6명에 대해 실시하였고, 집단 인터뷰는 15명에 대해 실시하였다.

인터뷰 대상자를 선정할 때 고려한 사항은 현재 디지털 포렌식 분석을 직접 수행하고 있거나 디지털 포렌식 지원 등 관련 업무를 수행하는 사람, 그리고 대학에서 디지털 포렌식 교육을 담당하는 전공 교수들이 포함되도록 하는 것이었다.

나. 인터뷰 항목

전문가 인터뷰 항목은 크게 해당 기관의 디지털 포렌식 업무 구조, 전체적인 디지털 포렌식 절차 진행 방식 및 관련 업무지침 내용, 디지털 포렌식 도구 관련 사항, 디지털 포렌식 전문가 관련 사항, 형사소송법 개정에 따른 준비 현황 등으로 구성하였다.

유형	세부내용
디지털 포렌식 업무구조	• 디지털 포렌식 부서의 구성 및 운영 방식
디지털 포렌식 절차 진행방식 및 업무지침내용	• 현장수사단계에서부터 결과제출에 이르기까지 전체적인 프로세스 진행 방식 • 디지털 포렌식 업무지침 마련 여부 및 지침의 내용
디지털 포렌식 도구 관련 사항	• 디지털 포렌식 도구에 대한 검증(인증)의 필요성 • 디지털 포렌식 도구검증 기구의 필요성
디지털 포렌식 전문가 관련 사항	• 디지털 포렌식 전문가 자격 요건 • 디지털 포렌식 전문가 자격 검증시스템 유무 • 디지털 포렌식 전문가에 대한 교육훈련체계
형사소송법 개정에 따른 준비	• 법정에서 전문가 증언에 대비한 포렌식 분석관에 대한 교육 • 과학적 분석결과에 대한 입증 기준으로서 Daubert test에 대한 인식

2. 인터뷰 결과에 나타난 현행 디지털 포렌식 프로세스의 한계

가. 디지털 포렌식 전문인력의 부족

디지털 포렌식 프로세스 업무품질을 확보하기 위해서는 기본적으로 디지털 포렌식 분석관 내지 조사관들이 디지털 포렌식에 대한 충분한 이해를 기반으로 포렌식 도구의 활용에 대한 지식과 경험이 필요하며, 포렌식 절차를 진행하는 과정에서 무결성과 보안을 유지할 수 있는 유효하고도 신뢰할 수 있는 조사방식을 준수해야만 한다. 이와 같이 디지털 포렌식 분석관 등이 전문가로서의 지위를 확보하고 유지하기 위해서는 자신의 기술수준과 경험을 증명할 수 있어야 하고, 정기적인 교육과 훈련을 통해 자신의 능력을 향상시키고자 노력해야만 한다.

디지털 포렌식 프로세스의 신뢰를 평가함에 있어서 디지털 포렌식 전문가의 자격과 수준에 관한 문제가 제기될 수 밖에 없고, 따라서 디지털 포렌식 전문가에 대한 교육훈련과 능력검증의 필요성이 요구된다고 할 것이다. 그런데 현재 우리의 디지털 포렌식 업무의 현실은 이와는 상당히 동떨어진 측면이 있음을 확인할 수 있었다.

인터뷰 조사 결과, 현행 디지털 포렌식 프로세스가 디지털 포렌식의 절차적 표준에서 일반적으로 요구되는 사항들을 제대로 준수하지 못하는 가장 큰 장애요소로서 전문인력의 부족을 지적하였다. 즉, 디지털 증거의 압수·수색을 요하는 현장수요는 급증하고 있는데 비해서 디지털 포렌식 조사를 전담할 수 있는 전문인력의 공급은 늘어나지 못하고 있고 오히려 축소되는 기관들도 있는 것으로 나타났다.

앞서 기술한 바와 같이 대부분의 범죄수사를 담당하고 있는 경찰의 경우 각 청별로 배치된 디지털 포렌식 조사인력으로는 분석을 담당하기에도 한계가 있기 때문에 디지털 증거 압수·수색 현장지원은 거의 어렵고, 따라서 일선 현장수사관들을 교육-연간 4회 장비 취급요령, 장비사용요령 등 - 시켜 디지털 증거의 압수·수색을 직접 할 수 있도록 하고 있다.[177] 그리고 다른 기관에 비하여 디지털 포렌식 조사관들이 대부분의 압수·수색 현장지원을 하고 있는 검찰의 경우에도 점차 늘어나는 현장 지원수요를 감당하기 위해서 현장 수사관을 교육훈련시켜 디지털 포렌식 조사관 대신 디지털 증거 압수·수색을 할 수 있도록 하는 방안을 고민중이라고 하였다. 또 다른 정부기관의 디지털 포렌식 담당자는 기관 운영자의 디지털 포렌식 업무에 대한 인식 부족으로 오히려 전문인력이 감소되었을 뿐만 아니라 처우도 좋지 못해 이직이 잦아서 업무의 부담이 가중되고 있다고 하였다.

디지털 포렌식 프로세스에 있어서는 기본적으로 압수·수색의 준비단계에서부터 현장 수사관과 디지털 포렌식 전문가의 협업을 통해 수사계획을 수립해야 하고, 디지털 증거를 압수·수색하는 현장에 디지털 포렌식 전문가의 지원을 통해 압수단계에서부터의 증거의 무결성 및 chain of custody가 유지되도록 해야 하는데, 현재 각 기관의 디지털 포렌식 업무에 종사하고 있는 인력구조상 이를 뒷받침하기 어렵게 되어 있다고 할 수 있다.

또한 급속히 발전하는 디지털 기술에 대응할 수 있기 위해서는 디지털 포렌식 전문가에 대한 지속적인 교육과 훈련 그리고 테스트를 통한 검증을 거쳐 그들의 지식과 기술수준을 유지할 수 있도록 해야 하는데, 교육과 훈련은 기관 내부에서 자체적으로 1년 1회 내지 2회에 걸쳐 행하고 있지만 교육훈련의 결과에 대한 테스트를 통한 자격검증은 하지 못하고 있다고 하였다. 즉 현재의 디지털 포렌식 인력만으로도 부족한데 포렌식 조사관들에 대한 자격검증을 거쳐 전문인력을 재선별한다는 것은 현실적으로 생각하기 어렵다는 것이다. 그리고 이러한 디지털 포렌식 업무 인력의 부족현상은 포렌식 조사관 1인이 분석한 결과에 대하여 다른 분석관에 의한 교차검증도 사실상

177) 인터뷰 담당자에 의하면, 경찰의 경우 압수수색 현장이 대부분 일반 개인사무환경이라 스마트폰 압수가 많고 따라서 수집단계에서는 특별한 기술력이 요청되기 보다는 봉인과 훼손방지만 잘하면 무결성은 확보되기 때문에 현장수사관이 압수수색을 담당해도 무리가 없다고 한다.; 전문가 인터뷰 내용 인용.

불가능하게 만듦으로써 분석결과의 신뢰성을 보다 구체적으로 담보하기 어렵게 하고 있다는 점에서도 문제가 있다고 할 것이다.[178]

그리고 디지털 포렌식 업무의 특수성을 감안하여 볼 때 디지털 포렌식 조사관이 자신의 전문성을 계속 유지할 수 있도록 해야 함에도 불구하고, 해당 정부기관의 인사규정상 해당 업무에 종사할 수 있는 기간이 한정되어 있어서 그 기간이 지나면 다른 업무를 하도록 배치되기 때문에 디지털 포렌식 업무의 연속성을 유지하기가 힘들게 되어 있다고 할 수 있다. 이로 인하여 디지털 포렌식 업무 담당자들로 하여금 지속적으로 자신의 지식과 기술을 개발하고 능력을 향상시키도록 동기부여 하는데도 한계가 있다고 할 것이다.

한편, 디지털 포렌식 전문가 자격과 관련해서는 현재 법무부 주관하의 민간 자격증인 디지털 포렌식 전문가 자격시험이 있어서 디지털 포렌식 업무에 지원할 수 있는 일정한 자격에 대한 검증이 이루어지고 있다. 따라서 디지털 포렌식 전문가의 자격인증과 관련해서는 어느 정도 절차가 갖추어져 있다고 보는 것이 전문가들의 일반적 인식이라고 생각되었다.

나. 디지털 포렌식 도구의 신뢰성 확보의 한계

디지털 포렌식 프로세스에 있어서 도구는 가장 기본적이면서도 핵심적인 구성요소라 할 수 있다. IT 기술의 발전에 따라 정보저장매체와 디지털 기반 이용환경이 급속히 다양화되면서 이를 조사하는데 활용되는 디지털 포렌식 도구 역시 지속적으로 변화·발전하고 있다. 현재 정부기관에서 주로 활용하는 디지털 포렌식 도구의 상당부분은 상용화된 도구이며, 부분적으로 각 기관별 업무수행의 특성에 따라 자체개발된 도구를 병행하여 사용하고 있다.

디지털 포렌식 도구는 그것이 개발될 당시 적용되었던 요구사항이 맞게 구현되는지에 대한 확인 내지 검증이 필요하다. 즉 누가 그 도구를 사용하더라도 동일한 데이터에 대해서는 동일한 결과를 산출해낸다는 신뢰가 있어야만 그 도구를 사용하는 분석관들

178) 디지털 포렌식 분석관이 산출해낸 결과의 신뢰성을 담보하기 위해서는 다른 분석관에 의해서도 동일한 결과가 산출되었다고 하는 교차검증의 중요성이 요구된다. 현재 정부기관 가운데 국가정보원만 별도로 검증팀을 따로 두고 분석결과에 대한 재검증을 실시하고 있다고 한다.; 전문가 인터뷰 내용 인용.

도 그리고 그 도구에서 산출된 결과를 법정 증거로서 제시할 수사기관의 입장에서도 믿고 사용할 수 있기 때문이다. 검증된 도구의 활용은 수집 및 분석업무의 정확성 그리고 분석결과의 신뢰도를 확보할 수 있는 전제조건이라 할 수 있는 것이다.

인터뷰 결과에 따르면, 거의 모든 디지털 포렌식 전문가들 - 학계나 실무계 모두 -은 도구 인증의 필요성에 대한 요구가 매우 높은 것으로 나타났다. 즉 현재로서는 상용도구이건 자체개발 도구이건 간에 기능적 요구사항에 대한 확인 및 검증을 할 수 있는 공식적인 절차나 기구가 없기 때문에, 해당 도구를 이용하는 전문가의 입장에서도 신뢰성 내지 정확성 문제에 확신을 갖기 어려운 측면이 있다는 것이다. 특히 디지털 포렌식 도구의 검증에 있어서 현실적 한계는 상용도구의 경우 적용된 기술이나 분석방법이 특허로 등록되어 있는 경우가 많아서 소스코드가 공개되지 않기 때문에 그 유효성을 검사할 수 있는 방법이 없다는 것이다. 상용도구 뿐만 아니라 정부기관에서 자체 개발한 디지털 포렌식 도구의 경우에도 수사방법의 기밀성 등을 이유로 소스코드를 공개하지 않고 있을 뿐만 아니라 실제 각 기관에서 어떠한 도구들이 사용되는지 조차 외부에서는 알 수 있는 방법이 없기 때문에 도구의 신뢰성에 대한 검증은 내부적으로도 외부적으로도 한계가 있다고 보고 있다. 디지털 포렌식 도구의 인증과 관련한 또 다른 현실적인 문제로서 지적된 것은 그러한 인증에 있어서 상당한 시간과 예산이 요구된다는 점이었다. 즉 정부기관의 경우에는 디지털 포렌식 도구의 인증에 투입할 예산의 여력이 충분하지 않다는 점도 지적되었다.

이와 같이 디지털 포렌식 도구의 신뢰성 및 정확성을 담보할 수 있는 절차적·기술적 표준이 결여되어 있음에도 불구하고 현재까지 법원에서 도구의 신뢰성에 대한 논의는 이루진 적이 거의 없다. 이러한 디지털 포렌식 도구의 신뢰성과 관련하여서 현재 법정에서 논의된 경우로는 EnCase 뿐이었다. 이 경우도 EnCase의 신뢰성을 별도로 판단한 것이 아니라 단순히 '전세계적으로 많이 사용하고 있는' 것이기 때문에 신뢰할 수 있다고 판시하는 것으로 그쳤다. 즉 현재까지 우리 법원은 기본적으로 도구의 신뢰성 문제는 검토한 적이 없으며, 다만 최초 압수시 원본 해시값과 나중 해시값만 동일하면 중간의 신뢰성이나 무결성은 같이 판단하고 있기 때문에 도구 인증의 필요성이 논의될 여지가 없다고 할 수 있다.

디지털 포렌식 도구의 인증과 관련하여 전문가들은 현재 우리의 IT 기술력에 비추

어 볼 때, 민간주도하에 미국의 CFTT와 같이 디지털 포렌식 도구의 기능적 요구사항 구현의 정확성을 확인 내지 검증할 수 있는 시스템을 만들 수는 있지만, 민간주도 인증시스템을 만드는 경우 해당 기관의 공신력과 전문성을 문제 삼을 여지가 있기 때문에 정부 주도의 공신력 있는 인증기구의 도입이 필요하다고 제언하고 있다.

다. 디지털 포렌식 프로세스 표준화 작업에 대한 인식의 한계

디지털 포렌식에 있어서 압수·수색 준비단계에서부터 디지털 증거의 폐기 단계에 이르기까지 디지털 증거의 life cycle을 각 단계별로 표준화된 절차에 따라 유지·관리·통제할 수 있는 프로세스를 갖추게 되면, 각 단계별로 발생할 수 있는 증거의 오염 및 훼손 가능성을 차단할 수 있을 뿐만 아니라 각 단계별 연계성 유지로 인하여 단순히 증거 변개의 부재 뿐만 아니라 절차 진행에 따른 치환 내지 조건의 부재를 입증할 수 있기 때문에 그러한 프로세스의 준수에 대한 입증만으로 디지털 증거의 신뢰를 확보할 수 있다고 할 것이다. 디지털 포렌식에 있어서 요구되는 가장 본질적인 요소가 고도의 일관성과 재현가능성이라는 점에서 보면 프로세스 표준화는 디지털 포렌식에 있어서 필수적인 것이라 할 것이다.

유럽의 경우 이러한 디지털 포렌식 프로세스 표준화의 요구에 따르기 위해 ISO 17020, ISO 17025, ISO 27001 등과 같은 표준을 반영한 디지털 포렌식 처리절차를 확립하고자 노력하고 있으며, 유럽내 디지털 포렌식 실험실들도 ISO 인증을 받는 경우가 많아지고 있다. 즉, 이러한 절차적 표준에의 준수는 사용되는 프로세스와 절차가 적절하고 적합한 품질을 가지고 있다는 외부적 인정을 제공할 수 있으며, 만약 그 절차가 준수되면 법정에서 그에 대한 이의제기를 하는 것이 훨씬 더 어려워질 것이기 때문이다.

이러한 유럽이나 미국의 경우와 달리 우리의 경우에는 아직까지는 디지털 포렌식 프로세스 표준화에 대한 논의가 거의 행해지고 있지 않다. 디지털 포렌식 업무를 담당하는 전문가들도 프로세스 표준화의 필요성에 대한 인식이 별로 없으며, ISO 인증을 받기 위한 요구사항들이 우리의 디지털 포렌식 업무와는 상당한 괴리가 있어서 ISO 인증에 대해서는 부정적인 입장을 나타내는 것이 일반적인 경향이라고 할 것이다. 실제 인터뷰에 응했던 대부분의 전문가들이 프로세스 표준화에 대해서는 거

의 생각해 본적이 없었던 것으로 나타났으며, 프로세스 표준화의 필요성에 대해서도 현재의 절차로 충분히 chain of custody를 유지할 수 있고, 법원에서도 프로세스 표준이나 인증문제가 다투어지지 않는 현실에서 표준화에 대한 논의는 큰 의미가 없는 것으로 생각하는 것으로 나타났다.

라. 형사소송법 개정에 따라 제기되는 실무상의 문제

2016년 5월 29일 형사소송법 제313조 제2항이 개정되면서, 진술서의 작성자가 공판준비나 공판기일에서 그 성립의 진정을 부인하더라도 과학적 분석결과에 기초한 디지털 포렌식 자료, 감정 등 객관적 방법으로 성립의 진정함이 증명되는 때에는 증거로 할 수 있게 되었다. 그리고 피고인 아닌 자가 작성한 진술서의 기재내용에 대해서는 피고인 등이 공판준비 또는 공판기일에 작성자를 신문할 수 있도록 규정하고 있다. 즉, 디지털 포렌식 전문가가 디지털 증거를 분석한 결과를 기재한 보고서가 증거로서 허용될 수 있게 되었을 뿐만 아니라 그 보고서를 작성한 디지털 포렌식 전문가가 법정에서 증인으로서 신문을 받게 되었다.

이 규정의 개정으로 앞으로 디지털 포렌식 분야에서 논의되어야 할 사안은 디지털 포렌식 전문가의 자격과 그 분석결과에 대한 신뢰도 검증, 제출된 디지털 포렌식 자료의 기초가 된 과학적 분석이 무엇인가에 대한 입증 등이라 할 수 있다. 즉 디지털 포렌식 전문가가 법정증언을 함에 있어서 자신이 한 분석절차나 산출한 결과를 정확하게 설명하지 못하거나, 피고측의 반대심문에 적절히 대응하지 못하면 어렵게 분석한 자료를 증거로 사용하지 못하는 결과를 초래할 수도 있다. 즉 디지털 포렌식 전문가가 비전문가인 법관 또는 배심원 등이 쉽게 이해할 수 있는 방식으로 디지털 포렌식 분석결과를 설명할 수 있도록 하는 훈련이 필요한 상황이라 할 수 있다. 그리고 디지털 포렌식 전문가가 분석에 적용한 과학적 기술 내지 지식이 신뢰할 수 있는 것인가에 대한 입증이 요구될 가능성도 배제하기 어렵다고 할 것이다. 현재로서는 과학적 증거의 허용가능성에 대한 일반적 기준은 Daubert test - 결과를 산출해낸 이론과 기술의 검증 여부, 알려진 또는 잠재적 오류율, 학술저널이나 출간물을 통한 동료평가, 결과를 산출해낸 이론과 기술의 운용을 통제하는 기준의 존재 및 유지 여부, 관련 과학공동체 내에서의 광범위한 승인 - 인데, 법정에서 요구할 수 있는 이러한 심사기준을 어떻게

충족시킬 것인지에 대한 논의도 필요하다고 할 것이다.

이와 관련하여 정부기관의 포렌식 전문가들은 법정증언을 위한 훈련의 필요성 및 디지털 포렌식에 적용된 과학적 기술의 신뢰도 입증, 분석결과의 신뢰성 입증 방식 등의 문제에 대하여 고민은 하고 있지만, 아직까지는 준비가 안되어 있는 것으로 보여졌다. 다만 법정 증언과 관련해서는 일부 기관에서 디지털 포렌식 조사관 교육내용의 일부로 시행하고 있는 것을 볼 수 있었지만, 체계적인 교육이기 보다는 이미 법정증언을 해봤던 다른 분석관이나 조사관들의 사례를 교육하는 수준에 그치고 있었다.

제3장

KOREAN INSTITUTE OF CRIMINOLOGY

주요 국가들의 디지털 포렌식 시스템 및 프로세스

탁희성 · 이원상

제3장

주요 국가들의 디지털 포렌식 시스템 및 프로세스

제1절 미국의 디지털 포렌식 시스템

1. 디지털 포렌식 기관

가. 국립사법연구소(National Institute of Justice:NIJ)

1) NIJ 개요

NIJ는 과학을 통해 범죄와 사법에 관한 지식과 이해를 향상시키고자 하는 미 법무부 산하 연구개발 및 평가 기관이다. NIJ는 과학에 기반한 형사사법실무를 육성하고, 엄격한 과학적 연구를 범죄의 예방과 감소를 위해 일하는 형사사법전문가들에게 전달하고, 기술을 통해 보다 효율적이고 공정하며 효과적인 형사사법시스템을 확립하고자 하는 목표를 갖고 있다.[179] 즉 포렌식 과학의 연구개발에 있어서 혁신은 범죄를 해결할 수 있는 새로운 기술을 만들고, 포렌식 실험의 신뢰성과 효율성을 증가시키기 때문이다.

따라서 NIJ는 포렌식 과학에 있어서의 혁신을 촉진하기 위해 국립과학재단(NSF) 및 국립표준기술원(NIST)과 파트너쉽을 유지하고 있다. 특히 NIJ와 NIST working groups은 여러 포렌식 분야에서 요구되는 과학적 증거의 취급과 보존에 관한 best practice를 개발하고 있는데, 디지털 포렌식과 관련하여서도 가이드라인과 best practice를 제시하고 있다.[180]

---

179) http://www.nij.gov/about/pages/welcome.aspx; 2016.9.1.
180) U.S. Dept.of Justice, The Impact of Forensic Science Research and Development, NIJ 2015, p.3.

2) NIJ의 표준 개발

NIJ 표준과 테스팅 프로그램은 특별히 법집행, 교정, 다른 형사사법기관의 요구에 초점을 맞춘 장비 표준을 개발하고 발표하는 것으로, 확립된 최소한의 요구조건에 따라 장비가 안전하고 신뢰할 수 있는 수준을 확보하는 것을 그 목표로 한다.[181]

NIJ 표준은 임의적 표준이기 때문에 제조업자에게 그 표준을 따르도록 요구하거나 강제할 수는 없다. 이와 같이 NIJ 표준이 구속력을 갖는 것은 아니지만 그것이 best practice로 연계되어지기 때문에 영향력이 크다. 즉 이 표준을 채택하지 않음으로서 초래된 나쁜 결과물의 결과로서 형벌 또는 벌금형이 뒤따를 수 있다는 것을 기관에서 고려하지 않을 수 없는 것이다. [182] 이러한 표준을 가짐으로써 사용자는 장비의 주요한 특성에 대한 성능정보, 제품의 적합성에 대한 신뢰의 수준을 제공하며 표준화된 테스팅 방법과 최소한의 성능 요구사항을 토대로 한 제품의 비교가 가능하게 된다고 할 수 있다.

NIJ 표준은 형사사법실무자의 운용상의 요구와 관련된 특정한 도구와 기술에 관한 성능수준을 연계하는 것이기 때문에, 유효하고 일관되게 재현할 수 있는 방식으로 테스팅을 할 수 있는 현장에서의 실무적 경험을 반영하고 있다.[183]

NIJ는 표준이 요구된다고 판단되면 새로운 표준을 개발하거나 기존의 표준을 업데이트 하는데, 그 프로세스는 다음과 같다. “먼저 장비 요구사항을 정의하기 위한 특별 기술위원회를 소집하고 실무자들의 요구를 논의한다. 그리고 실무자, 제조업자, 그리고 테스트를 하는 실험실의 요구를 각각 다룬 표준에 관한 3가지 문서를 발표한다. 이해관계자들에게 정보를 전달하고 그들로부터 input을 받으며, 기존의 표준에 관하여서는 정기적이고 필수적인 심사절차를 확립한다.”[184]

---

181) http://www.nij.gov/topics/technology/standards-testing/pages/welcome.aspx; 2016.9.5.
182) http://www.nij.gov/topics/technology/standards-testing/pages/welcome.aspx; 2016.9.5.
183) http://www.nij.gov/topics/technology/standards-testing/pages/welcome.aspx: 2016.9.5.
184) http://www.nij.gov/topics/technology/standards-testing/Pages/developing.aspx; 2016.9.5.

3) 디지털 포렌식 분야의 NIJ 표준과 가이드라인

NIJ가 디지털 증거와 포렌식 분야에서 발표한 표준 및 가이드라인은 다음과 같다.

가) Forensic Examination of Digital Evidence: A Guide for Law Enforcement

이는 2004년에 발표된 것으로 디지털 증거의 조사에 책임이 있는 법집행직원에 의한 활용을 위한 지침서이다. 이 지침서는 디지털 증거를 취급함에 있어서 준수되어야 할 가장 기본적인 사항들을 열거하고 있다.

" - 디지털 증거를 취급할 때 일반적인 포렌식 절차상의 원칙들이 적용되어야 한다.
- 디지털 증거의 수집과 보존을 위해 취해지는 조치들이 그 증거의 무결성에 영향을 미쳐서는 안된다.
- 디지털 증거의 조사를 행하는 사람은 그 목적을 위해 훈련을 받아야 한다.
- 디지털 증거의 압수·조사·저장·이전에 관한 활동들은 기록되고 보존되어야 하며, 리뷰를 위해 활용가능해야 한다.
- 조사관은 디지털 증거에 대한 정확하고 공정한 조사를 행할 필요성을 인식해야만 한다
- 조사는 원본증거의 복제본에서 행하는 것이 최선이며, 원본증거는 증거의 무결성을 보호하고 보존하는 방식으로 획득되어야 한다.
- 조사 프로세스의 목적은 디지털 증거를 추출하고 분석하는 것이다.
- 증거에 대한 포렌식 절차 전체에 걸쳐 취해진 조치들과 관찰이 기록되어야 한다
- 법집행직원들은 연방법률, 주법률, 지방법률을 준수하기 위한 정책과 절차를 개발해야 한다.
- 컴퓨터 포렌식 조사를 행하기 위한 기본적인 조치는 정책과 절차의 개발, 증거평가, 증거 획득, 증거조사, 기록과 보고이다."[185]

나) Electronic Crime Scene Investigation: A Guide for First Responders(2 ed.)

이 지침서는 전자현장을 보존하고, 디지털 증거를 인지·수집·안전하게 보호하는데 책임이 있는 주와 지방의 법집행직원 및 기타 최초의 대응자를 지원하기 위한 것이다.

---

185) http://www.nij.gov/publications/Pages/publication-detail.aspx?ncjnumber=199408;2016.9.5.

이 지침서는 디지털 증거를 수반하는 범죄현장에 직면한 사람, 디지털 증거를 포함하는 범죄현장을 처리하는 사람, 디지털 증거를 처리하는 직원을 관리·감독하는 사람, 그러한 범죄현장을 처리하는 기관을 관리하는 사람 모두를 위한 것이다.

이 지침서는 7개의 장으로 나뉘어지는데, ⅰ) 전자매체의 유형·설명·잠재적 증거, ⅱ) 조사도구와 장비, ⅲ) 현장 보존과 평가, ⅳ) 현장기록, ⅴ) 증거수집, ⅵ) 디지털 증거의 포장·이송·저장, ⅶ) 컴퓨터 범죄와 범죄유형별 디지털 증거 고려사항이 그것이다.

다) Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors

"이 지침서는 디지털 증거와 관련한 네 번째 지침서로 법집행직원과 검찰에 대한 것이다. 이는 디지털 증거의 수집, 관리, 준비, 법정제출에 있어서의 주요문제에 중점을 두고 있기 때문이다.

이 지침서 제1장은 디지털 증거에 적절한 압수와 수색의 문제를 다루는데, 일정한 유형의 정보의 공개와 접근을 규제하는 연방법률 - 전자통신 프라이버시 법, 프라이버시 보호법 등 -들을 검토하며, 수정헌법 제4조하에서 적용가능한 원칙들을 검토한다.

제2장은 디지털 증거의 무결성·공개에 관한 것으로, 네트워크 또는 전자매체 보다는 독립된 매체로부터 확보한 정보의 무결성을 유지하는 것과 관련된 문제를 다룬다.

제3장은 디지털 증거를 수반하는 사건의 재판전 준비에 관한 3가지 측면, 즉 조사의 범위에 관한 예비적 고려사항·검사·조사관 그리고 경찰간의 재판전 효과적인 의사소통, 다양한 증거에 관한 문제(진정성 및 전문증거) 등을 다룬다.

제4장은 디지털 증거를 제출하는 방법에 관한 문제를 다루며, 마지막 장은 이전 장에서 제시된 가이드라인을 아동 포르노 사건에 있어서 디지털 증거의 활용에 활용하는 방법을 설명한다."[186]

라) Investigations Involving the Internet and Computer Networks

이 보고서는 인터넷 또는 다른 컴퓨터 관련 범죄를 입증하는데 책임이 있는 조사관들에게 정보를 제공하는 것이다. 즉 초기 대응자부터 법정에 이르기까지 조사절차에

---

186) http://www.nij.gov/publications/Pages/publication-detail.aspx?ncjnumber=211314; 2016.9.5.

관한 정보를 제공하는 것으로 초기대응자에 의한 전자적 범죄현장 조사, 디지털 증거에 대한 포렌식 조사, 인터넷과 네트워크 조사, 수사상 기술의 활용, 디지털 증거의 법정제출, 디지털 증거 포렌식 부서의 개발 등의 내용으로 구성되어 있다.[187]

마) Investigative Uses of Technology: Devices, Tools, and Techniques

이 보고서는 기술과 관련된 범죄 또는 그러한 범죄를 조사하기 위해 활용할 수 있는 도구와 기술에 관하여 전혀 경험이 없거나 제한된 경험을 가진 법집행직원과 기타 형사사법직원들에게 기본적인 정보를 제공하기 위한 것이다. 따라서 조사를 지원할 수 있는 기술과 자원, 조사에 영향을 미칠 수 있는 기술에 대한 검토, 디지털 증거와 관련한 조사에 있어서 직면할 수 있는 기술관련 도구와 장비에 대한 일반적 설명, 압수·수색과 관련한 수정헌법 제4조에 대한 검토 등을 그 내용으로 하고 있다.[188]

4) 디지털 포렌식 분야의 NIJ 프로젝트

가) The National Software Reference Library(NSRL)

NSRL은 미 상무부 산하의 과학기술표준연구소(National Institute of Standards and Technology)에 기반을 두고 있으며, 컴퓨터와 관련한 범죄의 수사에 있어서 컴퓨터 기술의 효율적이고 효과적인 활용을 위해 미 법무부의 NIJ, 연방, 주, 그리고 지방 법집행기관, 그리고 NIST로부터 지원을 받고 있다. NSRL은 다양한 소스로부터 소프트웨어를 수집하도록 디자인되어 있으며, 이러한 소프트웨어로부터 산출된 파일의 특징들을 Reference Data Set 정보안에 포함한다.[189] 그리고 컴퓨터 시스템에 대한 조사를 함에 있어서 컴퓨터 포렌식 조사관을 지원하는데 우선을 두고 있다.

NSRL은 소프트웨어 패키지의 대규모 수집, 그러한 소프트웨어 패키지를 구성하는 파일에 관한 상세한 정보 또는 메타데이터를 포함하는 데이터베이스, 수집한 각각의 파일에 관한 데이터베이스안에 있는 메타데이터의 하위세트를 포함하는 공공데이터

187) http://www.nij.gov/publications/Pages/publication-detail.aspx?ncjnumber=210798; 2016.9.5.
188) http://www.nij.gov/publications/Pages/publication-detail.aspx?ncjnumber=213030; 2016.9.5.
189) http://www.nsrl.nist.gov/new.html; 2016.9.5.

세트 즉 NSRL Reference Data Set(RDS)으로 구성되어 있다.[190] 특히 NSRL RDS는 파일과 파일의 출처를 고유하게 확인하는데 사용될 수 있는 컴퓨터 파일상의 메타데이터를 포함하고 있기 때문에, RDS 안의 파일 특징들을 매칭하는 방식으로 컴퓨터상의 파일을 리뷰하기 위해 법집행기관, 정부기관 또는 일반 산업체에 의해서 활용될 수 있다. 이러한 NSRL 데이터는 무료로 다운로드 받을 수 있도록 되어 있다.

NSRL에 의해 수집된 각각의 파일과 관련하여서는 암호해쉬값(MD5 and SHA-1), 파일원본에 관한 데이터(파일을 포함하고 있는 소프트웨어 패키지와 그 패키지 제조업체), 파일에 관한 기타 데이터(파일이름과 사이즈) 등이 게재된다. 이와 같이 NSRL에 의해 게재된 데이터는 오로지 파일의 내용을 토대로 컴퓨터상의 파일을 신속하게 확인하는데 활용된다. 대부분의 경우에 NSRL 파일은 범죄포렌식조사를 하는 과정에서 운용시스템과 애플리케이션 파일과 같은 알려진 파일들을 제거하는데 활용된다.[191] 이는 수동으로 조사해야 하는 파일의 수를 줄여주기 때문에 수사의 효율성을 높일 수 있다. 즉 범죄수사의 일부로서 압수된 컴퓨터 또는 파일시스템에 있어서 어떤 파일들이 증거로서 중요한가를 판단하는데 수반되는 엄청난 노력을 줄이는데 도움이 된다.[192]

나) Computer Forensic Tool Testing

컴퓨터 포렌식 도구의 신뢰성을 확보하고자 하는 목적으로 설립된 Computer Forensic Tool Testing(CFTT)은 NIST 프로젝트로, 일반적인 도구 요구사항, 테스트 절차, 테스트 기준, 테스트 세트, 테스트 하드웨어의 개발을 통해 컴퓨터 포렌식 소프트웨어 도구를 테스팅하는 방법론을 확립하는 것이다. 그리고 그 결과는 도구 제작자가 도구를 개선하는데 필요한 정보, 이용자가 컴퓨터 포렌식 도구의 획득 및 이용에 관하여 정보에 입각한 선택을 하는데 필요한 정보, 이해관계자가 도구의 능력 - 포렌식 소프트웨어 도구가 일관되게 정확하고 객관적인 테스트 결과를 산출한다는 것을 담보하기 위해 요구되는 능력 - 을 이해하는데 필요한 정보를 제공한다.[193]

---

190) http://www.nsrl.nist.gov/new.html; 2016.9.5.
191) http://www.nsrl.nist.gov/new.html; 2016.9.5.
192) http://www.nsrl.nist.gov/; 2016.9.5.
193) https://www.nist.gov/content/computer-forensics-tool-testing-cftt-project; 2016.9.5.

CFTT는 적합성 심사와 품질심사에 관한 국제적으로 승인된 방법론을 토대로 컴퓨터 포렌식 도구를 심사한다. 도구심사절차는 유형별 요구사항을 개발한 후 도구를 선정하고, 테스트 절차를 진행하게 되는데, 그 절차는 다음과 같다. 즉 "테스트할 도구를 확보하고 그 도구의 문서를 검토한 후 그 도구에 의해 지원되는 특징에 따라 테스트 사례를 선정한다. 이와 같이 테스트 전략을 개발한 후 테스트를 이행하고, 테스트 보고서를 작성한 후 운영위원회와 판매자가 그 보고서를 검토한 다음 NIST가 웹에 테스트 보고서를 게시한다."[194]

나. RCFL(Regional Computer Forensic Laboratory)

1) RCFL의 구성과 임무

RCFL은 테러, 아동포르노그라피, 폭력범죄, 기업비밀절도, 지식재산권 침해, 경제범죄, 재산범죄, 인터넷 범죄, 사기 등과 같은 범죄수사를 뒷받침하는 디지털 증거의 조사를 위해 전적으로 전념하는 원스톱 풀서비스 포렌식 실험과 훈련 센터이다.[195] 1999년 시범사업을 시작으로 해서 현재 미국내에 16개의 RCFL[196]을 두고 있다. RCFL은 법과학시험기관장협회 시험기관인증위원회(ASCLD/LAB)[197]에 따라 디지털 증거에 있어서 전세계적으로 가장 공인된 디지털 포렌식 실험실 네트워크로서, 법집행공동체에서 활용가능한 가장 수준 높은 품질의 디지털 포렌식 서비스를 제공하는데 전념하고 있다.[198] RCFL은 법집행공동체를 위한 서비스 품질을 지속적으로 향상시키고 있으며, 그 일환으로 2014년 한해 동안 6개의 RCFL(Chicago, Great Houston, Kentucky, New Mexico, Northwest, Philadelphia)이 국제적인 인증을 받음[199]으로서 현재까지 16개 RCFL 14개가 ASCLD/LAB 국제인증을 받았다. 이러한 ASCLD/LAB

194) http://www.cftt.nist.gov/Methodology_Overview.htm; 2016.9.5.
195) https://www.rcfl.gov/about/about; 2016.9.1.
196) chicago, Northwest, Greater Houston, Orange County, Heart of America, Philadelphia, Intermountain West, Rocky Mountain, Kentucky, Sandiego, New Jersey, Silicon Valley, New Mexico, Western New York, North Texas.
197) ASCLD/LAB은 "American Society of Crime Laboratory Directors/Laboratory Accreditation Board"의 약자로서 디지털 포렌식 분석실의 신뢰성을 인증하는 범죄 및 포렌식 랩의 인가기관이다.
198) U.S. Dept. of Justice, Regional Computer Forensics Laboratory Annual Report For Fiscal Year 2014, p.4.
199) U.S. Dept. of Justice, op.cit., p.9.

을 통한 인증은 5년 동안 보장된다.[200]

RCFL 조사관들은 연방, 주, 그리고 지방 법집행기관에 근무한 경험과 재능이 결합된 사람들이며, RCFL은 일반적으로 15명으로 구성되는데 그 가운데 12명은 조사관, 3명은 RCFL 지원인력이다. RCFL의 임무는 범죄현장에서 디지털 증거를 압수하고 수집하는 것이며, 제출된 컴퓨터 증거에 대한 공정한 조사를 행하여 요구된 바에 따른 증명을 하는 것이다.[201]

2) RCFL의 관리감독

2002년 FBI는 RCFL의 운영을 관리감독하고 새로운 RCFL의 설립을 용이하게 하기 위하여 National Program Office(NPO)를 설립했다.[202] NPO가 RCFL을 지원하는 방식은 다음과 같다.

"ⅰ) 각 RCFL이 지속적인 품질 관리를 확보할 수 있도록 기술적 지원을 제공한다.
ⅱ) RCFL의 설립과 규제에 관한 정책, 실무, 법적 절차를 제도화한다.
ⅲ) 법집행기관, 민간영역, 학계 그리고 정부 기관들간의 정보의 교환과 배포를 위한 국가정보센터로서 기여하는 다른 정부기관들간의 업무관계를 육성한다.
ⅳ) 이 프로그램의 지지자로서 기여한다.
ⅴ) 새로운 디지털 증거 포렌식 도구를 개발하기 위하여 FBI와 다른 정부기관과 함께 일한다.
ⅵ) 디지털 증거 조사관과 법집행직원들을 위한 훈련 교육과정을 개발한다.
ⅶ) 법집행공동체에 의해 활용될 도구개발 노력과 훈련계획을 조정하고 전달한다."[203]

3) RCFL의 서비스

RCFL은 법집행공동체에 다수의 서비스를 제공하는데, 그 내용은 다음과 같다.

"ⅰ) 압수전 협의 - RCFL은 선서진술서에 포함될 수 있는 컴퓨터 관련 용어에 관하여 조언을 해줌으로써 컴퓨터 증거와 관련한 수색영장준비를 지원할 수 있다.

---

200) U.S. Dept. of Justice, op.cit., p.11.
201) https://www.rcfl.gov/about/about; 2016.9.1.
202) https://www.rcfl.gov/; 2016.9.1.
203) https://www.rcfl.gov/; 2016.9.1.

ii) 현장 압수 및 수집 - 이러한 유형의 지원요청은 최소 48시간 전에 서비스요청양식을 제출함으로써 행해져야 한다. 하지만 법집행직원이 예기치 않게 컴퓨터 증거를 발견한 경우에는 이러한 사전고지요건은 포기된다.

iii) 컴퓨터와 컴퓨터 관련 증거의 복제, 저장, 보존 - 데이터가 오염될 가능성이 있기 때문에 조사는 원본 증거의 복사본에 대해서 행해진다. 따라서 RCFL 조사관은 상황에 따라 현장에서 매체를 복제하거나 매체를 복제할 실험실로 전자장비를 가져와서 복제한 후에 조사를 수행한다.

iv) 디지털 형태로 저장된 매체에 대한 적정하고 정확하고 공정한 포렌식 조사 - 컴퓨터 포렌식 조사관은 과학자이기 때문에, 그들의 업무는 디지털 형태에서 조사관이 볼 수 있는 일정한 형태로 전환하기 위하여 컴퓨터/컴퓨터 관련 증거에 대한 엄격하고 객관적인 조사를 수행하는 것이다.

v) 법정증언 - 압수된 컴퓨터 증거로부터 기록이 복구된 경우, 검찰은 컴퓨터 또는 컴퓨터 관련증거를 법정에 제출하기 위해 조사관을 활용할 가능성이 있다. 전문가 증인으로서 조사관은 선서하에서 그들이 결과로서 발견한 것이 무엇이고 그 조사가 어떻게 수행되었는가에 대해 설명할 수 있다."[204]

4) RCFL 서비스 품질 강화를 위한 인증 지원노력

실험실들이 인증을 받기 위해서는 광범위한 평가를 수행하는 전문가 평가단에 의해 강도 높은 평가를 받게 되는데, 이러한 인증을 받는다는 것은 범죄 실험실의 관리, 직원, 품질시스템, 운영 및 기술적 절차, 장비, 물리적 설비들이 확립된 기준을 충족한다는 것을 입증하는 것이라 할 수 있다. 인증을 위한 요구사항은 국제표준기구(ISO) 17025-2005 표준과 ASCLD/LAB 추가 요구사항에 토대를 두고 있다.[205] 따라서 인증은 RCFL의 품질향상, 운용절차의 강화, 표준의 확립, 조사관 자격의 보장, 증거의 보호, 정확한 포렌식 결과의 보장에 기여하게 되는 것이다.

"■ 품질향상(Improves Quality) - 인증을 받은 실험실들은 적절한 품질통제와 품질보증절차를 준수해야 한다. 인증은 RCFL의 서비스 품질을 강화하는데, 그 이유

204) https://www.rcfl.gov/services; 2016.9.1.
205) U.S. Dept. of Justice, op.cit., p.11.

는 독자적이고 공정하며 객관적인 전문가 팀이 실험실의 결과물과 운영을 리뷰하기 때문이다.

- 운영강화(Strengthens operations) - 인증은 RCFL이 수행결과를 평가하도록 디자인된 기준에 의해 구속을 받도록 함으로써 운영을 강화한다.
- 표준확립(Establishes Standards) - 인증으로 인해 RCFL의 이용자와 일반인들은 실험실이 확립되고 널리 승인된 표준을 따르고 있다는 것을 보장받게 된다.
- 조사관 자격 보증(Gurantees Examiner Qualifications) - ASCLD/LAB은 실험실들이 직원가운데 인증받은 조사관들을 보유하고 있을 것을 요한다. 모든 조사관들은 FBI의 엄격한 컴퓨터 분석 대응팀(CART)의 인증 프로세스를 거쳐야 하며, 그렇게 할 때까지는 독자적으로 조사를 수행할 수 없다. CART 인증은 개인이 일정 정도의 지식을 가지고 있고, 조사관이 컴퓨터 포렌식에 있어서 짧은 과정을 택하는 최근의 경향에 대응할 수 있다는 것을 의미하며 따라서 전문가로 간주되는 것이다.
- 증거보호(Protects Evidence) - 인증은 프로그램의 엄격한 처리절차를 강화한다.
- 정확한 결과의 보장(Ensure Accurate Results) - 인증은 가장 기본적이고 복잡한 절차에 관한 경험적 토대로서 기여하는 충분한 서면 프로토콜을 요구함으로써 포렌식 결과를 향상시킬 수 있다."[206]

다. DCFL(Defense Computer Forensic Laboratory)

DCFL은 미 국방부 사이버범죄센터의 디지털 포렌식 전담부서(Defense Cyber Crime Center:DC3)로서 국방부 산하기관의 디지털 포렌식을 지원하고 있다. DC3은 우수한 디지털 포렌식과 멀티미디어 랩 서비스, 사이버 기술훈련, 기술적 솔루션 개발, 국방부의 임무에 해당하는 정보보호, 주요한 기반시설 보호, 법집행과 첩보, 문서와 매체 활용, 테러 대응을 위한 사이버분석을 제공하는 것을 그 임무로 하고 있다.[207] 이러한 DC3가 제공하는 서비스 가운데 디지털 포렌식을 담당하는 부서가 DCFL로, 국방부를 위하여 디지털과 멀티미디어 포렌식 조사·데이터 추출·전문가 증언 등을

206) U.S. Dept. of Justice, op.cit., p.10.
207) http://www.dc3.mil/index#dc3; 2016.9.10.

수행한다.

DCFL 운용은 품질통제와 동료심사를 받는 신뢰할 수 있고, 반복가능하며 유효한 시험결과를 가이드 하는 ASCLD/LAB에 따라 ISO 17025하에서 2005년에 인증을 받았다.[208] DCFL은 테러대응, 대정보 문제, 대인&대물 범죄, 네트워크 침입, 악성코드, 사기, 비행기사고, 손상된 매체와 수몰된 장치, 휴대폰, 테블릿&모바일 장치, 암호와 관련한 사건을 처리한다.[209]

DCFL을 구성하는 Section은 다음과 같다. "Evidence(EV) Section은 조사 또는 분석을 위해 DCFL에 제출된 모든 증거와 매체를 다루며, Intake(IN) Section은 실험 신청서가 접수되자마자 고객지원을 제공하기 위해 2011년 가을에 만들어졌다. Imaging&Extraction(I&E) Section은 실험실에 제출된 모든 매체에 대한 포렌식 복제를 행한다. 제출된 매체는 컴퓨터 및 그와 연결된 외부 매체에서 부터 게이밍 시스템, 휴대폰, GPS시스템과 같은 장치에 이르기까지 다양하다. Major Crime(MC) Section은 범죄수사를 지원하는 디지털 증거분석을 수행한다. 지원되는 사건 유형으로는 사기, 안전조사, 대인범죄, 재산범죄 등이 포함된다. Counterintelligence/Counter-terrorism(CI/CT) Section은 국가안전에 영향을 미치는 모든 비밀등급에 대한 정보활동수사를 지원한다. Intrusion(IN) Section은 컴퓨터 침입, 악성코드에 대한 조사와 분석 그리고 악의적인 암호관련 조사 또는 수사를 행한다. Litigation Support(LS) Section은 조사관이 재판 또는 군법회의 절차에서 증언을 제공하도록 하는 소송상의 요구와 출장을 조정한다. Quality Assurance(QA) Section은 모든 DCFL의 산물에 있어서 품질이 최우선하도록 보장한다. QA 활동의 범위는 기술적 조사에 대한 품질 리뷰에서부터 기술문서작성 그리고 디지털 포렌식과 멀티미디어 포렌식에 있어서 유지되는 실험실 표준의 보장에 까지 미친다."[210]

ASCLD/LAB에 의한 지속적인 인증을 유지하는 DCFL을 지원하기 위하여 2002년 국방사이버범죄 연구소(Defense Cyber Crime Institute:DCCI)가 만들어졌다. DCCI는 국방부의 법집행과 정보활동단체에 고유한 도구와 절차를 만들기 위한 깊이있는

208) http://www.dc3.mil/digital-forensics/; 2016.9.10.
209) http://www.dc3.mil/digital-forensics/digital-forensics#process; 2016.9.10.
210) http://central.gutenberg.org/articles/defense_computer_forensics_laboratory: 2016.9.10.

연구를 수행할 자원으로서 역할을 수행한다. 즉 DCCI의 임무는 디지털 포렌식 도구와 기술의 연구와 개발, 디지털 포렌식 도구와 기술에 대한 테스트 및 평가와 인증을 하는 것이다. 특히 DCCI는 범죄수사·정보활동수사·정보보호·정보작전에서 사용되는 사이버포렌식 관련 도구·기술·절차를 개발·분석하고 테스트함으로써, 인증된 도구와 기술 프로세스가 정확하고 신뢰할 수 있으며, 반복가능하다는 것을 보장한다.[211]

2. 디지털 포렌식 업무 관련 지침 및 가이드라인

가. Electronic Crime Scene Investigation : A Guide for first Responders

1) 목적과 기본원칙

이 지침서는 NIJ에 의해 발간된 것으로 컴퓨터 범죄현장 그리고 디지털 증거의 인지·수집·보호에 책임이 있는 주 법집행직원과 지방 법집행직원 그리고 기타 초동수사를 담당하는 사람을 지원하기 위한 것이다.[212]

이 지침서는 디지털 증거를 취급하는 사람은 디지털 증거의 취약성을 명심하고 증거수집 및 보존에 관한 원칙과 절차를 인지하고 있을 것을 요한다. 따라서 디지털 증거를 취급할 때 적용되어야만 하는 "일반적인 포렌식 절차원칙으로서, ⅰ) 디지털 증거의 수집·보존·이송 절차가 증거를 변경하지 않아야 한다. ⅱ) 디지털 증거는 그 목적을 위해 특별히 훈련을 받은 사람에 의해서만 조사되어야 한다. ⅲ) 디지털 증거의 압수·이송·저장하는 과정 중에 행해진 모든 사항은 전부 기록되어야 하고, 보존되어야 하며, 재검토가 가능해야만 한다."[213]고 기술하고 있다. 그리고 범죄현장에서 초동수사를 담당하는 사람이 디지털 증거를 취급함에 있어서 따라야 할 조치들로서 " ⅰ) 현장에 있는 모든 디지털 증거를 인지·확인·압수·보존하라, ⅱ) 증거가 발견된 구체적인 장소와 전체 현장을 기록하라, ⅲ) 디지털 증거를 수집하고 라벨을 붙이고 보존하라, ⅳ) 안전한 방법으로 디지털 증거를 포장하고 이송하라"[214]고 기술하고 있다.

---

211) http://central.gutenberg.org/articles/defense_computer_forensics_laboratory; 2016.9.10.
212) U.S. Dept. of Justice, Electronic Crime Scene Investigation: A Guide for First Responders, 2nd.ed. 2008, p.vii.
213) ibid.

그리고 초동수사를 담당하는 사람은 전자 장치를 압수할 때 전자 장치안에 저장된 데이터에 부적절하게 접근한 경우에는 연방법률 - 통신프라이버시법률, 프라이버시법 - 을 위반할 수 있다는 것을 명심해야 한다. 따라서 현장에서 디지털 증거를 압수할 수 있는 적절한 법률상 권한을 갖고 있다는 것을 확실히 하기 위해 적절한 관할권에 대하여 검사에게 자문을 구해야만 한다.[215]

이 지침서 제2판에는 없지만 2001년에 발간된 제1판에는 개요 부분에 포렌식 절차에의 준수를 기술하고 있다. 즉 디지털 증거의 특성상 법정에서 채택되기까지 논란이 있을 수 있으므로 이에 대처하기 위해서 적합한 포렌식 절차 - 수집, 조사, 분석, 보고 - 를 준수해야 한다고 기술하고 있다. 수집단계에서는 디지털 증거의 검색·파악·수집 및 해당 과정의 기록이 이루어져야 하고, 조사단계에서는 디지털 증거를 가독성 있는 상태로 변환하고 입증가치의 존부에 따라 데이터를 분리하며, 분석단계에서는 사건의 관점에서의 중요성과 증거로서의 입증가치를 검토하며, 마지막 보고 단계에서는 조사과정과 복구한 데이터에 대한 설명을 보고서로 작성하고, 조사자의 자격과 조사절차의 타당성 등에 대한 증언이 요구될 수 있다고 기술되어 있다.[216]

2) 지침서의 구성

가) 전자장치의 유형과 설명 그리고 잠재적인 증거

이 지침서 제1장은 범죄수사나 기소에 있어서 증거로 활용할 수 있는 정보를 포함할 수 있는 전자장치 - 하드 드라이브, 외장 드라이브 등 기타 전자장치 -의 유형과 그 구성요소에 대한 설명 그리고 그 안에 잠재되어 있을 가능성이 있는 디지털 증거가 무엇인가를 기술하고 있다. 즉, 컴퓨터 시스템, 저장장치, 휴대용 장치, 주변장치, 기타 디지털 증거의 잠재적 소스, 컴퓨터 네트워크 별로 구성요소에 대한 설명 및 그로부터 발견될 수 있는 잠재적 증거를 기술하고 있다.[217]

---

214) U.S. Dept. of Justice, op.cit., p.ix.
215) U.S. Dept. of Justice, Electronic Crime Scene Investigation: A Guide for First Responders, 2nd.ed. 2008, p.vii-viii.
216) U.S. Dept. of Justice, Electronic Crime Scene Investigation: A Guide for First Responders, 2001, pp.2-3.
217) U.S. Dept. of Justice, op.cit., pp. 1-12.

나) 수사도구와 장비

이 지침서 제2장은 디지털 증거를 포함하는 물품이나 장치를 수집할 때 필요한 도구와 장비에 대한 정책과 절차를 기술하고 있다. 즉 디지털 증거 압수시 표준적인 압수도구와 자료를 활용해야 하고, 디지털 증거를 손상시키거나 파괴할 수 있는 정전기나 자기장을 만들거나 방출할 수 있는 도구나 자료는 피해야만 한다고 기술하고 있다. 그리고 컴퓨터 범죄현장의 복잡성이 초동수사를 담당하는 직원의 전문기술을 초과하는 경우에는 디지털 증거수집에 있어서 훈련을 받고 고급 장비를 다룰 수 있는 직원에게 지원을 요청할 것을 요구하고 있다.[218]

다) 현장 보존과 평가

이 지침서 제3장은 현장보존과 평가와 관련하여 초동수사를 담당하는 사람은 우선적으로 현장에서의 안전을 고려해야 하며, 현장에서 취해지는 모든 조치들이 해당 부서의 정책과 연방법률, 주 법률 등을 준수하도록 요구하고 있다. 절차적으로는 현장과 현장에 있는 모든 사람에 대한 안전조치를 취한 후에는 최초 대응자가 모든 잠재적 증거를 시각적으로 확인하고, 디지털 증거와 물리적 증거의 무결성을 확보해야 하며, 이를 위해 최초 대응자는 가능한 한 빨리 현장에 있는 디지털 증거를 기록하고, 사진찍고, 안전하게 확보해야 한다고 기술하고 있다.[219]

이와 같이 이 지침서는 최초 대응자가 현장을 보존하고 평가함에 있어서 준수해야 할 요건들을 다음과 같이 기술하고 있다.

"ⅰ) 범죄현장 보존을 위한 해당 부서의 정책을 따라야 한다.
ⅱ) 개인용 또는 휴대용 장치를 포함한 모든 전자장치를 즉시 보존해야 한다.
ⅲ) 권한없는 사람이 범죄현장에 있는 전자장치에 접근하지 않도록 해야 한다.
ⅳ) 권한없는 사람으로 부터의 기술적 지원 또는 도움의 제안은 거부해야 한다.
ⅴ) 모든 사람을 범죄현장 또는 증거가 수집되어질 장소로부터 즉시 내보내야 한다.
ⅵ) 어떠한 전자장치도 변경되지 않는 조건을 확보해야 한다.
ⅶ) 만약 이미 전원이 꺼져있는 경우 컴퓨터 또는 전자장치를 분리해야 한다.

---

218) U.S. Dept. of Justice, op.cit., pp. 13-14.
219) U.S. Dept. of Justice, op.cit., p.15.

이 경우 키보드나 마우스 이동 가능한 저장매체 등에 지문이나 DNA 증거가 있을 수 있으므로 이를 보존하기 위한 적절한 조치가 취해져야 하고 기록으로 남아야 한다."[220]

그리고 만약 컴퓨터 전원이 켜져 있거나 전원상태가 확인되지 않는 경우에 최초 대응자가 취해야할 준수사항도 함께 기술되어 있다.

"ⅰ) 컴퓨터가 켜져있는 상태를 나타내는 징후를 보고 들어야 한다. 즉 팬이 돌아가는 소리, 드라이브가 돌아가는 소리를 듣거나 LED가 켜져 있는지를 보고 체크해야 한다
ⅱ) 디지털 증거가 파괴되고 있는 표시를 디스플레이 스크린에서 점검해야 한다.
ⅲ) 원격 컴퓨터 또는 장치로부터 컴퓨터가 접속되어 있는 징후를 관찰해야 한다
ⅳ) 인스턴트 메시지 또는 채팅룸과 같은 다른 컴퓨터 또는 이용자간의 지속적인 통신을 하고 있는 신호를 관찰해야 한다
ⅴ) 모든 카메라 또는 웹캠을 주목하고, 그것이 작동중인가의 여부를 판단해야 한다"[221]

라) 현장기록

이 지침서 제4장은 컴퓨터 범죄현장의 기록에 대한 권고사항을 제공하는 것으로 법률이나 기관의 정책을 대체하고자 하는 것은 아니라는 점을 서두에 밝히고 있다.

범죄현장에 대한 기록은 수사에 관한 기록이기 때문에, 현장 위치, 현장 그 자체, 컴퓨터의 상태, 전원과 조건, 저장매체, 무선 네트워크 장치, 휴대폰, 스마트폰, PDA, 다른 데이터 저장장치, 인터넷과 네트워크 접속, 다른 전자장치 등을 정확히 기록하는 것이 중요하며, 모든 디지털 증거가 컴퓨터나 다른 장치와 가까운 곳에 존재하는 것은 아니라는 것을 인식하고 있어야 한다고 되어 있다.[222] 즉 현장은 복합적인 장소로 확대될 수 있기 때문에 최초 대응자는 컴퓨터 및 다른 전자장치에 대한 모든 물리적 연결장치 그리고 컴퓨터 등에 링크되어 있거나 링크할 수 있는 네트워크 및 무선 접속 포인트를 기록하도록 하고 있다.[223]

---

220) U.S. Dept. of Justice, op.cit., p.16.
221) U.S. Dept. of Justice, op.cit., p.16.
222) U.S. Dept. of Justice, op.cit., p.19.

현장에서 직원은 시리얼 넘버 또는 다른 식별자를 찾기 위해 컴퓨터나 다른 전자장치를 이동해서는 안되는데, 이는 이러한 이동이 컴퓨터 등의 장치에 손상을 초래하거나 그 안에 포함된 디지털 증거를 손상시킬 수 있기 때문에 기본적으로 전원이 차단될 때까지는 이동해서는 안된다고 기술하고 있다.[224]

마) 증거수집

이 지침서는 증거수집의 단계에서 증거를 수색 및 수집할 수 있는 적절한 권한 - Plain view, 동의, 법원명령과 같은 - 이 있어야 한다는 점을 강조하고 있다. 즉, 최초 대응자는 증거를 압수할 수 있는 권한을 확인해야 하며, 기관의 가이드라인을 준수하고 상급자에게 자문을 구하거나 적절한 권한에 관하여 문제가 생긴 경우에는 검사와 접촉하도록 기술하고 있다.[225]

디지털 증거는 물리적 장치의 무결성 뿐만 아니라 그 안에 포함된 데이터의 무결성을 보존하기 위해서 조심스럽게 취급되어야 하며, 경우에 따라 특수한 수집·포장·이송 기술을 요하는 디지털 증거가 있을 수 있다는 점을 명심해야 한다. 특히 휴대폰이나 스마트폰과 같은 통신장비는 일단 증거로서 확인되어 수집되면 데이터의 송수신을 차단하고 확보하도록 요구하고 있다.[226]

이 지침서는 최초 대응자가 접한 상황별로 디지털 증거 수집시 취해야 하는 조치들을 열거하고 있으며, 이에 따르도록 하고 있다. 예시된 상황은 ⅰ) 모니터가 켜있고, 스크린상에 프로그램, 애플리케이션, work product, 사진, 이메일, 인터넷 사이트 등이 디스플레이 되어 있는 경우, ⅱ) 모니터가 켜있고 스크린 세이버 또는 그림이 보이는 경우, ⅲ) 모니터가 켜있지만 마치 모니터가 꺼져있는 것처럼 디스플레이가 아무것도 표시하고 있지 않은 경우, ⅳ) 모니터 전원이 꺼져있고 디스플레이가 아무 표시도 되어 있지 않은 경우, ⅴ) 모니터 켜져 있고 디스플레이가 아무 표시도 되어 있지 않은 경우 등으로 나누어 디지털 증거 수집시 취해야 하는 조치를 단계별로 기술하고 있다.[227]

---

223) U.S. Dept. of Justice, op.cit., p.20.
224) U.S. Dept. of Justice, op.cit., p.19.
225) U.S. Dept. of Justice, op.cit., p.21.
226) ibid.
227) U.S. Dept. of Justice, op.cit., pp.22-23.

또한 이 지침서는 컴퓨터 전원이 켜져 있는 경우와 꺼져 있는 경우로 나누어서, 데스크탑이나 타워, 미니컴퓨터에서 준수해야 할 증거수집절차 그리고 랩탑 컴퓨터에서 준수해야 할 증거수집절차를 기술하고 있다.[228] 이외에 최초 대응자가 디지털 증거를 수집할 필요가 있는 잠재적 입증가치가 있는 기타 전자장치 또는 주변장치의 유형들을 열거하고 있다. 그리고 이와 같이 증거수집단계에서 준수해야 할 절차들을 Flow Chart로 보여주고 있다.[229]

바) 디지털 증거의 포장, 이송, 저장

디지털 증거는 극한기온, 습도, 물리적 충격, 정전기, 자기장에 민감하기 때문에 데이터의 손상이나 변형을 피하기 위해서는 기록, 사진촬영, 포장, 이송, 저장시 예방조치가 취해져야 한다고 기술하고 있다.

먼저 포장절차와 관련하여서는 "ⅰ) 수집된 모든 디지털 증거는 포장하기 전에 적절히 기록하고 라벨을 붙이며, 표시를 하고, 사진을 찍고, 비디오로 기록하거나 스케치하고 목록을 만들어야 한다. ⅱ) 디지털 증거가 잠재적 증거, 흔적 증거, 생물학적 증거를 포함할 수 있기 때문에 이를 보존하기 위한 적절한 조치가 취해져야 한다. 디지털 증거 이미징은 이러한 잠재적 증거, 흔적 증거, 생물학적 증거에 대한 보존조치가 행해지기 전에 이루어져야 한다. ⅲ) 모든 디지털 증거는 정전기 방지 포장상태로 포장해야 한다. ⅳ) 모든 디지털 증거는 휘어지거나 스크래치가 나거나 기타 변형되지 않는 방식으로 포장해야 한다. ⅴ) 디지털 증거가 저장 및 포장된 용기에 라벨을 붙여야 한다. ⅵ) 휴대폰이나 스마트폰은 발견된 당시의 전원상태로 두어야 한다. ⅶ) 휴대폰이나 스마트폰은 그 장치에 의하여 데이터 메시지의 송수신을 차단하기 위해 신호차단소재 - faraday 차단 백, 방사선 차단소재, 알루미늄 호일 등 - 로 포장해야 한다. ⅷ) 압수된 전자장치에 사용된 모든 전원공급 장치와 어댑터를 수집해야 한다."[230] 고 기술하고 있다.

다음으로 이송절차에 관해서는 "ⅰ) 디지털 증거는 자기장으로부터 떨어져 있어야 한다. ⅱ) 디지털 증거를 자동차 안에서 장기간 보관하는 것을 피해야 한다. ⅲ) 컴퓨터

228) U.S. Dept. of Justice, op.cit., pp.24-26.
229) U.S. Dept. of Justice, op.cit., p.29.
230) U.S. Dept. of Justice, op.cit., pp.31-32.

와 전자장치는 이송하는 동안에 충격과 진동으로부터 손상되지 않도록 포장하고 안전하게 보존해야 한다. ⅳ) 디지털 증거의 이송과 이송된 모든 증거에 대한 chain of custody를 유지해야 한다"[231]고 기술되어 있다.

마지막으로 저장절차와 관련하여서는 "ⅰ) 디지털 증거는 기관의 정책에 따라 목록화되어야 한다. ⅱ) 디지털 증거는 극한의 온도와 습도에 노출되지 않는, 안전하고 온도조절장치가 되어 있는 장소 또는 환경에 저장되어야 한다. ⅲ) 디지털 증거는 자기장, 습기, 먼지, 진동, 기타 손상이나 파괴를 유발할 수 있는 것에 노출되지 않아야 한다"[232] 고 기술되어 있다.

사) 범죄유형별 컴퓨터 범죄와 디지털 증거 관련 고려사항

이 지침서는 최초 대응자가 범죄유형별로 잠재적으로 가치 있는 디지털 증거의 출처를 확인하는 것을 돕기 위하여 범죄유형별로 고려해야 할 사항들을 제시하고 있다. 이 경우 컴퓨터 또는 다른 전자장치에 남아있는 지문이나 DNA가 중요할 수 있기 때문에 그러한 증거를 수집해야만 하지만, 그러한 흔적증거나 생물학적 증거를 복구하고 분석하는 행위와 결합된 파괴적인 절차는 디지털 증거나 조사나 분석을 위해 복구될 때 까지 연기되어야 한다고 기술하고 있다.[233]

지침서는 범죄유형별로 잠재적인 디지털 증거를 포함할 수 있는 요소들을 기술하고 있는데, 아동학대 또는 착취, 컴퓨터 침입, 화폐위조, 사망조사, 가정폭력, 협박, 강요, 이메일 협박, 성희롱, 스토킹, 도박, 신원절도(명의도용), 마약, 온라인사기 또는 경제사기, 성매매, 소프트웨어 불법복제, 통신사기, 테러(국토안보) 등이 그것이다.[234]

나. Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors

1) 지침서의 목적

1980년 후반부터 디지털 증거가 범죄를 해결하고 범죄자를 기소하는데 사용되어

231) U.S. Dept. of Justice, op.cit., pp.32-33.
232) U.S. Dept. of Justice, op.cit., p.33.
233) U.S. Dept. of Justice, op.cit.,p.35.
234) U.S. Dept. of Justice, op.cit.,pp. 36-47.

왔지만 판사와 변호사, 배심원들은 디지털 증거의 중요성과 신뢰성에 강한 의구심을 갖고 있다. 따라서 재판에서 사실인정자들의 오해를 막기 위해서는 단순한 용어와 신중하게 선택된 보조도구를 가지고 그 개념이 설명되어야 한다는 것 그리고 검사와 수사관이 증거를 복구하고 분석하는데 직면한 문제들을 완전히 이해해야 하며, 조사관과 기술적 문제에 대한 지식을 공유하고 전략을 논의해야 한다[235]는 점을 인식해야 한다는 전제하에서, 이 지침서는 디지털 증거와 관련한 기술적·법률적 핵심쟁점을 다루고 있다.

2) 압수와 수색 문제

이 장에서는 디지털 증거의 수집과 사용에 직접 적용되는 연방 헌법, 법률들을 검토하고 있다. 즉 디지털 증거의 수집과 관련하여 국회가 특별히 취급할 가치가 있다고 인정한 정보에 대한 접근과 공개에 적용되는 연방법령, 즉 Wiretap Act, Pen Regster and Trap and Trace Statute, Stored wire and Electronic Communication Act, Privacy Protection Act, 그리고 수정헌법 제4조에 적용되는 원칙을 다루고 있다. 만약 이러한 법률을 위반하는 경우에는 디지털 증거의 증거능력이 훼손되거나 민사소송의 대상이 될 수 있다고 기술하고 있다.[236]

가) 연방 도청법(Wiretap Act)

도청법(18 U.S.C. §2510 et seq.)은 전송중에 통신내용을 도청하는 것에 중점을 두는 법률로, 미국내에서 유선전화·대화 및 전자통신의 내용을 도청하는 것을 금지하고 있다. 즉 법률상 예외조항이 적용되지 않는 한, 사적인 통신에 참여하고 있는 당사자가 아닌 사람이 전자적·기계적 또는 다른 장치를 사용하여 통신에 참여하고 있는 당사자들 간의 통신을 도청하는 것을 금지하고 있다.[237] 도청할 수 있는 권한을 부여하는 관할법원의 명령서 발급이 있는 경우에는 예외에 해당한다.

도청법 위반은 민·형사상 책임을 초래할 수 있으며, 정부기관의 직원이 위반한 경우에는 증거배제의 결과를 초래할 수 있기 때문에, 감시할 통신이 도청법에 규정된

235) U.S. Dept, of Justice, Digital Evidence in the Courtroom; A Guide for Law Enforcement and Prosecutors, NIJ Special Report, 2007, p.xi.
236) U.S. Dept, of Justice, Digital Evidence in the Courtroom; A Guide for Law Enforcement and Prosecutors, NIJ Special Report, 2007, p.1.
237) ibid.

보호되는 통신 가운데 하나인지의 여부 그리고 하고자 하는 감시가 통신의 도청에 해당하는지의 여부에 대하여 판단해야만 한다.[238]

나) Pen/Trap 법률

Pen Register and Trap and Trace 법률(18 U.S.C. §3121 et seq.)은 통신과 관련한 전화번호, 통신경로, 주소지, 신호정보의 실시간 획득을 규제하는 법률이다. 도청법이 통신내용의 획득을 그 대상으로 하는 반면에, Pen/Trap 법률은 통신내용의 획득을 포함하지 않으며 통신에 관한 정보를 그 대상으로 한다.[239] Pen/Trap 법률은 전화와 인터넷 통신에 적용되며, 예외조항이 적용되지 않는 한 누구든지 유선통신 또는 전자통신에 관한 비내용적 정보를 동의 없이 실시간으로 획득하는 것을 금지한다.[240] 따라서 이러한 금지에 대한 예외조항이 적용되지 않는 경우, 법집행기관은 동 법률에 포함된 비내용적 정보를 획득하기 전에 법원으로부터 Pen/Trap 명령을 받아야만 한다.[241]

다) 전자통신 프라이버시 보호법(Electronic Communications Privacy Act)의 저장된 통신 조항

ECPA의 저장된 통신에 관한 장(18 U.S.C.§2701 et.seq.)은 통신서비스제공자의 가입자와 고객의 프라이버시 보호를 규정하고 있다. 이 법률은 고객과 가입자를 위해 통신서비스제공자에 의해 저장된 파일 뿐만 아니라 기록들을 보호한다. ECPA는 통신서비스제공자의 유형에 따라, 제공자로 하여금 법집행기관에 가입자와 고객의 구체적인 정보의 유형을 공개하도록 강제하는데 필요한 법적 절차의 유형을 규정하고 있다.[242] 또한 ECPA는 획득하고자 하는 정보의 유형에 따라 필요한 법적 요구사항으로서 소환장(Subpoena), 법원명령(18 U.S.C.§2703 하의 Court Order), 수색영장(search warrant) 등으로 구분하여 민감한 정보일수록 이를 획득하기 위한 법적 절차를 강화하고 있다(소환장<법원명령<수색영장 순).[243] 따라서 소환장으로는 고객이나

238) U.S. Dept, of Justice, Digital Evidence in the Courtroom; A Guide for Law Enforcement and Prosecutors, NIJ Special Report, 2007, p.2.
239) U.S. Dept, of Justice, op.cit., p.2.;18. U.S. Code §3121(c).
240) ibid. ;18. U.S. C. §3121(b).
241) ibid.; 18. U.S. C. §3121(a).
242) U.S. Dept, of Justice, Digital Evidence in the Courtroom; A Guide for Law Enforcement and Prosecutors, NIJ Special Report, 2007, p.3.

가입자의 신원에 관한 정보와 기본적인 기간내 접속기록 등을 요구할 수 있으며, 법원명령에 의해서는 기타 비내용적 가입자 정보와 고객 또는 가입자의 서비스 이용에 관한 상세한 기록 등을 요구할 수 있다.[244] 마지막으로 저장된 통신의 내용은 그 내용을 고객이나 가입자가 열람한 경우에는 소환장으로 가능하지만, 열람하지 않은 경우에는 수색영장에 의해서만 확보할 수 있도록 하고 있다.[245]

라) 프라이버시 보호법(Privacy Protection Act)

프라이버시 보호법(42. U.S.C §2000aa et seq.)은 법집행기관이 공개적인 배포를 목적으로 보유하고 있는 자료를 압수하거나 수색하기 위해 수색영장을 활용하는 것을 제한하고 있다. 이 경우 보호되는 자료는 '작업결과물(work product;저자나 출판사가 작성한 자료)'과 '기록자료(documentary materials; 작업결과물을 기록하거나 지원한 모든 자료)'이다.[246]

따라서 해당 자료가 PPA의 보호대상이면, 법집행기관은 그것을 확보하기 위해 수색영장을 사용할 수 없지만, ⅰ) 수색 또는 압수할 자료가 범죄의 수단 또는 결과물이거나 금제품인 경우, ⅱ) 그러한 자료의 즉각적인 압수가 사망 또는 심각한 신체적 상해를 막는데 필요하다고 믿을만한 합리적인 이유가 있는 경우, ⅲ) 그러한 자료를 보유한 사람이 그 자료와 관련된 범죄를 범했거나 범하고 있다고 믿을만한 합리적인 이유가 있는 경우에는 수색영장 사용금지조항이 적용되지 않는다.[247]

마) 헌법적인 문제

다른 증거와 마찬가지로 디지털 증거의 수색에 대해서도 연방과 주 헌법상의 압수수색에 관한 법률과 법원규칙이 적용되므로, 수정헌법 제4조에 의한 보호를 받는다. 따라서 일반적으로 법집행기관은 영장요건의 예외사항 - 동의, 긴급한 상황, 체포에 수반한 수색, 보관물품의 수색, plain view 원칙 -이 적용되지 않는 한 반드시 영장을

---

243) ibid.
244) U.S. Dept, of Justice, Digital Evidence in the Courtroom; A Guide for Law Enforcement and Prosecutors, NIJ Special Report, 2007, pp. 4-5.
245) U.S. Dept, of Justice, Digital Evidence in the Courtroom; A Guide for Law Enforcement and Prosecutors, NIJ Special Report, 2007, pp. 5-7.; 18. U.S.C. §2703(a).
246) U.S. Dept, of Justice, op.cit., p.7.
247) ibid.

발부받아야 한다.[248]

바) 특권 또는 특허 정보

일정한 경우 법집행기관이 수색을 할 장소에 성문법 또는 보통법하에서 특권이 부여된 것으로 간주되는 정보가 있다고 믿을만한 이유가 있는 경우, 영장을 작성하여 수색을 하기 전에 법집행기관은 관할지역에 부과된 법적 한계를 확인하고 준수하도록 주의해야만 한다.[249]

사) 주 밖에 있는 기록의 확보

법집행기관이 확보하고자 하는 기록을 갖고 있는 ISP가 주 밖에 위치한 경우가 있을 수 있는데, 이 경우 판사가 관할지역을 넘어서는 집행영장을 발부하기를 거부할 수 있으며, 설령 집행영장이 발부되었다고 하더라도 주 밖에서 증거를 보유한 자가 주 밖에서 발행된 집행영장을 존중하지 않을 수 있다는 문제가 있다. 특히 ISP의 경우 합법적인 구속력이 없는 주 밖에서 발행된 집행영장에 따라 정보를 공개하게 되면 ECPA하에서의 책임을 부담해야 하는 문제가 있기 때문에 집행영장에 따라야 할 법적 의무가 없는 것으로 여긴다.[250]

이와 같이 주 밖에 있는 기록을 확보하기 위한 방안으로서, 먼저 검찰이 법원으로 하여금 집행영장 발부를 설득하는 것이고, 이에 의해 수색영장을 정당하게 발부받게 되면 법집행기관은 주 밖에 있는 기록을 보유한 사람을 설득하는 것이다. 즉 합법적인 수색영장하에서 선의를 가지고 그 절차를 신뢰한 기업은 ECPA하에서 제기될 수 있는 민형사상 소송에 대해 완벽히 방어할 수 있다고 설명하는 것이다.[251]

만약 판사가 주 밖에 있는 기록에 대한 수색영장 발부를 거부하거나 수령인이 영장 집행을 거부하는 경우에는, 재판 소환장(trial subpoena), 관할권 제한을 받지 않는 대배심(Grand Jury) 또는 다른 수사 소환장(investigative subpoena), 형사절차상 주 밖에 있는 증인의 출석을 보장하기 위한 통일법(Uniform Act to Secure the Attendance of Witness From Without a State in Criminal Proceedings:Uniform

248) U.S. Dept, of Justice, op.cit., pp. 8-10.
249) U.S. Dept, of Justice, op.cit., p.11.
250) U.S. Dept, of Justice, Digital Evidence in the Courtroom; A Guide for Law Enforcement and Prosecutors, NIJ Special Report, 2007, p.12.
251) U.S. Dept, of Justice, op.cit., p.13.

Act)과 함께 사용된 재판 또는 대배심 소환장 등과 같은 방안을 고려해야 한다. 특히 Uniform Act의 경우 판사는 이 법에 의거하여 소환장을 발부할 권한이 있고, 수령인은 반드시 응하도록 되어 있기 때문에 법의 위력을 충분히 발휘할 수 있는 장점이 있지만, 절차에 소요되는 시간이 많으며 재판이 진행되어야 비로소 기록을 획득할 수 있다는 문제가 있다.

3) 디지털 증거의 무결성, 개시, 공개(Integrity, Discovery and Disclosure of Digital Evidence)

가) 예비 조사(Preliminary Inquiries)

경우에 따라 디지털 증거가 법집행기관에 의해 확보되기 전에 고의 또는 과실로 변경될 수 있는데, 이러한 경우 조사를 위해 검찰로 넘겨진 증거는 결국 절차의 연속성과 신뢰성을 확보하지 못한 채 활용될 수 없게 된다.[252] 따라서 법집행기관에 증거를 제공하는 사람에게 일정한 예비질문을 해야 할 필요가 있으며, 이러한 예비질문을 통해 제공된 증거에 관한 필수적인 근거가 제공될 수 있다.[253] 이러한 증거의 신뢰가능성과 설득력은 여전히 사실인정자 - 판사 또는 배심원 -에 의해 평가되어야만 한다.[254]

나) 데이터의 무결성(Integrity of data)

디지털 증거의 허용가능성과 설득력(증명력)을 위해서는 그것이 법집행기관에 의해 확보된 것이든 민간 증인 또는 피해자로부터 확보된 것이든 간에, 매체로부터 확보된 정보가 진실한 것이고 원본 데이터를 정확히 재현한 것이라는 것이 법정에서 입증되어야 한다.[255]

절차의 연속성(chain of custody)은 물리적 물품 그 자체에 대한 것과 그것과 결합된 데이터 양자에 모두 요구되는 것이다. 일반적으로 그리고 특히 디지털 증거에 있어서는 절차의 연속성(chain of custody)과 관련하여 인증표준, 실험실 정책, 절차

252) U.S. Dept, of Justice, op.cit., p.15.
253) U.S. Dept, of Justice, op.cit., p.16.
254) ibid.
255) U.S. Dept, of Justice, Digital Evidence in the Courtroom; A Guide for Law Enforcement and Prosecutors, NIJ Special Report, 2007, p.16.

및 기타 다른 가이드라인을 명확히 인식하고 있어야 한다.[256]

증거획득과 조사과정에서 데이터의 무결성을 확보하기 위해서는, 법집행기관이 참여하기 전에 수집된 증거의 유형, 증거를 취급한 사람의 이름과 직위 및 법집행기관에 제공하기 전까지 증거를 통제한 사람의 신원, 디지털 증거를 수집하고 저장한 도구나 방법 및 수집 후 증거에 접근한 사람의 신원, 증거가 수집된 일시, 증거수집시 증거가 발견된 장소 등에 대한 질문에 대하여 답을 해야만 한다.[257]

다) 입증할 기록의 작성(Building the record to make the case)

증거의 허용가능성과 설득력을 확보하기 위해서는 증거를 정확하고 철저하게 기록하는 것이 중요하다. 따라서 법집행기관은 데이터의 획득, 조사, 저장을 위해 취한 조치들을 포함하여 데이터에 관련하여 취해진 모든 조치들을 철저하게 기록해야만 한다.[258] 조사기록과 관련하여서는 기록의 준비와 보관과 관련한 기관의 정책을 준수하고, 보유한 기록들은 개시될 수 있으므로 이를 리뷰할 기회를 고지하고 제공해야 하며, 다른 사건의 기록과 혼합해서는 안된다는 점을 염두에 두어야 한다.

라) 원본 증거의 반환(Returning original evidence)

전자증거를 압수당한 자는 조사가 시작되었는가의 여부와 상관없이 그 반환을 요구할 수 있다. 하지만 압수된 데이터가 금제품이면 그 매체를 반환하는 것이 적절한지 여부를 고려해야 하고, 만약 법원이 원본을 피고측에 반환해서는 안된다고 판단한 경우에는 원본 또는 포렌식 복제본에의 접근을 피고인에게 제공할 필요가 있을 수 있다. 사전에 피고측에 압수된 증거에 대한 적절히 통제된 접근을 제공할 수 있도록 준비해야 한다.[259]

증거가 반환되어지는 경우에는 진정성, 정확성, 소유권, 전문증거, 절차의 연속성과 같은 잠재적으로 논쟁될 수 있는 쟁점들에 관하여 반드시 약정을 요구해야 하는데, 약정은 피고인으로부터 확보되어야 한다.[260]

---

256) ibid.
257) U.S. Dept, of Justice, op.cit., P.17.
258) U.S. Dept, of Justice, op.cit., P.18.
259) U.S. Dept, of Justice, op.cit., P.19.
260) U.S. Dept, of Justice, op.cit., P.20.

마) 피고측에 증거를 개시할 의무(Obligation to disclose evidence to the defense)

증거개시원칙은 검찰로 하여금 지속적으로 피고측에 증거를 제공할 의무가 있다는 것이다. 피고측 변호인은 피고측 조사관이 분석하기 위해 증거에의 접근을 강제할 수 있다.[261]

일반적인 증거개시에 있어서는 피고측에게 디지털 증거의 복제본을 제공하거나 그 조사에 편의를 제공해야 한다. 또한 검찰은 무죄를 입증하는 자료를 확인·보존할 의무 그리고 피고측에 제공할 의무가 있는데, 이러한 의무는 관할권에 따라 차이가 있지만 최소한 무죄를 증명하는 증거가 공판전에 발견될 때에는 피고측에 활용할 수 있도록 해야만 한다.[262]

4) 법정제출과 증거법칙

디지털 증거의 제출은 전문적이고, 발전중인 기술 그리고 때로는 복잡한 기술에 익숙할 것을 요하기 때문에, 조사관과 검사는 일반적인 디지털 증거의 기술적인 기본 동작에 관한 지식을 알아야 하고, 그 사건의 구체적인 기술적 세부사항을 이해해야만 한다.[263]

따라서 재판전에 준비해야 할 사항으로는, 크게 ⅰ) 현재까지 조사의 범위를 리뷰할 때 검찰이 고려해야 할 필요가 있는 예비적 고려사항, ⅱ) 검사와 수사관 그리고 조사관간의 재판전 효율적인 의사소통, ⅲ) 입증문제(진정성과 전문법칙) 등으로 나누어 검토해야 한다.

가) 예비적 고려사항

디지털 증거를 수반하는 사건을 지정받은 검사의 첫 번째 임무 가운데 하나는 수사의 범위를 리뷰하는 것으로, 사실인정자(판사, 배심원)에게 그 사건에 대한 이해가능한 이론을 준비하여 제시해야 하고, 기술적 문제의 본질 - 디지털 증거가 첨단기술범죄와 관련이 있는가, 관련은 없지만 디지털 증거가 사건의 중요한 부분에 해당하는가 아니면 단순히 그 사건을 조사하는데 포함되어 있는 것인가 -을 정확히 해야 한다.[264]

---

261) ibid.
262) ibid.
263) U.S. Dept, of Justice, Digital Evidence in the Courtroom; A Guide for Law Enforcement and Prosecutors, NIJ Special Report, 2007, p.23.
264) ibid.

다음 고려사항은 그 사건에서 디지털 증거의 출처와 특성을 확인하고 설명하는 것이며, 추가적인 출처를 조사해야하는지에 대한 고려와 모든 적절한 기소유형에 대한 고려 등이 행해져야 한다.

나) 재판전 의견교환

디지털 증거를 조사하는 단계에서 검사, 수사관 조사관은 재판전에 사건을 제출할 계획을 수립하기 위해 회의를 해야 한다. 이 단계에서 검사가 고려해야 할 사항은 다음과 같다. ⅰ) 명확히 해야 할 모든 요소 그리고 추가분석 또는 추가 조사가 필요한 부분에 대한 논의, ⅱ) 사건에 대한 법이론, 기소된 범죄의 구성요건, 모든 예측가능한 변론 등을 명확히 하기 위한 조사관 및 수사관과의 재판전 회의 실시, ⅲ) 직접 심문과 교차 심문의 가능한 범위와 방향에 대한 조사관 및 수사관과의 리뷰, ⅳ) 디지털 증거의 유형의 구분(실질적 증거와 설명 증거)

다) 증거에 대한 고려사항

증거법칙은 관할권마다 다르지만 대다수의 주 들은 연방증거법의 모델을 따르고 있다. 디지털 증거는 관련성, 진정성, 전문법칙과 같은 문제를 제기할 수 있는데, 이는 디지털 증거 그 자체 뿐만 아니라 그 증거를 제출하는 전문가 증언 및 그와 결합된 입증문제를 수반할 수 있다.

증거에 관한 고려사항은 디지털 증거의 특성과 출처에 의해 영향을 받을 수 있으므로, 입증요건의 정의, 컴퓨터에 저장된 실질 증거, 컴퓨터가 생성한 실질 증거, 재판을 위해 준비된 컴퓨터에 의해 생성된 실질증거와 설명증거, 전문가 증언 등을 논의할 필요가 있다.

ⅰ) 입증요건과 관련해서는 관련성(Relevance) 검토(연방증거법 제401조[265]), 진정성(Authentication) 검토(연방증거법 제901(a)[266]), 전문증거(Hearsay)(연방증거법 제801(c)[267] 등을 고려해야 한다

265) 증거는 (a) 그것이 없는 경우보다는 있는 경우에 어떤 사실의 판단에 더 혹은 덜 도움이 되고, (b) 그 사실이 소송의 진행과정 결정에 있어 의미를 가지는 사실일 때, 관련성이 있다.; FRE Rule 401(Test for Relevant Evidence).

266) (a) 원칙 : 증거를 제출하고자 하는 자는 그 증거가 자신이 제출하고자 의도하는 것과 동일한 진정성 있는 증거임을 입증해야 한다; FRE 901(a)(Authenticating or Identifying Evidence)

ii) 컴퓨터에 저장된 실질 증거와 관련하여서는 컴퓨터 저장기록의 가장 일반적 전문증거 예외조항(제803(6)[268])에 의거한 입증방법을 고려할 수 있으며, 컴퓨터에 저장된 실질 증거의 인쇄물에 대해서는 best evidence rule(연방증거법 제1002조[269], 제1003조[270])에 따른 원본 요건과 요약서 제출(연방증거법 제1006조)[271] 등을 고려해야 한다.

iii) 컴퓨터가 생성한 실질증거와 관련해서는 연방증거법 제901(b)(9)[272]을 고려할 필요가 있다.

iv) 재판을 위해 준비된 컴퓨터에 의해 생성된 실질증거와 설명증거와 관련해서는 적절성 여부(연방증거법 제403조)[273], 전문법칙의 예외조항(연방증거법 제803(1)조[274], 제803(6)조[275], 제803(8)조[276], 제807조[277], 제703조[278] 등)에

---

267) (c) 전문증거: 전문증거란 (1) 진술자가 현재 재판이나 준비기일에서 증언을 하는 중에 말한 것이 아닌 진술로서, (2) 당사자 중 일방이 그 진술내용의 진위를 입증할 목적으로 제출한 진술을 말한다; FRE Rule 801(c).

268) (6) 일상적인 업무기록 : 일상적인 행동이나 사건, 상황, 의견 또는 진단에 대해 (A) 당시 상황을 알고 있는 자가 직접 기록하거나 그로부터 정보를 받아서 즉시 또는 약간의 시차를 두고 한 기록, (B) 회사, 조직, 직업, 영리 또는 비영리 업무의 수행중에 정기적으로 행한 기록 그리고, (C) 기록을 남기는 것이 그 업무 중의 하나인 경우의 기록, (D) 이상과 같은 조건은 기록 보관자나 기타 자격을 갖춘 증인의 증언, 제902(11)조 또는 제902(12)조에 정한 확인서 또는 다른 법에서 정한 확인서에 의해서 입증할 수 있다, (E) 반대 당사자는 정보의 출처, 기록 방법, 기록 작성 상황에 신빙성이 없다는 점을 지적하여 본 규칙에 정한 기록의 증거능력에 이의를 제기할 수 있다.

269) 본 규칙과 연방법률에서 달리 정한 경우를 제외하고는 그 내용을 증명하기 위해서는 글이나 기록, 사진의 원본을 제출해야 한다; FRE Rule 1002(Requirement of the Original)

270) 원본의 진정성이나 사본 작성과정에서 결함이 있어서 사본을 증거로 하는 것이 정의에 반하는 경우를 제외하고는 사본은 원본과 같은 증거능력이 있다.; FRE Rule 1003(Admissibility of Duplicates).

271) 증거를 제출하고자 하는 자는 글이나 기록, 사진의 분량이 너무 커서 법정에 제출하기 적당하지 않은 경우에는 요약서, 차트, 계산서 등으로 내용을 입증할 수 있다. 이 경우 증거를 제출하고자 하는 자는 상대방이 원본이나 사본을 검증하거나 복사할 기회를 주어야 하며, 법원은 원본이나 사본을 법원에 제출할 것을 명할 수 있다; FRE Rule 1006(Summaries to Prove Content)

272) 프로세스 또는 시스템에 관한 증거 : 프로세스 또는 시스템을 증거로 하기 위해서는 설명을 통해 그 절차나 구조가 정확한 결과를 도출한다는 점을 입증해야 한다; FRE Rule 901(b)(9)(Evidence about a process or system).

273) 법원은 증거의 증명력 보다 부당한 편견, 쟁점의 혼동, 배심원에 대한 호도, 불필요한 지역이나 시간낭비, 증거의 중복으로 인한 폐해가 훨씬 더 큰 경우에는 관련성있는 증거의 증거능력을 인정하지 않을 수 있다.; FRE Rule 403(Excluding Relavant Evidence for Prejudice, Confusion, Waste of Time, or Other Reasons)

274) 다음 진술은 진술자의 출석가능성 여부와 상관없이 전문법칙의 예외로서 증거능력이 있다. (1) 지각한 것의 즉각적인 표현 : 어떤 사건이나 상황을 설명하거나 묘사하는 진술로서 진술자가 지각과 동시에 혹은 지각한 후에 바로 행한 진술; FRE Rule803(1)(Exceptions to the

의 해당 여부를 검토해야 한다.

v) 전문가 의견의 진술과 관련해서는 두 개의 중요한 판정법이 있는데, Frye Test[279]와 Daubert Test[280]이다. Daubert test는 연방법원에서 적용되는데, 이는 사실심 법원이 '쓰레기 과학'의 인정을 억제하기 위한 문지기로서 역할을 하며, 신뢰할 수 있는 과학적·기술적 포렌식 기법을 개발하도록 촉구하는 연방대법원의 제안이었다. 이후 과학분야로 엄격히 제한되던 Daubert test가 Kumho Tire Co. Ltd v. Carmichael 판결에 의해 기술분야로 확장되었다.[281] 하지만 여전히

Rule Against Hearsay-Regardless of Whether the Declarant Is Available as a Witness)

275) 일상적인 업무의 기록 : 일상적인 행동이나 사건, 상황, 의견 또는 진단에 대해 (A) 당시 상황을 알고 있는 자가 직접 기록을 하거나 그로부터 정보를 받아서 즉시 또는 약간의 시차를 두고 한 기록, (B) 회사, 조직, 직업, 영리 또는 비영리 업무의 수행중에 정기적으로 행한 기록; 그리고 (C) 기록을 남기는 것이 그 업무중의 하나인 경우의 기록, (D) 이상과 같은 조건은 기록보관자나 기타 자격을 갖춘 증인의 증언, 제902(11)조 또는 제902(12)조에 정한 확인서 또는 다른 법에서 정한 확인서에 의해 입증할 수 있다.(E) 반대 당사자는 정보의 출처, 기록방법, 기록작성상황에 신빙성이 없다는 점을 지적하여 본 규칙에 정한 기록의 증거능력에 이의를 제기할 수 있다; FRE Rule 803(6)(Exceptions to the Rule Against Hearsay-Regardless of Whether the Declarant Is Available as a Witness).

276) 공공문서: 공공기관의 진술 혹은 기록이 (A)(ⅰ) 그 공공기관이 활동의 기록이면서, (ⅱ) 기록의무에 근거해서 관찰한 사실을 포함하고 있을 경우에는 증거능력이 있다. 단, 형사사건에서 법집행기관이 인지한 사실을 기록한 경우에는 그러하지 아니하다.(ⅲ) 수사권을 부여받은 기관이 인지한 사실은 민사사건에서 증거로 사용할 수 있고, 또 형사사건에서 정부측에 불리한 증거로 사용할 수 있다. (B) 단, 반대 당사자가 본 규칙에 기록된 정보의 출처나 기타 정황상 신빙성에 문제가 있다는 점을 입증한 경우에는 그러하지 아니하다.; FRE Rule 803(8) (Exceptions to the Rule Against Hearsay-Regardless of Whether the Declarant Is Available as a Witness).

277) 포괄적 예외 : (a) 원칙: 다음의 경우는 전문증거가 제803조 내지 제804조에 따라 전문법칙의 예외로 인정받지 못하는 경우에도 전문증거라는 이유로 증거에서 배제되지 않는다. (1) 신용성의 정황적 보장이 있고, (2) 쟁점사실에 대한 증거이며, (3) 진술의 제출자가 상당한 노력을 기울여 확보할 수 있는 다른 증거보다 쟁점사실을 증명하는 효과가 뛰어나고, (4) 그 진술의 증거능력을 인정하는 것이 본 규칙과 정의의 관점에서 바람직하다고 판단되는 진술 (b) 고지: (a)항에 정한 진술의 증거능력을 인정하기 위해서는 제출자가 상대방에 게 증거제출 계획, 진술자의 이름 및 주소 등 관련 사실을 고지하여 상대방이 그에 대해서 미리 대비할 기회를 주었어야 한다.;FRE Rule 807(Residual Evidence).

278) 전문가증인은 의견을 형성함에 있어 개인적으로 지각한 사건 관련 사실이나 자료를 근거로 할 수 있고, 특정분야에서 알려진 사실이나 자료 자체는 증거능력 이 없더라도 그 사실이나 자료를 기초로 한 전문가증인의 의견은 증거능력이 있다. 이 경우 의견 형성의 기초가 된 자료나 사실을 배심원에게 공개함으로써 배심원이 전문가의 의견을 이해하는 데 도움 되는 효과가 그 공개로 인한 부정적 효과보다 월등하게 큰 경우에만 전문가증인은 사실이나 자료를 배심원들에게 공개할 수 있다.: FRE Rule 703(Bases of Expert's Opinion Testimony)

279) Frye v. U.S. 54 App. D.C. 293 F.1013(1923)

280) Daubert v. Merrell Dow Pharmaceuticals, 509 U.S. 579(1993).

281) U.S. Dept, of Justice, Digital Evidence in the Courtroom; A Guide for Law

많은 주들이 Frye test를 활용하고 있다.[282]

5) 디지털 증거의 프레젠테이션

디지털 증거가 포함된 재판은 디지털 증거의 허용가능성에 관한 법률적 문제의 제기와 아울러 법정에서 디지털 증거에 대한 검사의 설명에 복잡하거나 익숙하지 않은 용어나 개념이 수반되는 문제가 있다. 따라서 사건 프레젠테이션에 관한 세심한 계획수립과 전체에 걸쳐 디지털 증거가 어떻게 활용되는가가 재판의 성공적인 결과에 필수적인 요소라 할 것이다.[283]

디지털 증거가 수반된 사건을 어떻게 설명하거나 보여줄 것인가에 대한 지침은 다음과 같다.

가) 청중에 대한 교육

사건이 복잡하면 소송과정의 모든 단계에서 판사와 배심원 모두를 교육시켜야 한다. 이와 같이 청중이 최소한의 능력을 보유하도록 하거나 이해시키는 것이 중요하지만 그들을 전문가로 만들려고 시도해서는 안된다.[284]

나) 입증 또는 반박을 위해 필요한 것

디지털 증거를 수반하는 사건에서 검사는 증거에 대한 합당한 해석을 통해 배제할 수 있거나 배제해야 하는 것을 결정해야 한다. 이 경우 ⅰ) 기술적인 이상 현상 즉 비용상의 문제로 또는 운영체제의 복잡성으로 인한 버그나 결함을 의심없이 받아들이는 전문가의 해석에 대한 반박가능성, ⅱ) 사건의 다른 부분에 미치는 중요도에 따른 반박대상의 선정, ⅲ) 변론에 대한 적시성 등을 고려해야 한다.[285]

다) 전문가 증인과 기술적 증거

판사들은 기술적인 증언을 할 경우 전문가 자격을 요구할 수 있기 때문에 수사를 지원하고 재판에서 증언할 검찰측 증인으로서 전문가를 선택할 때는 전문가 단체에 관련 분야의 전문기술이 존재하는지 여부, 전문가 후보가 그 단체에서 어떻게 평가되

Enforcement and Prosecutors, NIJ Special Report, 2007, p.38.

282) ibid.

283) U.S. Dept, of Justice, op.cit., p.39.

284) ibid.

285) U.S. Dept, of Justice, op.cit., p.40.

는지를 판단해야 한다.[286] 그리고 검사는 증거법칙과 절차가 전문가의 관찰과 결론의 허용가능성, 발견가능성, 유용성에 어떻게 영향을 미치는지를 전문가가 이해하고 있는지 확인해야 한다.[287]

검찰은 Daubert 또는 Frye test에 따른 이의제기에 대처하기 위하여 증인을 준비해야 하는데, 이 경우 고려해야 할 사항으로는 직접 심문을 위한 준비와 교차심문을 위한 준비로 구분한다.[288]

라) 복잡하고 기술적인 쟁점에 대한 프레젠테이션

복잡한 디지털 증거 또는 복잡한 사건을 설명하는데 유용한 방법으로는, ⅰ) 기술적 용어와 개념을 배심원이 쉽게 이해할 수 있도록 정의하는 것, ⅱ) 복잡한 시스템 또는 개념을 설명하기 위해 사진·그림·그래프 등을 활용하는 것, ⅲ) 초기 변론과 후속 증인의 증언을 통해 배심원의 지식을 확립하는 것, ⅳ) 프레젠테이션에 관한 기술적인 우려사항들을 재검토하는 것 등이 있다.[289]

마) 최후변론

디지털 증거 사건에서 최후변론을 할 때 기억해야 할 핵심사항은 다음과 같다.[290]

ⅰ) 비디지털 증거보강을 위한 디지털 증거의 제시

ⅱ) 증거와 복잡한 쟁점에 대한 재검토

ⅲ) 배심원이 새로 익힌 기술적 지식의 관점에서 증거의 중요성을 설명하고 명확하지 않은 것을 연결하는 것

ⅳ) 배심원이 상당한 컴퓨터 지식 또는 경험을 가지고 있는 경우, 증거의 중요성이 설명되는 최후변론 과정에서 배심원과 연결고리를 만드는 것

---

286) U.S. Dept, of Justice, op.cit., p.41.
287) ibid.
288) U.S. Dept, of Justice, op.cit., pp.42-43.
289) U.S. Dept, of Justice, op.cit., p.48.
290) U.S. Dept, of Justice, op.cit., p.50.

다. Forensic Examination of Digital Evidence: A Guide for Law Enforcement

1) 목적과 원칙

이 지침서는 법집행기관이 독자적인 정책과 절차를 개발하는데 도움을 주기 위한 것이며, 준수해야할 강제사항은 아니기 때문에 개별사건에 따른 상황 그리고 연방과 주 법률의 적용으로 인해 이 지침서와 다르게 수행할 수 있다.[291]

디지털 증거를 취급할 때는 다음과 같은 일반적인 포렌식 원칙과 절차가 적용되어야 한다.

ⅰ) 디지털 증거를 수집하고 보존하기 위해 취해진 조치들이 증거의 무결성에 영향을 미쳐서는 안된다.
ⅱ) 디지털 증거의 조사를 행하는 사람은 그 목적을 위해 훈련을 받아야만 한다.
ⅲ) 압수·조사·저장 또는 디지털 증거의 이전과 관련한 활동들은 기록되고, 보존되고, 리뷰를 위해 활용 가능해야 한다.

디지털 증거가 처리되는 방식은 사건의 범위를 고려한 디지털 증거의 평가(Assessment), 무결성을 보호하고 보존하는 방식에 의한 획득(Acquisition), 디지털 증거를 추출하고 분석하는 조사(Examination), 복구된 데이터에 대한 해석과 그것을 논리적이고 유효한 형태로 만드는 분석(Analysis), 포렌식 전과정에 걸쳐 수행된 행위와 관찰에 대한 기록과 보고(Documenting and Reporting)으로 이루어진다.

이 지침서는 디지털 포렌식에 대한 이와 같은 원칙과 방식을 토대로 컴퓨터 포렌식 조사를 시행하는데 필요한 기본적인 단계이자 수행되어야 하는 순서를 5가지 제안하고 있다. ⅰ) 정책과 절차의 개발, ⅱ) 증거 평가, ⅲ) 증거 획득, ⅳ) 증거 조사, ⅴ) 기록과 보고 가 그것이다.

2) 정책 및 절차의 개발

원칙 : 컴퓨터 포렌식 분야는 특별히 훈련을 받은 직원, 관리지원, 부서운용을 유지

---

291) U.S. Dept. of Justice, Forensic Examination of Digital Evidence: A Guide for Law Enforcement, NIJ Special Report, 2008, p.1.

하기 위해 필수적인 예산을 요한다. 이는 조사관을 위한 포괄적인 훈련 프로그램, 유효한 디지털 증거 복구 기술, 고도화된 부서 운영을 최대한 효율적으로 유지할 책무를 구성함으로써 이루어질 수 있다.[292]

절차 : 기관은 컴퓨터 포렌식 부서의 설립과 운영에 관한 정책과 절차를 개발해야 한다.[293]

규약과 절차(Protocols and Procedures)로는 다음의 내용들이 포함되어 있다.

"ⅰ) 부서기능이 효과적으로 수행될 수 있도록 부서의 핵심기능 - 첨단기술범죄수사, 증거수집, 포렌식 분석 등-을 구체화하는 업무 명세서 개발(Mission Statement),

ⅱ) 컴퓨터 포렌식 부서 구성원의 자격 요건에 대한 정의(Personnel),

ⅲ) 소프트웨어 사용권한·자원배정·지속적인 교육훈련 등과 관련한 관리적 고려사항(Administrative Considerations),

ⅳ) 포렌식 서비스 요청절차와 디지털 증거조사를 위해 채택된 요청의 수용절차 확립을 위한 가이드라인 개발(Service request and intake),

ⅴ) 조사의 우선순위와 배정에 대한 기준 결정 및 시행(Case Management),

ⅵ) 증거의 수령·절차·기록·취급 및 조사와 결합된 결과물에 관한 가이드라인 확립(Evidence handling and retention),

ⅶ) 디지털 증거의 보존과 처리를 위한 표준운영절차 (Standard operating procedure)의 개발(Case processing),

ⅷ) 획득된 결과가 타당하고 독립적으로 재연 가능함을 보증하기 위한 기술적 처리절차에 대한 검증(Developing technical procedures)"[294]

3) 증거 평가(Evidence Assessment)

원칙 : 디지털 증거는 행동방침을 결정하기 위하여 사건의 범위를 고려하여 철저히

---

292) U.S. Dept. of Justice, Forensic Examination of Digital Evidence: A Guide for Law Enforcement, NIJ Special Report, 2008, p.3.

293) ibid.

294) U.S. Dept. of Justice, Forensic Examination of Digital Evidence: A Guide for Law Enforcement, NIJ Special Report, 2008, pp.3-5.

평가되어야 한다.[295]

절차 : 수색영장, 다른 법률적 권한, 사건의 세부사항, 하드웨어와 소프트웨어의 특성, 찾고자 하는 잠재적 증거, 조사되어야 할 증거의 획득을 둘러싼 정황을 리뷰함으로서 철저한 평가를 수행한다.[296]

가) 사건평가(Case assessment)

사건 수사관의 서비스 요청시 포렌식 조사요청을 위한 법적인 권한을 확인하고, 완전한 지원요청서 여부를 확인해야 하며, 절차의 연속성에 대한 기록을 작성해야 한다. 이 과정에서 포렌식 조사관은 수사관과 다른 포렌식 분석과정의 필요 여부, 다른 수사방법의 적용가능성, 주변기기의 구성요소와 연관성, 잠재적 증거, 추가적 정보, 사용자의 컴퓨터 능력평가, 조사할 증거의 우선순위, 필요한 장비 및 인원 등을 고려하여 논의해야 한다.[297]

나) 현장 고려사항(Onsite Considerations)

현장에서는 각 개인의 안전 그리고 수색 전 그리고 과정중 적절한 안전이 확보되어야 한다.[298]

컴퓨터 범죄 현장조사와 관련해서는 "Electronic Crime Scene: Investigation: A Guide for First Responders"를 참고할 수 있다.[299]

다) 조사장소 평가(Processing Location Assessment)

조사가 행해져야 하는 장소를 판단하기 위해 증거를 평가 - 증거복구 수행을 위해 현장에서 필요한 시간, 장기간 배치에 적합한 실행계획과 인원, 장시간 수색으로 인한 기업에 대한 영향, 현장조사에 대한 경험· 숙련도· 장비·자원 등의 적합성 - 해야 한다. 조사 장소로는 지정된 포렌식 연구실과 같은 통제 가능한 환경이 필요하지만, 불가피하게 현장조사를 하는 경우에는 주위환경을 충분히 통제해야 한다.

---

295) U.S. Dept. of Justice, op.cit., p.7.
296) ibid.
297) U.S. Dept. of Justice, op.cit., pp.7-8.
298) U.S. Dept. of Justice, op.cit., p.8.
299) ibid.

라) 법적 고려사항(Legal Considerations)

수색권한의 범위를 판단하고, 적용가능한 연방법·주법·지역 정책 및 법률과 관련하여 가능한 우려사항들을 확인해야 한다.

마) 증거평가(Evidence Assessment)

증거의 우선순위를 결정해야 한다.

4) 증거 획득(Evidence Acquisition)

원칙 : 디지털 증거는 본질적으로 취약하며, 부적절한 취급 또는 조사에 의해 변경, 손상, 파괴될 수 있다. 이러한 이유로 인해 이러한 유형의 증거를 보존하기 위해서는 특별한 예방조치가 취해져야만 한다. 그렇지 않으면 그것을 활용할 수 없게 되거나 부정확한 결과를 초래할 수 있다.[300]

절차 : 원본 디지털 증거는 그 증거를 보호하고 보존하는 방식으로 획득해야 한다.[301]

기본절차는 다음과 같다.[302]

ⅰ) 기관의 지침에 따라 디지털 증거를 보호한다

ⅱ) 조사자 시스템의 하드웨어와 소프트웨어에 대한 환경설정을 기록한다

ⅲ) 하드웨어와 소프트웨어를 포함하여 조사자 컴퓨터 시스템의 운용을 확인한다.

ⅳ) 저장매체에 대한 물리적 접근을 허용하기 위해 조사할 컴퓨터의 케이스를 분해한다.

ⅴ) 획득할 필요가 있는 저장매체를 확인한다. 이들 저장매체는 내장형, 외장형 또는 둘 다 일수 있다.

ⅵ) 내부 저장매체와 하드웨어 환경설정을 기록한다

ⅶ) 데이터의 변조, 손상, 파괴를 막기 위하여 (마더보드 또는 드라이브 뒷면에서 데이터 케이블 또는 전원 커넥터를 활용하여) 저장매체를 분리한다.

---

300) U.S. Dept. of Justice, Forensic Examination of Digital Evidence: A Guide for Law Enforcement, NIJ Special Report, 2008, p.11.

301) ibid.

302) U.S. Dept. of Justice, op.cit., pp.11-13.

viii) 통제된 부팅을 통해, 용의자 시스템으로부터 환경설정 정보를 검색한다
ix) 시스템을 종료한다
x) 가능하면 대상 저장매체를 옮겨서 조사자의 시스템을 활용한 획득을 수행한다. 조사자의 시스템에 대상 매체를 연결할 때 그것이 인식될 수 있도록 저장매체를 설정한다.
xi) 예외적인 경우 대상 시스템으로부터 저장매체를 제거하지 않는다는 결정이 행해질 수 있다.
xii) 증거를 획득할 때, 조사자의 저장매체가 포렌식적으로 무결한지 확인한다.

5) 증거 조사(Evidence Examination)

원칙 : 일반적인 포렌식 원칙들은 디지털 증거 조사시에도 적용된다. 서로 다른 유형의 사건과 매체는 서로 다른 조사방법을 요구할 수 있다. 디지털 증거에 대한 조사를 수행하는 사람은 이러한 목적을 위해 훈련을 받아야만 한다.[303]

절차 : 승인된 포렌식 절차를 활용하여 획득된 데이터에 대해 조사를 수행한다. 가능한 한 원본 증거에서 조사가 수행되어서는 안된다.[304]

증거조사를 수행할 때 다음의 단계들을 활용하는 것을 고려한다.[305]

i) Step 1. 준비(Preparation)
증거파일과 데이터를 복구하거나 추출할 수 있도록 별도의 매체상에 작업 디렉토리를 준비한다.

ii) Step 2. 추출(Extraction)
서로 다른 두 가지 유형의 추출이 있는데, 물리적인 추출과 논리적인 추출이 그것이다. 물리적 추출단계는 파일시스템과 상관없이 물리적인 전체 드라이브에서 데이터를 복구하고 식별한다. 논리적 추출단계는 설치된 운영시스템, 파일시스템, 그리고 응용 프로그램에 기반하여 파일과 데이터를 복구하고 식

303) U.S. Dept. of Justice, Forensic Examination of Digital Evidence: A Guide for Law Enforcement, NIJ Special Report, 2008, p.15
304) ibid.
305) U.S. Dept. of Justice, op.cit., pp.15-18.

별한다.

ⅲ) Step 3. 추출된 데이터의 분석(Analysis of extracted data)

분석은 그 사건에 있어서 추출된 데이터의 중요성을 판단하기 위해 추출 데이터를 해석하는 절차로, 타임프레임(timeframe) 분석, 데이터 은닉 분석, 응용프로그램과 파일 분석, 소유자와 점유자의 확인 등이 있다. 분석은 서비스 요청, 디지털 증거의 검색을 위한 법적 권한, 수사상 단서 또는 분석 상의 단서에 대한 리뷰를 요구할 수 있다.

ⅳ) step 4. 결론(Conclusion)

이러한 각 단계에서 얻어진 결과가 결론을 도출하기에 충분하지 않을 수 있지만, 개별적인 결과들 간의 연관성을 전체적으로 보면 훨씬 완벽한 그림이 제공될 수도 있다. 따라서 조사절차의 마지막 단계로서 추출과 분석결과를 전부 고려해야 한다.

6) 기록과 보고(Documenting and Reporting)

원칙 : 조사자는 디지털 증거조사의 분석결과와 조사결과를 완벽하고 정확하게 보고할 책임이 있다. 기록은 조사 전체에 걸친 지속적인 프로세스로, 디지털 증거를 조사하는 동안에 취해진 모든 단계를 정확하게 기록하는 것이 중요하다.[306]

절차 : 모든 기록은 완벽하고 정확하고 포괄적이어야 한다. 결과 보고는 의도된 청중을 위해 기술되어야 한다.

가) 조사자의 기록

기록은 조사와 동시에 행해져야 하며, 기록의 보관은 기관의 정책과 일치해야만 한다. 기록절차 전체에 걸쳐 조사자를 지원할 수 있는 일반적인 고려사항의 목록은 다음과 같다.

ⅰ) 사건 수사관 또는 검사와 협의시 기록한다

ⅱ) 사건기록과 함께 수색권한에 대한 사본을 유지한다

306) U.S. Dept. of Justice, Forensic Examination of Digital Evidence: A Guide for Law Enforcement, NIJ Special Report, 2008, p.19.

iii) 최초의 지원요청을 사건파일과 함께 유지한다.
iv) 절차의 연속성 기록을 유지한다
v) 완벽한 복제 행위가 허용되기에 충분할 정도로 상세하게 기록한다
vi) 기록 날짜, 시간 그리고 취해진 조치에 대한 설명과 결과를 포함한다.
vii) 조사하는 과정에서 부딪힌 불규칙성 그리고 그 불규칙성에 관하여 취해진 조치들을 기록한다.
viii) 네트워크 구조, 인가된 사용자 목록, 사용자 동의, 패스워드와 같은 추가적인 정보를 포함한다.
ix) 법집행기관 또는 조사자의 지휘시 또는 지휘로 인해 시스템이나 네트워크에 행해진 변화를 기록한다
x) 운영시스템과 관련 소프트웨어 버전과 현재 적용된 패치 사항들을 기록한다.
xi) 원격 저장소, 원격 사용자의 접근, 외부 백업을 고려하여 현장에서 획득된 정보를 기록한다.

나) 조사자의 보고

이는 수사관·검사 그리고 다른 사람에게 제출될 보고서를 작성함에 있어서 지침을 제공하기 위한 것으로, 기관의 정책상 순서나 내용과 같은 구체적인 보고서 작성 세부규칙을 지시할 수 있다. 보고서에 포함될 수 있는 일반적인 사항으로는 보고 직원의 신원, 사건 식별자 또는 제출번호, 사건 수사관, 제출자의 신원, 수령한 날짜, 보고날짜, 일련번호·제조번호·모델을 포함한 조사를 위해 제출된 물품의 설명 목록, 조사자의 신원과 서명, 문자열 검색·그래픽 이미지 검색·삭제된 파일 복구와 같은 분석과정에서 취했던 조치들에 대한 간단한 설명, 결과와 결론 등이 있다.

3. 디지털 포렌식에 대한 법적 평가

지난 10년 동안 디지털 포렌식 조사에 관한 항소법원 사건 100 케이스를 분석한 연구결과[307]에 따르면, 41건은 디지털 포렌식 프로세스의 수집과정에서의 쟁점들을

307) Kelly Anne Cole/Shruti Gupta/Dheeraj Gurugubelli/Marcus K Rogers, "A Review of Recent Case Law Related to Digital Forensics: The Current Issue", Proceedings of Conference on Digital Forensics, Security and Law, 2015.

다루고 있으며, 10건은 데이터 분석에 관한 것이며, 5건은 제출과 전문가 증언에 해당하는 것이었으며, 나머지 31건은 법률적 쟁점에 관한 것이었다고 밝히고 있다. 이를 좀더 세분화하면 다음과 같다. 먼저 디지털 포렌식 프로세스 수집과정에서 법원에 의해 다루어진 쟁점들은 영장 범위의 초과, 프라이버시에의 기대/영장없는 수색, 상당한 이유의 기준이 충족되지 않는 경우, 수색에의 동의가 없는 경우, 기간이 경과되었거나 무효한 영장 등으로, 디지털 포렌식 조사에 관하여 가장 자주 논쟁되어온 압수·수색의 방법에 관한 문제들인 것으로 나타났다.[308] 이와 같이 디지털 조사 과정에서 부적절한 압수·수색의 방법은 증거의 불인정을 초래한다.[309]

다음으로 데이터 분석과 관련한 쟁점에 해당하는 경우 대부분은 프로그램 결과물의 오류 또는 프로그램이 정확하게 작동하지 않은 경우, 타임 스탬프와 맥타임의 불확실성, 조사과정에 컴퓨터가 지워졌거나 오염된 문제들을 다루고 있다.[310]

제출 및 전문가 증언과 관련하여 법원에 의해 다루어진 문제는 제출을 위한 텍스트 메시지 또는 이미지를 보존하지 못하거나, 전문가가 도구의 소스코드를 완벽히 이해하거나 그것이 어떻게 작동하는지를 알아야만 하는가의 여부에 관한 것이었다.[311]

마지막으로 압수·수색의 방법에 관한 쟁점 다음으로 디지털 포렌식 조사와 관련하여 법원에 의해 가장 많이 다루어진 쟁점은 법률적 문제에 관한 것이었다. 즉, 학대받은 아동의 이미지가 실제적인 것인가 가상의 것인가 아니면 컴퓨터에 의해 생성된 것인가의 여부, 피고인이 패스워드 또는 파일의 암호 해독을 거부한 경우, 권한 없는 접속 또는 특정파일에 누가 접속했는가 아닌가의 여부, 양형에 있어서 이중 계산과 형가중 문제, 고의적인 소유 등이 그것이다.

아래에서는 디지털 포렌식 프로세스와 관련한 주요 쟁점들을 다룬 판결을 간략히 소개해 보고자 한다.

---

308) Kelly Anne Cole/Shruti Gupta/Dheeraj Gurugubelli/Marcus K Rogers, op.cit., p.97.
309) ibid.
310) ibid.
311) ibid.

가. 디지털 포렌식 도구에 대한 법원의 태도

과학적 증거가 법정 증거로서 허용되기 위해서는 그것에 적용된 과학적 법칙과 기술의 타당성이 인정되어야 한다. 미국 법원은 이러한 과학기술을 이용한 증거에 대한 법적 판단기준으로서 Frye test와 Daubert test를 적용하고 있는데, 이 두가지 test에서 공통적으로 요구하는 기준이 '관련 학계내에서의 일반적 승인 내지 인정'이다. 이 기준은 법원이 과학적 도구와 절차(방법)의 정당성을 입증하는 가장 중요한 요소가 되고 있다.[312] 디지털 증거에 있어서도 해당 증거를 식별·수집·분석하는데 있어서 사용되는 도구의 타당성에 대한 검증이 요구되는데, 가장 일반적으로 활용되는 포렌식 도구인 Encase의 유효성이 주로 법적 판단의 대상이 되고 있다.

1) People v. Rodreiguez, No.Fo31606

이 사건은 EnCase를 사용하여 피고인의 이메일을 복구한 것이 유효하고도 적법한 절차로서 허용될 수 있는가와 관련한 것으로, 피고인은 EnCase는 Frye test의 대상이 되어야 하며, EnCase 보고서 자체는 증거로서 허용되어서는 안된다고 주장하였다. 즉 미국의 대다수의 법원들이 과학적 또는 기술적 증거를 확보하고 분석하기 위한 절차가 유효한 절차로서 관련 과학적 공동체로서 일반적으로 승인된 것인가의 여부를 판단하는데 Frye test를 활용하는데, EnCase와 관련하여서는 컴퓨터 포렌식이라는 개념에 적용되고 있는 그러한 test에 관해 알려진 기록이 없다는 것이다.[313] 이에 대해 법원은 EnCase가 포렌식 관련업계에서 일반적으로 허용되는 기준에 해당한다고 판단했다.

따라서 심리 결과 피고인은 EnCase가 Frye test 하에서 컴퓨터 증거를 복구하기 위한 적절하고도 승인된 방법이라는 점은 인정했지만, EnCase 보고서 자체는 검찰이 그 문서가 진정한 것임을 입증할 수 없기 때문에 증거로서 허용되어서는 안된다고 주장했다. 이에 대해 법원은 전문가에 의해 작성된 EnCase 보고서는 증거로서 허용된다고 하면서 피고인의 주장을 기각했다.[314]

---

312) 노명선, "디지털 증거의 증거능력에 관한 판례 동향과 분석(I)", 수사연구, 2014, 68면.
313) Guidance Software, Encase Legal Journal, 2003, p.54.
314) Guidance Software, op.cit.p.55.

2) United States v. habershaw, 2001 WL 1867803(2002 D. Mass)

피고인은 컴퓨터 포렌식 소프트웨어를 가지고 'sector by sector'수색을 한 것은 영장의 범위를 벗어난 것이라고 주장했다. 이에 대하여 법원은 영장의 범위내에 있는 정보인 한 컴퓨터로부터 정보를 복구하기 위해 어떠한 수단도 사용할 수 있다고 하면서, 삭제된 컴퓨터 파일을 복구한 정부의 수색을 지지한 U.S. v. Upham 판결에 의거하여 피고인의 주장을 기각했다.[315]

이 사건에서는 EnCase Timeline이 중요한 것으로 입증되었다. 법원에 제출된 전문가 보고서는 Timeline view로부터 스크린 캡쳐한 것이 사건의 순서에 관한 중요한 맥락을 제공하는데 중요한 것으로 표시했다. 하지만 라이브 환경에서 컴퓨터를 작동하고 파일에 접근했던 사건담당 조사관의 조치들이 피고측 컴퓨터 포렌식 전문가에 의해 의문이 제기되었다. 피고측 전문가는 그 증거가 사건담당 조사관에 의해 컴퓨터 안에 심어질 수 있다고 주장했다. 하지만 사건담당 조사관은 자신이 현장에 있는 시간동안 파일이 접속되었고, 자신이 도착하기 전에는 그 시간동안 컴퓨터상에 어떤 파일도 만들어지거나 변경되지 않았다는 것을 입증할 수 있었다. 즉 Timeline은 컴퓨터가 사건담당 조사관에 의해 이미징을 하기 위해 최종적으로 정지되었던 시점으로부터 어떤 추가적인 활동도 없었다는 것을 보여주었다. EnCase의 증거파일의 통합된 chain of custody 특성은 컴퓨터 이미징을 Timeline 상에서의 어떤 활동의 중지와 연결시키는데 도움이 되었다.[316]

나. 디지털 포렌식 프로세스에 대한 법원의 태도

미 연방증거법에 디지털 포렌식 프로세스와 관련한 구체적인 규정이 존재하지는 않는다. 다만 디지털 증거의 진정성과 동일성을 뒷받침 할 수 있는 기술적·절차적 사항의 준수여부를 토대로 디지털 증거를 법정 증거로 허용할 것인지의 여부에 대한 판단을 하고 있다. 따라서 미국 법원들은 디지털 증거를 인정하기 위해서는 디지털 포렌식이 중요한 의미를 갖는다는 점을 분명히 하고 있다.

---

315) ibid.
316) Guidance Software, op.cit., p.56.

1) Simon Property Group, L.P. v. mySimon, Inc. 194 F.R.D.639 (S.D.Ind.2000)[317]

원고의 증거개시신청 즉, 피고에 의해 사용된 컴퓨터·서버·전자기록장치 뿐만 아니라 집에 있는 컴퓨터를 포함해서 특히 4명의 이름으로 사용된 장치들의 확인, 그리고 당해 컴퓨터상의 파일 삭제에 관한 상세한 정보의 요구와 관련하여 법원은 전자의 확인은 허용했지만 후자의 요구는 기각했다.

법원은 쟁점에 관한 기록이 희박하다는 점에 비추어, 원고는 자신의 비용으로 4명의 이름으로 사용된 컴퓨터로부터 삭제된 컴퓨터 파일을 복구하는 작업을 시도할 자격이 있다고 결론지었다. 따라서 원고는 하드 드라이브에 대한 mirror image 또는 snapshot을 만들기 위해 당해 컴퓨터를 점검할 전문가를 선정하고 그 비용을 지불해야 하며, 피고는 전문가 선정에 반대할 기회가 있으며, 법원은 그 전문가가 법원의 사무관으로서 점검과 복제를 수행하도록 임명하게 된다.

전문가는 각 컴퓨터의 하드 드라이브의 mirror image로부터 모든 활용 가능한 워드 프로세싱 문서, 전자메일 메시지, 파워포인트 또는 유사한 프레젠테이션, 스프래드시트, 기타 유사한 파일들을 복구하기 위하여, 그리고 피고측 변호인에게 합리적으로 편리한 형식으로 제공하기 위해 자신의 전문지식을 활용해야 한다. 법원의 의도는 운영시스템을 구성하는 파일들과 컴퓨터 내의 고수준의 프로그램이 복제되지 않도록 하고, 그 복제가 이 사건과 관련이 있을 가능성이 있는 자료를 포함할 것으로 합리적으로 여겨지는 파일 유형으로 제한하고자 하는 것이었다. 따라서 가능한 한 최대로, 전문가는 피고측 변호인에게 모든 복구된 삭제 파일이 삭제된 시점을 보여주는 활용가능한 정보, 그리고 복구될 수 없는 모든 삭제파일의 내용과 삭제에 관한 활용가능한 정보를 제공해야 한다.

전문가는 이 소송이 끝날때까지 피고측 변호인에게 제공된 모든 파일의 복제본과 하드 드라이브 mirror image 복제본을 보유해야만 한다. 이 소송이 종료되면 전문가는 기록을 파기해야 하며, 원고 또는 그의 변호인 또는 다른 사람에게 모든 파일 또는 문서의 내용을 공개해서는 안된다. 그리고 전문가는 법원에 수행한 업무의 범위

317) https://cyber.harvard.edu/digitaldiscovery/library/process/simon.html; 2016.9.30.

를 제시하고 피고측 변호인에게 제공된 기록의 양과 범위를 개괄적으로 보여주는 보고서를 제출해야 한다.

2) United States v. Bunty, 617 F. Supp. 2d 359 (E.D. Pa. 2008)[318]

피고인은 정부가 중요한 그리고 자신의 무죄를 입증할 수 있는 증거를 훼손했다고 주장했다. 즉 피고인으로부터 압수한 플래시 드라이브를 우선적으로 포렌식 복제를 하지 않은 채 포렌식적으로 불안전한 환경에서 연결시켰으며, 두 개의 압수된 랩탑 컴퓨터를 각 내용에 대한 포렌식 복제를 하지 않은 채 랩탑의 본래 소유권자인 피고인의 고용회사 Bearing Point and Wyeth에 반환했다고 주장했다.

이러한 피고인의 주장에 대하여 정부는 다음과 같이 반박하였다. 첫째, 정부는 2006년 1월 27일에 연방직원이 공항에서 피고인 소유의 플래시 드라이브에 접속하지 않았으며, 그 장치는 전문가에 의한 차후의 포렌식 조사를 위해 그 직원에 의해 보존되고 압류되었다. 둘째, 두 개의 랩탑 하드 드라이브는 포렌식 전문가에 의해 이미지 복제되었으며, 원본 하드 드라이브는 정부에 의해 보관되었다. 이에 대하여 피고인은 정부의 주장을 반박할 어떤 증거도 제출하지 않았으며, 따라서 법원은 공항에서 압수된 랩탑 컴퓨터 또는 플래시 드라이브에 관하여 어떤 훼손도 발견하지 못했다고 판단했다.

또한 피고인은 정부가 우선적으로 포렌식 복제를 하지 않은 상태에서 공항에서 정부소유의 컴퓨터로 플로피디스크의 내용을 확인함으로 인해 증거가 훼손되었다고 주장했다. 즉 원본 디스크에 접속하여 봄으로 인해, 혐의가 제기된 아동 포르노그라피가 공항수색이 있던 2006년 1월 27일 이전에 마지막으로 접속되었던 시간에 관하여 중요한 정보를 제공하게 될 플로피디스크상의 마지막 접속 데이터가 훼손되었다고 주장했다. 즉, 연방직원이 플로피 디스크상의 각각의 파일과 결합된 마지막 접속 데이터를 변경함으로써 피고인으로 하여금 그 파일들을 가지고 있는 동안에 그 파일들에 접속하지 않았다는 것을 배심원에게 주장하지 못하게 만들었다고 주장했다. 피고인은 그 디스크가 자신의 점유하에 있는 동안에 그 파일들이 오픈되지 않았으며, 따라서 그는 플로피 디스크안에 있는 것이 무엇인지 알지 못했다고 배심원에게 주장하고자

318) https://www.courtlistener.com/opinion/2246387/united-states-v-bunty/; 2016.9.30.

하였던 것이다.

이에 대하여 정부는 플로피 디스크와 관련하여 연방직원이 그 플로피 디스크를 열어봤고, 따라서 각 파일과 결합된 마지막 접속 데이터가 변경되었다는 것을 인정했다. 하지만 정부는 마지막 접속데이터는 단지 그 직원이 플로피 디스크상에 있는 이미지를 봤던 정보만을 변경했다고 하는 전문가 증언을 제공했다. 즉 마지막 접속 데이터에 대한 변경은 플로피디스크에 대한 중대한 변경이 아니었으며, 그 직원은 최소한도의 가능한 침해적 수단으로 수색을 했다고 주장했다. 이에 법원은 ICE에 있는 두명의 컴퓨터 포렌식 전문가로부터 2006년 1월 27일에 한 연방직원의 행위가 플로피 디스크상의 기초가 되는 포렌식 데이터에 미친 영향에 관하여 증언을 들었다. 두 명의 컴퓨터 포렌식 전문가는 그 수색을 하는 동안에 연방직원은 플로피 디스크상의 6개 파일을 열어서 그 파일 안에 있는 이미지를 보고 그 파일을 닫은 것 그 이상의 어떤 행위도 하지 않았다고 증언했다. 심리후 법원은 피고인이 아닌 정부가 그 피고인이 혐의가 제기된 아동 포르노그라피를 고의로 보유하고 있다는 것을 입증할 책임이 있고, 피고인은 변경된 마지막 접속 데이터에 관하여 그리고 그 데이터가 변경되지 않았다면 입증할 수 있었던 것에 관하여 연방직원과 포렌식 전문가를 반대심문할 수 있다는 점을 지적했다. 그리고 정부도 연방직원의 행위로 인하여 정부측에 도움이 되었을지도 모르는 데이터를 증거로서 활용할 수 있는 능력을 상실했기 때문에, 연방직원이 악의로 했거나 또는 그 사건에 대한 편견을 유발하기 위해서 한 것이라는 점을 피고인측이 입증해야 함에도 하지 못했으므로 증거의 오염을 이유로 사건을 기각해달라는 피고인의 신청은 거부되었다.

다. 디지털 포렌식 전문가에 대한 법원의 태도

디지털 포렌식 전문가는 자신이 작성한 보고서가 법원에 제출되는 경우 그와 관련하여 증인으로서 결과물에 대한 전문적인 증언을 할 수 있어야 한다. 이러한 전문가의 증언능력과 관련하여 미 연방증거법 제702조는 "전문가의 과학적·기술적 또는 기타 전문적인 지식이 사실인정자가 증거를 이해하거나 쟁점사실을 판단하는데 도움이 되는 경우, 그 증언이 충분한 사실 또는 데이터에 근거한 경우, 그 증언이 신뢰할 수 있는 원칙과 방법의 산물인 경우, 전문가가 그 원칙과 방법을 그 사건의 사실에

정확하게 적용한 경우에, 지식·기술·경험·훈련·교육에 의해 전문가로서 자격이 부여된 증인은 의견의 형식으로 증언을 할 수 있다"고 규정하고 있다. 즉 미국의 경우 당해 전문가가 증인으로서 자격을 갖추기 위해서는 해당 주제에 대해 지식·기술·경험을 갖고 있거나 훈련 또는 교육을 받았음을 입증하면 충분하다고 보고 있다. 이 규정에 근거하여 디지털 포렌식과 관련한 전문적인 교육 내지 훈련을 받았거나 경험을 갖고 있는 디지털 포렌식 전문가들은 전문가로서의 자격을 갖고 법정에서 증언을 할 수 있다.[319]

1) Galaxy Computer Services, Inc. v. Baker[320]

원고측은 피고측이 삭제한 파일을 복구하여 그 내용을 전문가 보고서에 기재한 조사관을 증인으로 신청했으며, 이에 대해 피고측은 그 조사관인 " i) 테일러의 전문가 의견은 재판에 관한 쟁점과 무관한 것이다, ii) 테일러는 전문가 증언을 제공할 자격이 없다, iii) 테일러는 적절한 절차를 준수하지 않았다, iv) 테일러는 변경된 데이터 또는 삭제된 데이터에 관하여 의견을 밝힐 수 없다"는 이유로 증인배제를 요청하였다.[321] 또한 피고측은 그 조사관이 컴퓨터 전문가로서 증언할 자격이 없다고 주장하면서, 다음과 같은 이유를 제시하였다. " i) 피고인은 컴퓨터 사이언스에 있어서 학위를 갖고 있지 않다, ii) 그는 컴퓨터 언어에 능통하지 않다, iii) 그는 컴퓨터 프로그래머가 아니다, iv) 그는 컴퓨터 사이언스에 관하여 보유한 자격증이 없다, v) 그는 마이크로 소프트 관련 자격증을 위한 훈련이나 특별한 교육을 받지 않았다."[322]

이에 대하여 법원은 조사관인 테일러는 지식·기술·경험·훈련 그리고 교육에 기반한 전문가로서 자격이 있다고 인정하면서 다음과 같이 피고측 주장을 배척하였다. "컴퓨터 포렌식 분야는 컴퓨터 프로그래밍, 즉 프로그램 코드를 읽거나 쓰는 배경지식을 요하지 않는다. 그리고 그는 5년간 컴퓨터 포렌식 분야에서 일해 왔고, 이 기간 동안 자신의 조사결과를 토대로 약 1,600-1,700건의 포렌식 보고서를 작성하여 그중

319) 노명선/백명훈, 디지털 포렌식, 2016, 465면.
320) Galaxy Computer Services, Inc. v. Baker, 325 B.R.544(E.D.Va.2005); 노명선, 앞의 책, 456면에서 재인용.
321) http://www.leagle.com/decision/2005869325BR544_1800/GALAXY%20COMPUTER%20SERVICES,%20INC.%20v.%20BAKER; 2016.9.30.
322) http://www.leagle.com/decision/2005869325BR544_1800/GALAXY%20COMPUTER%20SERVICES,%20INC.%20v.%20BAKER; 2016.9.30.

다수가 법원에서 증거로 채택된 바 있다. 또한 그는 하이테크 범죄수사협회의 구성원이며, 크랜필드 대학에서 컴퓨터 포렌식에 대한 대학원 집중훈련과정 3개를 마쳤다."[323]

또한 피고측은 "테일러의 데이터 복구 서비스는 하드 드라이브 조사시 내부 chain of custody를 준수하지 못했다고 주장했다. 즉 갤럭시 컴퓨터로부터 데이터를 복구하고 분석한 것이 정확하고 오염되지 않았다고 담보할 수 없다고 주장하였다. 그리고 이러한 chain of custody 문제는 하드 드라이브 일부가 오염되었을 수 있고 따라서 결론적으로 신뢰할 수 없다"고 주장했다. 하지만 이에 대하여 법원은 "chain of custody에 있어서 단절 가능성은 단지 증거의 가치에만 영향을 미친다"고 하면서 테일러가 증언을 하도록 허용하였다.

2) Nucor Corp v. Bell, 2008 WL 4442571 (D.S.C. Jan. 11, 2008)

이 사건에서 전문가는 반대당사자가 랩탑에서 증거를 지우기 위해 추적할 수 없는 삭제프로그램을 사용했다는 증거에 대해 증언을 제공했다. 법원은 전문가에 의해 사용된 방법이 데이터와 의견 사이의 분석적인 갭을 충분히 채웠다고 보아 전문가 증언을 배제해달라는 신청을 기각했다.

Daubert test 요소들을 긍정하면서 법원은 드라이브상에 제로 블록이 어떻게 나타났는가에 대한 가설을 검증했고, 제로 패턴들을 정확히 복제했다고 지적했다.[324]

법원은 반복할 수 있는 것으로 판단된 검증으로부터 얻어진 증거를 허용했다. 즉 전문가가 데이터가 예상되는 방법으로 하드 드라이브에 쓰여졌다는 것을 입증하기 위한 테스트에 있어서 각 단계를 철저히 기록했기 때문이다.[325]

일반적으로 디지털 포렌식 보고서의 결과물을 복제하는데 포렌식 이미지를 활용할 수 없는 경우, 그 방법의 정확성이나 신뢰성 여부를 평가할 수 없기 때문에 그 보고서에 대한 신뢰가 감소될 수 있다. 포렌식 이미지 복제본을 활용하여 그리고 유사한 분석 소프트웨어를 활용하여 재현할 수 없는 결과를 가진 보고서는 낮은 신빙성이

323) http://www.leagle.com/decision/2005869325BR544_1800/GALAXY%20COMPUTER%20SERVICES,%20INC.%20v.%20BAKER; 2016.9.30.
324) Daniel B. Garrie/J. David Morrissy, "Digital Forensic Evidence in the Courtroom: Understanding Content and Quality", Northwestern Journal of Technology and Intellectual Property, vol.12, 2014, p.126 .
325) ibid.

허용되며 따라서 예외적인 경우에는 재검토되어야 한다.[326]

3) United States v. Hilton[327]

검찰측 증인인 전문수사관 Marx는 당해 이미지들이 주 사이의 상거래에서 돌아다니던 것이라는 것을 입증하기 위하여 두 가지 요인들을 확인했다. 즉 "첫째, 소니 백업테이프안에 있는 파일들은 MIRC라고 하는 하위 디렉토리안에 있었는데, 거기에는 인터넷 채팅방과 연결하는데 사용되는 소프트웨어가 포함되어 있었다. 이것은 Marx에 따르면 그 이미지가 인터넷으로부터 다운로드 받았다고 추정할 수 있다. 둘째, 이미지 파일 각각의 시간과 날짜 특성은 모뎀을 통해 전송된 파일이라는 것을 나타낸다. 모뎀은 통상 컴퓨터와 전화선을 연결하기 위해 사용된다"고 증언했다.

이에 대하여 피고인은 모뎀의 의미와 작용은 일반적 지식의 범위안에 있는 것이 아니며, 법원이 당사자들에게 이를 증거로 이용한다는 사실에 대해 고지하지 않았기 때문에, 연방증거법 제201조의 규정을 근거로 모뎀과 관련된 사실인정은 부정되어야 한다고 주장했다. 그리고 Marx의 추상적 증언 만으로는 합리적 의심을 넘어서지 못했다고 주장했다.

이에 법원은 "검찰은 모뎀 전송에 대한 직접적인 증거를 제시할 필요가 없고, Marx 전문수사관의 증언은 그 파일들이 인터넷 또는 전화망을 통해 전송되었음을 인정하기에 부족하지 않다"고 하면서 피고인의 유죄를 인정하였다.[328]

제2절 영국의 디지털 포렌식 시스템

1. 디지털 포렌식 기구

가. Forensic Science Service(FSS)

FSS는 영국과 웨일즈내의 몇 개의 포렌식 실험실들이 합쳐져서 1991년에 영국정부

326) ibid.
327) U.S. v. Hilton, 257 F.3d 50(1st Cir.2001); https://www.courtlistener.com/opinion/199515/united-states-v-hilton/2016.9.7.
328) 노명선, 국제기준에 적합한 디지털 포렌식 기술교육의 표준모델 개발, 2012, 147면.

의 내무성의 집행부서로 설립되었으며, 1996년 메트로폴리탄 경찰실험실과 합병되었다. 2005년 이후 정부소유 민관합작 공기업이 된 FSS는 영국과 웨일즈의 경찰과 정부기관에 법과학 서비스를 제공해왔으며, 단일한 법과학 업무수행 기관으로 영국 전체에 걸쳐 주요한 포렌식 소스에 대한 상담·훈련·지원업무를 담당했다. 기본적으로는 범죄와 관련한 법과학적 증거의 감정 업무를 담당해왔으며, 세계 최초로 DNA 데이터베이스를 구축하여 이를 범죄수사에 활용했다.[329] 또한 FSS는 포렌식 소프트웨어와 기술, 특히 DNA 해석과 데이터베이스, 디지털 포렌식에 있어서 선두가 되기 위해 내부 전문가와 주요 국제 전문가를 끌어들였다.[330]

하지만 FSS가 영국내 형사사법시스템의 주요부분을 담당했음에도 그 업무 자체는 경찰과 별도로 독자적으로 수행했다. 이로 인해 경찰이 포렌식 서비스를 위해 경쟁입찰을 활용하는 경우가 늘어남에 따라 시장점유율의 손실이 초래되자 2009년 초에 정부가 5천만 파운드를 투입하였으며, FSS가 유지가능한 사업을 제공할 수 있도록 하기 위해 3개 지역에 있는 실험실을 폐쇄할 계획을 수립했다.[331] 이후 영국 정부는 매달 손실이 2천만 파운드에 이른다는 것을 명분으로 2010년 FSS를 폐쇄하고, 그 운영의 대부분은 가능한 이전하거나 매각될 것이라고 발표했다. 이에 대해 국제적인 포렌식 과학자들은 FSS 폐지가 영국 형사사법시스템에 잠재적으로 손해가 될 것이라는 비판과 함께 오판을 초래할 것이라는 우려를 제기했다.[332] 하지만 2012년 3월 31일에 FSS는 결국 폐쇄되었고, 따라서 현재 법과학 업무는 민간영역에서 계약에 의해 행해지거나 경찰내부 실험실을 통해 수행되고 있다.[333] 다만 FSS 폐쇄 이후 FSS 아카이브는 - 수집된 사건 파일, 현미경 슬라이드, 섬유샘플, DNA 샘플과 같은 작업샘플을 보관한 - 오래된 사건에 대한 재심을 위해 내무성의 관리·감독하에 계속 유지되고 있다.[334] 또한 FSS 아카이브는 장기미제사건의 해결에 큰 중요성을 갖는데, 문제는 FSS 폐쇄 이후 계약에 의해 포렌식 업무를 수행하는 민간 회사들에 대해 장기미제 형사사건 검토위원회가 장기미제사건과 관련하여 자료의 제출을 요구하거나

329) 김혜경/김택수, 선진국의 법과학 체계 및 입법례 비교, 2014, 85면.
330) https://en.wikipedia.org/wiki/Forensic_Science_Service; 2016.9.7.
331) ibid.
332) http://www.bbc.com/news/uk-35793073; 2016.9.7.
333) https://en.wikipedia.org/wiki/Forensic_Science_Service; 2016.9.7.
334) ibid.

재검토가 필요한 자료에 대한 접근권한을 주장할 수 없게 되었다는 점 때문에 논의의 필요성이 제기되고 있다.[335]

한편 FSS 폐쇄로 인하여 Forensic Science Regulator(FSR) 역할의 중요성이 강조되었는데, 이는 FSR이 형사사법시스템에 제공되는 포렌식 서비스의 품질표준에의 준수여부를 담보하기 때문이다. 따라서 2011년 하원의 과학기술위원회는 FSR에 법률상 권한을 부여할 것을 정부에 제안하기도 했다.[336]

나. FSS 폐쇄에 따른 대응방향

1) 국제표준 인증기준을 통한 법과학서비스 기관의 관리 모색

영국 하원의 과학기술위원회는 FSS 폐쇄절차를 밟은 2012년 1년 동안에 FSS의 어떤 업무도 ISO 17025 인증이 없는 민간 FSP에 이전되지 못한다고 밝힌 바 있다.[337] 즉 FSS 업무를 대체하게 될 민간 FSP 뿐만 아니라 경찰 내부의 연구소에 대해서도 ISO 17025 인증을 통한 법과학서비스 품질 유지 및 관리의 필요성을 강조한 것이다.

이러한 ISO 17025에 대한 인증은 국립 인증기관인 영국 인증서비스(UK Accreditation Service)에 의해 행해지는데, 이는 특정한 분석을 수행할 수 있는 연구소의 기술적 자격에 대한 권위 있는 보장을 제공할 뿐만 아니라 형사사법시스템과 관련한 특정한 부분 즉, 증거의 연속성·사건파일의 관리·증거물의 저장 등에 관한 리뷰를 한다.[338] 조달체계를 통해서 경찰에 포렌식 서비스를 제공하기 위해 계약을 맺은 모든 법과학서비스 제공자들은 자신들의 서비스에 대한 ISO 17025 인증을 받아야만 한다.[339]

몇몇 경찰 포렌식 연구소들은 민간 포렌식 서비스 제공자와 동일한 품질 표준(ISO

---

335) 김혜경/김택수, 선진국의 법과학 체계 및 입법례 비교, 2014, 99면.
336) House of Commons Science and Technology Committee, Forensic Science, Second Report of Session 2013-2014 vol.1., 2013, p.3.
337) House of Commons Science and Technology Committee, Seventh Report of Session 2010-12, The Forensic Science Service, HC855, paras 100-109; House of Commons Science and Technology Committee, Forensic Science, Second Report of Session 2013-2014 vol.1., 2013, p.22에서 재인용.
338) House of Commons Science and Technology Committee, Forensic Science, Second Report of Session 2013-2014 vol.1., 2013, p.20.
339) ibid.

17025)에 대한 인증을 확보하지 못했지만[340], 민간 법과학서비스 제공자에게 요구되는 ISO 17025 표준에 대한 인증유지 요건이 경찰 내부 연구소에 대해서는 의무적인 것이 아니기 때문에 현재 경찰내부 연구소들은 이러한 표준에 대한 인증없이 법과학 활동들을 수행할 수 있다고 한다.[341]

2) 민간분야 포렌식 서비스의 활용

FSS 폐쇄에 따른 업무이전에 있어서 포렌식 서비스 품질규제를 담당하는 FSR은 승인된 FSS환경으로부터 이전된 모든 업무는 똑같이 승인을 받은 기관으로만 옮겨질 수 있다는 입장을 취했다. 하지만 FSS 폐쇄를 발표하고 1년 만에 업무이전을 완료한 상황[342]에서 민간 포렌식서비스 회사들은 신속하게 포렌식 과학자들을 채용했지만 그들이 어떻게 신속하게 FSS의 자리를 채울 것인지는 분명하지 않았다. 가장 큰 규모의 포렌식 서비스 회사인 LGC도 기껏해야 전체 시장의 1/4정도 밖에는 담당하지 못하기 때문이었다.[343]

FSS 이전 업무를 담당했던 National Policing Improvement Agency(NPIA)는 FSS 이전이 행해지는 과정에서 적절한 품질표준이 엄격히 유지되었다고 했지만, 실제로 민간 포렌식서비스 회사인 LGC는 ISO 17025 인증을 위하여 UKAS에 신청을 한 후이기는 하지만 인증은 받지 못한 상태에서 West Yorkshire 경찰에 의해 제공된 새로운 시설에서 활동들을 시작했다. 물론 West Yorkshire에서 수행한 업무에 대해서는 현재 인증을 받은 상태이지만, 이전 당시에는 인증을 받은 LGC 실험실에서와 동일한 프로세스와 표준에 따라 업무를 수행할 수 밖에 없었다.

또한 내무성은 민간 포렌식 서비스 제공자에게 그들이 형사사법시스템에 제공하는 서비스에 대하여 새로운 또는 잠재적인 개선사항의 확인 및 개발을 수행하도록 하는 계약상 의무를 두었다. 하지만, 민간회사가 연구와 개발활동을 수행하는 것이 필수적인 요건은 아니었기 때문에, 위축된 포렌식 시장 상황하에서 상업적으로는 매력없는

---

340) House of Commons Science and Technology Committee, op.cit., p.3.
341) House of Commons Science and Technology Committee, op.cit., p.20, p.23.
342) House of Commons Science and Technology Committee, Forensic Science, Second Report of Session 2013-2014 vol.1., 2013, p.23.
343) http://www.theguardian.com/science/2011/sep/08/forensic-science-service-closure-damage; 2016.9.7.

결과지만 형사사법시스템에는 막대한 이익이 되는 일에 민간 FSP가 연구개발에 투자할 것을 기대하기는 어렵게 되었다.

3) 경찰 과학수사연구소

FSS의 업무를 이전받은 경찰내부 연구소는 민간 포렌식서비스 제공자와 동일한 수준의 능력 즉 ISO 17025의 표준에 따른 인증을 받을 의무가 없었다.[344] 따라서 인증에 의해 제공되는 보장이 없었기 때문에 포렌식 증거의 품질이 저하될 수 있으며, 법정에서 훨씬 더 의심스러운 것이 될 수 있다는 문제가 제기되었다.[345]

FSS가 설립되기 이전에도 경찰내부 연구소들은 포렌식 업무를 다루어 왔지만 경찰 또는 검찰과 너무 밀접해서 잘못된 유죄판결의 잠재적 혹은 현실적 원인으로 간주되었고, 그것이 FSS가 설립된 이유가운데 하나였다.[346] 그런데 FSS가 폐쇄되고 품질표준도 결여된 상태에서 다시 경찰서비스 안으로 포렌식 업무가 포함되는 것은 공정성에 관한 심각한 문제를 제기할 수 있고, 경찰 내부 과학자들에게 우호적인 결과를 산출하도록 하는 압박의 우려가 제기될 수 있는 것이다.[347] 즉 정부는 FSS가 본래 경찰과 법과학 서비스 제공을 분리시키기 위해 만들어진 것이라는 것을 간과한 것이라 할 수 있다. 따라서 과학기술위원회는 전문가 증언의 제공과 관련하여 경찰의 공정성의 문제는 법률위원회(Law Commission)가 지속적으로 재검토해야 한다고 제언하고 있다.[348]

나. Forensic Science Regulator(FSR)

1) 설립 및 기능

FSR은 형사사법시스템에 있어서 법과학 서비스의 제공이 적절한 과학적 품질 표준의 적용을 받도록 보장하기 위해 2007년 설립되었는데, 당시 FSR 설립을 발표했던 의회 국무차관은 FSR의 역할은 “정부와 형사사법시스템에 법과학을 제공함에 있어서

344) House of Commons Science and Technology Committee, Forensic Science, Second Report of Session 2013-2014 vol.1., 2013, p.23.
345) House of Commons Science and Technology Committee, op.cit., p.24.
346) House of Commons Science and Technology Committee, op.cit., p.25.
347) ibid.
348) ibid.

품질표준에 관하여 조언을 하는 것일 뿐만 아니라, 새로운 또는 개선된 품질표준에 관한 요구사항을 확인하고 필요한 경우에 새로운 표준을 개발하는데 앞장서는 것, 그리고 법정에서와 procurement 에서 공통적인 표준을 준수함을 입증할 수 있는 조언과 지침을 제공하는데 있다"[349]고 설명했다.

이렇게 설립된 FSR에 대해 내무성 국무장관이 제시한 역할은 다음과 같다.

"ⅰ) 경찰과 전반적인 형사사법시스템에 법과학 서비스를 제공함에 있어서 품질표준의 준수를 설정하고 감시한다.

ⅱ) 경찰내부 서비스와 포렌식 제공자를 포함하여, 경찰을 통해 전반적인 형사사법시스템에 법과학 서비스를 제공하는 기관들의 표준에 대한 적절한 평가를 한다

ⅲ) 국립 DNA 데이터 베이스와 국립 탄환정보시스템(the National DNA Database (NDNAD)® and the National Ballistics Intelligence System (NaBIS))에서 시작한 국립 법과학 정보 데이터베이스에 적용하는 품질표준에의 준수를 확립하고 감시한다.

ⅳ) 형사사법기관, 서비스 제공자 그리고 적절한 것으로 여겨지는 다른 기관에 대해 법과학에 있어서의 품질표준에 관한 문제에 대해 조언을 제공한다.

ⅴ) 법과학 서비스 제공에 있어서 품질표준에 관하여 일반국민과 이해관계자로부터의 이의제기 등을 처리한다."[350]

FSR은 내무성에 의해 지원을 받지만, 공적수탁인이며, 형사사법시스템을 위하여 내무성과 별개로 운용된다. 이러한 독립성은 FSR로 하여금 공정한 권고와 결정을 하도록 한다.[351]

2) 책임과 목표

FSR의 책임은 새로운 또는 개선된 품질표준에 관한 요구사항을 확인하고, 새로운 표준을 개발하는데 앞장서며, 필요한 경우 법과학서비스 제공자가 공통적인 표준을

---

349) http://www.publications.parliament.uk/pa/cm200607/cmhansrd/cm070712/wmstext/70712m0002.htm#07071262000011; Forensic Science Regulator, Business Plan 2013/2014, ver.1.0, p.2.에서 재인용.

350) Forensic Science Regulator, Business Plan 2013/2014, ver.1.0, p.2.

351) Forensic Science Regulator, Business Plan 2012 to 2017, p.1.

준수함을 입증할 수 있도록 자문과 지침을 제공하는데 있다.[352] 이를 상술하면 다음과 같다.

"ⅰ) 법과학 서비스의 제공에 있어서 새로운 품질표준과 개선된 품질표준에 대한 요구사항을 확인한다.
ii) 적절한 경우, 경찰 내부 서비스를 포함해서 경찰에 법과학 서비스를 제공하는 기관들의 인증을 요구한다.
iii) 법과학 분야에 있어서 새로운 기술과 어플리케이션을 인증하고 승인하는 절차를 결정한다
vi) 필요한 경우 새로운 개발을 주도하면서 국내 포렌식 데이터베이스에 적용하는 표준을 개발한다.
v) 포렌식 서비스의 품질에 관련한 문제에 대해 정부, 형사사법시스템 기관 그리고 서비스 제공자들에게 자문과 지침을 제공한다.
vi) 법과학의 표준에 관한 소개 또는 이의제기의 관리를 포함하여, 표준의 보증과 모니터링을 제공하기 위해 충분한 합의를 확보한다.
vii) 법과학 품질표준에 관련한 국제적인 개발에 참여한다."[353]

그리고 FSR는 일반국민과 이해관계자들이 형사사법시스템에 제공된 법과학 서비스에 대한 신뢰를 갖기를 원하기 때문에, 법과학이 일관되게 매우 높은 품질표준을 충족하도록 해야만 한다. 즉 영국에 있어서 형사사법시스템에 제공되는 법과학은 일관되게 높은 품질의 표준과 경찰, 검찰, 법원 그리고 일반국민에 의해 기대되는 무결성을 충족해야만 하는 것이다. 포렌식 프로세스의 모든 단계에 있어서 낮은 품질의 활동들은 입증가치가 있는 증거의 파괴·오염 또는 증거의 흔적을 복구하거나 명확하게 분석하지 못하는 결과를 초래할 수 있으며, 결국 이는 실패한 수사, 실패한 기소 심지어는 오판으로 이어지게 되기 때문이다.[354]

따라서 FSR은 다음과 같은 업무목표를 설정하고 있으며, 그 목표별로 구체적인

352) https://www.gov.uk/government/organisations/forensic-science-regulator/about; 2016.9.7.
353) Home Office, Consultation on new statutory powers for the forensic science regulator, 2013, p.6.
354) Forensic Science Regulator, Business Plan 2012 to 2017, p.2.

실천방안을 제시하고 있다.

"ⅰ) 법과학서비스는 형사사법시스템의 요구를 충족하는데 맞추어진 적절한 표준을 제공하며 독립적이고 효율적인 품질평가의 대상이 된다.
ⅱ) 형사사법시스템의 법과학 요구사항에 따라 법과학서비스 제공자, 정부 등에 높은 품질의 자문과 지침을 제공한다.
ⅲ) 품질 미달을 조사하고 문제를 제기할 수 있는 효율적인 수단이 있다.
ⅳ) 영국 전역의 품질표준을 달성하기 위하여 스코틀랜드와 북부 아일랜드에 있는 기관들과 효율적인 협력을 한다.
ⅵ) 법과학에 관한 유럽 또는 국제적 표준을 개발하기 위한 프로젝트에서 영국이 선도한다."[355]

또한 높은 표준을 개발하고 유지하기 위해 FSR은 다음의 역할을 하게 된다고 기술하고 있다.

"ⅰ) 영국 전역에 걸쳐 법과학 품질표준을 달성하기 위한 방향과 일치된 접근방법을 제공한다
ⅱ) 모든 법과학 활동들의 중심에 품질을 둔다
ⅲ) 실무규범에 기반하여 모든 범위의 포렌식 프로세스에 관하여 하나의 품질 표준 체계를 만든다
ⅳ) 독립적이고 권위있는 자문의 소스로서 법과학 자문위원회를 활용한다
ⅴ) 자동차처럼 유효한 품질표준을 제공하기 위해 특정분야 전문가의 활용을 유지한다
ⅵ) 광범위하게 상의하기 위하여 모든 영역의 이해관계자들과 관계를 맺어야 한다."[356]

이와 같이 FSR이 best advice와 실행가능한 표준의 개발을 달성하는데 있어서는 법과학 실무자, 전문가, 기타 이해관계자들의 지속적인 참여가 중요하기 때문에, 지속적인 이해관계자들의 참여와 FSR에 의해 조직된 전문가 그룹 - 법과학 자문위원회,

355) Forensic Science Regulator,op.cit., pp.3-4.
356) Forensic Science Regulator, Business Plan 2012 to 2017, p.2.

품질표준 전문가 그룹, DNA 전문가 그룹, 법의병리학 전문가 그룹, 디지털 포렌식 전문가 그룹, 오염전문가 그룹, 진문품질표준 전문가 그룹, 법의학 전문가 그룹 -을 활용하고 있다.[357]

FSR은 2017년 3월 말경 형사사법시스템 내의 모든 포렌식 분야가 FSR의 실무와 행동규범을 토대로 단일한 품질표준체계로 운영되어질 것을 예정하고 있다.[358]

3) FSR의 권한

포렌식에 있어서 업무품질을 유지하는 것은 일반국민을 보호하고, 그들의 자유와 프라이버시를 보호하며 사법의 집행에 있어서 일반국민의 신뢰를 유지하는데 있어서 필수적인 부분이다. FSR은 경찰과 전반적인 형사사법시스템에 법과학 서비스를 제공하기 위한 품질표준을 확립하고, 이러한 표준의 준수 여부를 모니터함으로써 이러한 부분에서 핵심적인 역할을 하고 있다. 하지만 FSR은 그러한 표준에의 준수를 강제할 법률상 권한이나 힘이 가지고 있지는 않다.[359] 즉, 영국의 경우 형사사법시스템에 대한 포렌식 서비스의 제공은 법률적인 근거 없이 자율적으로 규제되고 있다. 다행히 현재까지는 법정에서 디지털 증거가 신뢰를 받을 수 있도록 결함을 조사하고, 높은 수준의 표준을 유지하는 것이 포렌식 서비스제공자와 경찰 모두에게 이익이 되기 때문에, 포렌식 서비스에 대한 자율적 규제가 현재까지는 효과적이라 할 수 있다.[360]

하지만 범죄현장에서부터 경찰 또는 민간실험실에 의한 분석을 거쳐 법정에 증거로 제출할 때까지 포렌식 증거에 대한 국민의 신뢰를 담보해야 하는 정부의 입장에서, 최근 몇 년동안 법적 규제체계 없이 포렌식 분석을 수행하는 기관의 수가 급격히 증가하고 있는 상황에서 포렌식서비스 기관들이 필수적인 표준들을 충족하지 못할 수도 있다는 문제에 대해 관심을 가질 수 밖에 없는 것이다.[361] 앞으로도 계속하여 표준들이 유지될 수 있도록 보장하기 위해서는 법률적인 근거가 필요하기 때문에 FSR에 대한 법적 권한의 부여를 검토하고 있는 것이다. 즉 영국 정부는 FSR의 역할과

---

357) Forensic Science Regulator,op.cit., p.4.
358) ibid.
359) Home Office, Consultation on new statutory powers for the forensic science regulator, 2013, p.4.
360) Home Office, Consultation on new statutory powers for the forensic science regulator, 2013, p.8.
361) Home Office, op.cit., p.9.

포렌식 표준에 관한 FSR의 기존의 실무규범을 법적인 근거위에 두고자 하는 것이며, FSR에 오판의 심각한 위험을 초래할 수 있는 품질 미달에 관한 조사권한을 부여하고자 하는 것이다.[362] 이에 따라 내무성은 2013년 법적권한부여에 관한 검토보고서를 작성하여 업무를 진행하고 있다.

4) FSR의 실무와 행동규범(Codes of Practice and Conduct)

가) 실무와 행동규범의 배경과 범위

형사절차법 위원회(Criminal Procedure Rules Committee)는 법원이 전문가 의견이 증거로서 허용될 수 있을 정도로 충분히 신뢰할 수 있는 것인가의 여부를 판단할 필요가 있기 때문에, 전문가에 대해 그들의 보고서 안에 그러한 정보를 제공할 책임을 추가했다.[363] 그리고 전문가 의견의 신뢰성을 판단함에 있어서 고려되어질 수 있는 것이 무엇인가에 관하여, 법원에 지침을 제공하는 형사절차법 part 33을 보완하는 형사실무명령을 수정하였다. 즉 전문가 의견의 신뢰성을 판단함에 있어서 법원이 고려하도록 요청되는 요인들은 다음과 같다.[364]

a. 데이터의 범위와 품질, 사용된 방법의 유효성
b. 만약 의견이 적절히 설명된 경우, 행해진 추론이 얼마나 안전한가 또는 위험한가
c. 방법의 정확성
d. 전문가 의견이 토대로 삼은 모든 범위의 자료는 다른 사람에 의해 리뷰된다
e. 전문지식의 범위
f. 전문가에게 활용가능한 정보의 완전성
g. 당해 문제에 관하여 다양한 전문가 의견이 있는가의 여부
h. 그 분야에서 확립된 실무와의 차이

이를 반영하여 FSR은 2014년에 형사사법시스템내에서 포렌식 서비스 제공자와 실무자들을 위한 “실무와 행동규범(Codes of practice and coduct)”을 출간하였다.

---

362) ibid.
363) Forensic Science Regulator, Codes of Practice and Conduct for forensic science providers and practitioners in the Criminal Justice System, ver.2.0 2014, p. 2.
364) ibid.

실무와 행동규범은 법과학 실무자에 대한 행동규범과 법과학 서비스 제공자에 대한 실무규범으로 되어 있다.

먼저 법과학 실무자에 대한 행동규범으로는,

"1. 최우선시 되는 의무는 법원과 법집행기관에 대한 것이다.
2. 정직·무결성·객관성·공정성을 가지고 행동하고, 가장 빠른 기회에 이해충돌로 인식될 수 있는 모든 인적·사업적·재정적 이해관계를 분명히 하라
3. 전문적인 능력의 한계 내에서만 전문가 자문과 증거를 제공하라
4. 관련분야 내에서의 주목할만한 연구 및 개발을 고려하면서, 전문적인 능력을 유지·개발하기 위한 모든 합리적인 조치를 취하라.
5. 보유하게 된 물품의 무결성과 연속성을 확립하고, 보유하는 동안에 무결성과 연속성이 유지된다는 것을 보장하라
6. 결과물에 중요한 영향을 미칠 수 있는 증거물/증거로서 작성된 기록/정보에의 접근을 모색하라
7. 유효성을 입증할 수 있는 방식을 활용하여 업무를 하라
8. 결과물에 중요한 영향을 미칠 새로운 정보 또는 상황이 있다면 모든 업무를 재검토할 준비를 하라
9. 만약 오판을 초래할 수 있는 상황이 있다고 믿을만한 정당한 근거가 있다면 기관내 적절한 사람에게 알려라
10. 법률상 의무, 법원 명령, 고객의 명시적인 권한 공개가 아닌 한 비밀을 유지하라"[365]고 기술하고 있다.

다음으로 실무와 행동규범이 대부분을 내용을 차지하고 있는 법과학 서비스 제공자에 대한 실무규범은 BS EN ISO/IEC 17025:2005(시험 및 교정 실험에 관한)에 맞춰 조정된 것이며, 실험에 기반한 법과학 서비스의 제공자들이 형사사법시스템 내에서의 고객의 요구사항을 충족하는 일관된 결과와 서비스를 제공할 수 있는 능력을 입증할 수 있는 관리시스템에 관한 요건들을 명시하고 있다.[366]

---

365) Forensic Science Regulator, Codes of Practice and Conduct for forensic science providers and practitioners in the Criminal Justice System, ver.2.0, 2014, p.9.

이 실무규범의 주된 주제는 국제적 표준인 BS EN ISO/IEC 17025:2005의 관련조항과 용이한 이용을 위해 해석을 제공하는 문서인 ILAC-G19:2002를 상호참조 하도록 하는 것이다. 하지만 이 실무규범은 국제적인 표준을 대신하고자 의도하는 것은 아니다.[367] 이 실무규범에의 준수는 효과적인 관리시스템을 적용하여 고객 만족도를 높이고 포렌식 과학에 대한 신뢰도에 있어서 형사사법시스템과 일반국민들에게 신뢰를 제공하고자 의도된 것이다. 따라서 모든 실무자들은 실무규범안에 포함된 원칙들을 준수해야만 한다.[368] 이 실무규범과 부속자료들은 BS EN ISO/IEC 17025:2005[369], BS EN ISO/IEC 17020:2012[370], ILAC-G 19:2002[371] 등의 요건에 있어서 관련한 변화를 반영하여 업데이트 된다.[372]

이 실무규범은 현장에 기반한 요소와 실험실에 기반한 요소를 가진 과학을 포함할 수 있도록 의도된 것이므로, 다음과 같은 업무범위에 적용된다. 즉 초기 현장에서 법과학 활동, 현장조사 전략, 증거물의 복구·보존·이전·저장, 현장에서 이용할 선별심사, 증거물의 평가·선정·조사·샘플링·심사·분석, 실험에 기반한 방법론을 활용한 테스팅 활동, 취해진 활동의 기록, 조사와 테스트 결과에 대한 평가와 리뷰, 결과의 보고와 제출, 해석과 의견 등이 그것이다.[373]

형사사법시스템에 법과학 서비스를 제공하는 모든 실무자와 제공자들은 이 실무규범에 구속된다. 하지만 때때로 다른 전문분야의 전문가가 증거를 제공하도록 요청되는 경우가 있는데 이 경우 그러한 제공자가 최소한 행위규범을 알고 있도록 해야 하며 그에 따르도록 요구해야 한다.[374]

---

366) Forensic Science Regulator, op.cit., p.10.
367) Forensic Science Regulator, Codes of Practice and Conduct for forensic science providers and practitioners in the Criminal Justice System, ver.2.0, 2014,p.10.
368) Forensic Science Regulator, op.cit., p.11.
369) 국제표준화기구에 의해 제정된 실험실 또는 교정기관이 능력에 관한 일반요구사항의 국제표준규격.
370) 검사기관 운영기준
371) 국제실험실 인증협회(International Laboratory Accreditation Cooperation)가 만든 법과학 실험실 가이드라인
372) Forensic Science Regulator, op.cit., p.11.
373) Forensic Science Regulator, op.cit., pp.11-12.
374) ibid.

나) 디지털 포렌식 서비스에 대한 실무와 행동규범

이 규범은 FSR의 실무와 행동규범의 부속자료로서, 디지털 포렌식 서비스 제공자로 하여금 '형사사법시스템내의 실무자와 법과학 제공자에 관한 실무와 행동규범'에 따르도록 하며, 범죄현장 활동에 관한 표준인 BS EN ISO/IEC 17020:2012 그리고 모든 실험실 기능에 관한 표준인 BS EN ISO/IEC 17025: 2005에 따라 승인을 받도록 하고 있다.[375] 이 부속규범은 디지털 분석의 제공에 특별히 관계된 실무규범의 요건들 가운데 몇가지에 대한 추가적인 설명을 제공하는 것이다.[376]

이 부속규범은 디지털 포렌식 업무가 디지털 데이터 저장매체와 모바일 전화 장치에 있어서 데이터의 식별, 캡쳐, 보존, 조사, 평가, 보고, 저장에 적용할 때에만 적용한다. 이 부속규범에 기술되어 있는 내용은 크게 기술적 기록, 테스트 방법(방법의 선택), 방법의 인증(위험평가방법, 측정에 기반한 방법의 인증, 채택된 방법의 인증 확인, 방법에 있어서 사소한 변화의 확인), 테스트 물품의 취급(증거물 취급, 보호, 저장), 리뷰 등이며, 각각의 항목에 있어서 참조해야 하는 ISO/IEC 17025:2005 또는 실무 및 행동규범 등이 제시되어 있다.[377]

2. 디지털 포렌식 관련 지침 및 가이드라인 -Good Practice Guide for Digital Evidence[378]

가. 개요

이 best practice guide는 Association of Chief Police Officers(ACPO) Crime Business Area에 의해 제작된 것으로, 법집행기관을 지원하기 위한 것 뿐만 아니라 사이버 보안사고와 범죄를 조사함에 있어서 지원하는 모든 사람들을 위한 지침으로서 제공하는데 목적을 두고 있다.[379] 이 지침은 디지털 포렌식 부서 내에서 행해지는

375) Forensic Science Regulator, Codes of Practice and Conduct : Appendix:digital Forensic Service, Issue1, 2014, p. 3.
376) ibid.
377) Forensic Science Regulator, op.cit., pp. 4-8.
378) http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf; 2016.9.10. 원문 전체를 다운로드 받을 수 있다.
379) Association of Chief Police Officers, ACPO Good Practice Guide for Digital Evidence, ver.5, 2012, p.2.

업무에 막대한 영향을 미치는 기술적 변화 그리고 법적·정책적 변화에 따라 리뷰를 통해 업데이트 되어진다.

나. 적용대상

이 지침서는 우선적으로 디지털 증거를 취급하는 영국 법집행직원들을 위해 쓰여진 것이므로,

"ⅰ) 디지털 증거를 복구할 목적으로 수색현장으로부터 장비의 확보·압수·이송에 관련된 사람들, 그리고 범죄수사를 위해 필요한 디지털 정보의 식별에 관여하는 사람들

ⅱ) 디지털 증거의 식별·제출·저장을 계획하고 관리하며, 그 증거를 이용하는 조사자

ⅲ) 디지털 증거를 복구하고 재생산하는 사람들, 그리고 그 기능을 수행하도록 훈련을 받은 사람들, 그리고 법정에서 자신이 행한 조치에 대하여 증언을 제공하도록 관련 훈련을 받은 사람들

ⅳ) 디지털 증거의 복구·식별·해석에 있어서 지원을 하도록 요청을 받을 수 있는 사람들의 선정과 관리에 관련되어 있는 사람들"[380]이 그 적용대상이다.

다. 디지털 증거에 관한 원칙

이 지침서는 디지털 증거에 관한 원칙과 그 원칙에 대한 세부적인 설명을 기술하고 있다.

먼저 디지털 증거에 관한 원칙으로는 다음 4가지를 제시하고 있다.

"Principle 1 : 법집행기관, 그 기관에 채용된 사람 또는 그들의 소속직원 어느 누구도 차후에 법정에서 요구될 수 있는 데이터를 변경해서는 안된다.

Principle 2 : 어떤 사람이 원본 데이터에 접속할 필요가 있다는 것을 발견한 경우, 그 사람은 그렇게 할 수 있는 자격이 있어야 하고, 그러한 조치의 중요성과 함의를 설명하는 증거를 제공할 수 있어야 한다.

---

380) ACPO, op.cit., p.6.

Principle 3 : 디지털 증거에 적용된 모든 프로세스에 대한 기록과 감사추적(audit trail)이 만들어져야 하고 보존되어야 한다. 독자적인 제3자가 그러한 프로세스를 조사할 수 있어야 하고 동일한 결론에 도달할 수 있어야 한다.

Principle 4 : 수사를 담당하는 사람은 법률과 원칙이 고수되도록 종합적인 책임을 진다."[381]

라. 디지털 포렌식 프로세스

ACPO 지침서는 Sec.3 - Sec.7에 걸쳐서 디지털 포렌식 프로세스를 단계별로 기술하고 있다.

1) 계획(Plan)

디지털 매체의 급증과 디지털 통신수단의 진보로 인하여 디지털 증거가 잠재적으로 존재할 가능성이 있는 소스의 유형을 확인하여 확보하는 것이 중요하게 되었다.[382] 따라서 조사자는 디지털 증거의 존재를 식별하고, 조사 전체에 걸쳐 증거를 보존하고 해석하기 위한 적절한 전략을 개발하는 것이 중요하다. 이 단계에서는 디지털 포렌식 업무가 행해지는 전체적인 조사에 있어서의 이익에 대한 정당한 고려가 주어져야 하며, 디지털 포렌식 조사의 제한된 자원을 적절히 통제하기 위해 디지털 포렌식 전략이 검토될 때 비례성 여부가 평가되어야 한다.[383]

2) 수집(Capture)

증거의 수집과 관련하여 지침서가 기술하고 있는 내용은 크게 비례성 문제, 정당성 문제 그리고 절차의 연속성 문제이다. 먼저 압수와 관련한 비례성 문제로는 압수물품의 증거보유 가능성 여부 및 압수 범위를 고려해야 하고, 정당성의 문제와 관련해서는 수색의 책임자가 피압수자의 물건을 이동하기 위한 합리적인 근거와 정당화 사유가

---

381) ibid.
382) Association of Chief Police Officers, ACPO Good Practice Guide for Digital Evidence, ver.5, 2012, p.7.
383) Association of Chief Police Officers, op.cit., p.8.

있어야만 한다는 점을 강조하고 있다.[384] 이와 관련하여 Police and Criminal Evidence Act(PACE) 실무규범의 수색규정, 수색영장, 유럽 인권협약의 적용 등이 고려되어야 한다.[385] 절차의 연속성과 관련해서는 앞서 기술한 Principle.3.에 따라 디지털 증거와 관련하여 행해진 모든 조치들에 대한 기록이 보관되어야 하는데, 그 기록에는 장비가 있는 장소의 사진/도표, 현장에 있는 사람에 의해 제공된 모든 정보에 관한 세부사항, 현장에서 취해진 모든 조치에 대한 기록이 포함되어야 한다고 기술하고 있다.[386]

3) 분석(Analysis)

디지털 장치에 저장된 데이터의 분량과 복잡성으로 인해 조사자가 해당 장치 안에 저장된 모든 데이터를 추출하는 것은 가능하지도 바람직하지도 않을 수 있다. 따라서 조사자는 디지털 조사의 목적과 성격을 고려하여 조사의 우선순위를 명확히 해야 한다.[387] 조사시 검토해야 할 데이터의 양이 엄청나게 많은 경우에는 그러한 데이터를 검토할 최적임자가 누구인가에 대한 고려가 행해져야만 한다. 또한 복구된 디지털 증거의 입증가치가 명확하다는 것을 확실히 해야 하므로, 디지털 데이터에 대한 해석을 담당하는 실무자는 그와 관련한 권한과 임무수행을 위한 훈련을 받아야만 한다.[388]

디지털 증거의 분석과 관련해서 실무자들은 급격한 디지털 기술의 발전으로 인해 자신의 지식에 대한 중대한 도전에 직면할 수 있다는 것을 항상 염두에 두어야 하고, 따라서 디지털 포렌식 조사에 있어서 자신의 지식의 한계를 인식하고, 그 이상의 조사 또는 추가적인 전문적인 지식을 요하는 경우가 있을 수 있음을 항상 인식하고 있어야만 한다.[389]

4) 제출(Presentation)

디지털 포렌식 실무자는 중립성의 의무를 인식하고 있어야만 하며, 디지털 포렌식 증거의 범위와 한계를 둘다 전달해야만 한다.[390]

---

384) Association of Chief Police Officers, op.cit, pp.8-9.
385) Association of Chief Police Officers, op.cit., p.9.
386) Association of Chief Police Officers, op.cit, p.9, 10.
387) Association of Chief Police Officers, op.cit, p.10.
388) Association of Chief Police Officers, op.cit, p.10.
389) ibid.

디지털 포렌식 조사의 결과는 사건전체에 걸쳐 조사자/수사관에게 구두로 전달되거나, 그 사건의 결과에 대한 진술서 또는 보고서로 전달되며, 증언이 요구되는 경우 법정에서 전달된다.[391] 먼저 구두에 의한 피드백은 조사과정 전체에 걸쳐 정기적으로 제공되는 것으로 차후 공개를 위해 이메일을 통해 덧붙이거나 영상녹화물로 기록하는 것이 good practice이다.[392] 다음으로 디지털 포렌식 조사의 최종산물인 진술서 또는 보고서는 독자가 이해할 수 있도록 기술되어야 하고, 특정 항목이 보고서안에 재작성된 경우에는 그 표현이 정확하다는 것을 담보할 수 있는 조치가 취해져야 한다. 그리고 보고서에 포렌식 실무자의 의견증거가 제공된 경우에는 이 의견이 토대를 둔 사실을 기술해야 하며, 어떻게 그가 이러한 결론에 이르렀는지에 대해서는 기술해야 한다.[393] 마지막으로 실무자는 조사를 수행하는 것 뿐만 아니라 그 절차의 유효성, 조사를 행하기 위한 경험과 자격에 대해 증언을 할 수도 있다. 이와 같이 증거를 제공하는 경우 실무자는 사실을 표현할 때와 의견을 제공할 때를 명확하게 구분해야 하며, 전문가 증거를 제공하는 경우 자신의 전문영역에 한해서만 해야 한다.[394]

5) 일반적 사항(general)

이 지침서는 마지막 Section 7에 일반적 사항으로서 디지털 포렌식 업무에 종사하는 사람들의 전문성 개발을 위한 훈련과 교육[395], 업무수행에 있어서의 위험(심리적·신체적· 생물학적)과 그로 인한 잠재적 영향력의 최소화를 위한 조치[396], 디지털 포렌식 계약에 있어서 ISO 17025, ISO 17020의 표준에 따른 인증에의 준수 및 계약자에 대한 데이터보호법 규정준수 및 참여기관 내부정책에의 준수[397], 증거개시와 관련한 법무부지침, CPS 매뉴얼, CPIA 실무규범 참조[398]와 관련한 내용들이 기술되어 있다.

---

390) Association of Chief Police Officers, op.cit, p.12.
391) ibid.
392) ibid.
393) ibid.
394) ibid.
395) Association of Chief Police Officers, op.cit, p.13.
396) Association of Chief Police Officers, op.cit, p.13.
397) Association of Chief Police Officers, op.cit, p.14.
398) Association of Chief Police Officers, op.cit, pp.14-15.

제3절 EU의 디지털 포렌식 시스템

1. 유럽 법과학연구소 네트워크(ENFSI)

가. ENFSI의 개요

ENFSI(European Network of Forensic Science Institutes)는 유럽의 법과학연구소들이 법과학 분야의 전문지식을 공유하고, 교환하기 위해서 만들어진 네트워크이다. 무엇보다 선제적으로 전 세계적으로 법과학 분야에서 문제시 되는 내용들을 인식하고, 유럽 차원에서 법과학의 수준을 향상시키고 새로운 기술을 전파하기 위한 것을 목적으로 삼고 있다.[399] 따라서 ENFSI의 기반구축과 강화, 기술발전과 신뢰성 확보를 통한 유럽차원의 멤버십 확대, 해외 다른 국가 및 지역의 유사 기관과의 관계설정, 경쟁력 제고를 위해 ENFSI의 연구소에 최고의 기술과 국제적 기준 적용 등을 위해 노력하고 있다.[400] 그를 위해 관련 회의나 세미나, 협동연구 및 숙련도 검사 등의 활동을 하고 있으며, 관련 파트너들에 대한 포렌식 이슈들에 대한 조언, 포렌식 관련 실무메뉴얼 등을 간행하기도 한다.[401]

ENFSI는 1992년 서유럽의 몇몇 법과학 연구소들이 정기적으로 서로 관련 있는 주제들에 대해 회의를 하는 것으로 시작되었다. 이후 1993년 네덜란드의 Rijswijk에서 11개 연구소들이 ENFSI를 만드는 것에 합의하고, 그 범위를 유럽 전역으로 확대하였다.[402] 하지만 실제적인 창립은 1995년 10월 20일 네덜란드 Rijswijk에서 각 참여기관들이 정식으로 양해각서에 서명을 하고, 위원회를 선출하고, 로고를 만들면서 이루어졌다. 그리고 나서 1999년 Moscow 회의에서 헌법이 회원들에 의해 승인되었고, 2002년 회원들의 재정부담에 의해 사무국이 설립되었으며, 네덜란드 법과학 연구소가 그 역할을 수행하게 되었다. 그리고 2009년에는 유럽이사회(European Council)에 의해 유럽 법과학에 대한 독점적 지위를 인정받게 되었다.[403] 그러므로 유럽에서 법과학과 관련된 사안에 대해서는 ENFSI의 견해가 매우 공신력 있고, 의미있는 역할

399) http://www.enfsi.eu/about-enfsi;2016.9.30.
400) ibid.
401) ibid.
402) http://www.enfsi.eu/about-enfsi/history;2016.9.30.
403) ibid.

을 수행하게 되었다. 현재 ENFSI의 총 회원수는 36개 국가의 66개에 달하고 있으며, 유럽 이외에도 Europol, Eurojust, UNODC(United Nations Office on Drugs and Crime), AFSN(Asian Forensic Sciences Network) 등 여러 기관들과 협력을 하고 있다.[404]

나. ENFSI의 조직체계

ENFSI의 조직은 크게 이사회, 사무국, 상임위원회, 전문가 작업그룹, 그리고 프로젝트 그룹으로 이루어져 있다.[405] 이사회는 3년 임기의 총 5명으로 구성되어 있고, ENFSI의 최고 권한을 가지고 있으며, ENFSI의 정책을 결정한다.[406] 또한 사무국은 그 자체로 법적 지위를 가지고 있으며, 위원회의 감독을 받고, 주요 업무는 일반적으로는 ENFSI 커뮤니티를 지원하고, 특정한 부분에 있어서는 위원회를 지원한다. 또한 ENFSI의 웹사이트를 관리하며, 특별한 워킹 그룹이 관리하는 콘텐츠의 편집에도 관여한다.[407]

ENFSI에는 크게 Quality & Competence Committee와 Research & Development Committee의 두 상임위원회가 있다. 전자는 주로 자질과 경쟁력을 발전시킬 수 있는 정책, 전문가작업그룹 및 회원들에 대한 조언, 회원 연구소들에 대한 최선의 실무와 국제적 표준 적용과 관련된 업무들을 수행하고, 후자는 ENFSI의 연구개발 정책, 전문가작업그룹 및 회원들에 대한 연구개발 관련 조언, 연구소간 국제적인 협동연구 촉진 등의 업무들을 수행하고 있다.[408] 그리고 ENFSI에는 총 17개의 전문가작업그룹이 존재하고 있다. 해당 그룹은 동식물 및 토양의 흔적(Animal, Plant and Soil Traces), 디지털 이미징(Digital Imaging), DNA, 문서(Documents), 약물(Drugs), 폭발물(Explosives), 지문(Fingerprint), 총기(Firearms/GSR), 화재 및 폭발조사(Fire and Explosions Investigation), 정보기술 포렌식(Forensic Information Technology), 음성 및 오디오 분석 포렌식(Forensic Speech and Audio Analysis), 필적(Hand-

404) http://www.enfsi.eu/about-enfsi/external-relations;2016.9.30.
405) http://www.enfsi.eu/about-enfsi/structure;2016.9.30.
406) http://www.enfsi.eu/about-enfsi/structure/board;2016.9.30.
407) http://www.enfsi.eu/about-enfsi/structure/secretariat: 2016.9.30.
408) http://www.enfsi.eu/about-enfsi/structure/standing-committees;2016.9.30.

writing), 자국(Marks), 페인트와 유리(Paint & Glass), 도로 사고 분석(Road Accident Analysis), 범죄현장(Scene of Crime), 그리고 섬유 및 머리카락(Textile and Hair)으로 구분되어 있다.

이 가운데 정보기술 포렌식 작업 그룹(Forensic Information Technology: FIT)의 활동이 본 보고서의 주제와 관련을 맺을 수 있다. 따라서 그에 대해서는 별개로 살펴보고자 한다.

다. FIT의 개요

FIT는 컴퓨터나 네트워크, 전자기기 등에 있는 정보를 조사하고, 수사나 법원에 제출할 증거를 제출하는 등 모든 과학기술적 훈련과 관련된 업무에 중점을 두고 있다. 따라서 컴퓨터 데이터 분석이나 인터넷 수사의 기술적 관점, 전자기기 조사 등과 관련된 활동을 하고 있으며, 그에 대한 전문가들이 참여하고 있다.[409] 그러므로 FIT작업 그룹은 ENFSI의 글로벌 목적에 순응하도록 조직을 유지하고, ENFSI 회원 연구소들의 정보기술 포렌식을 발전시키고 촉진시키며, 디지털 증거와 관련된 다른 작업 그룹들과의 협력을 구축하고, 정보기술 포렌식의 품질을 확보하며, 중요한 기술관련 기관들과의 관계고 구축하는 것을 목적으로 삼고 있다.[410] 그를 위해 매년 FIT 작업 그룹 회의를 개최하고, 품질 재고·연구개발·교육훈련을 위한 위원회를 운영하고 있다. 그를 위해 FIT 작업 그룹 내에는 의장과 부의장, 사무국, 품질 재고 운영자, 연구개발 운영자들, 교육훈련 운영자들, 프로그램 운영자 등으로 조직이 구성되어 있다.[411]

예를 들어, FIT 작업 그룹이 2015년 11월 작성된 "Best Practice Manual for the Forensic Examination of Digital Technology"를 살펴보면,[412] 해당 매뉴얼은 ENFSI 회원 연구소들에 대해 관련 절차에 대한 프레임워크와 품질재고 원칙들, 훈련

---

409) http://www.enfsi.eu/about-enfsi/structure/working-groups/information-technology; 2016.9.30.

410) http://www.enfsi.eu/sites/default/files/documents/terms_of_reference_fitwg_v2_20141120_0.pdf.;2016.9.30.

411) ibid.

412) http://www.enfsi.eu/sites/default/files/documents/enfsi-bpm-fit-01_2.pdf('디지털 포렌식을 위한 모범 실무 매뉴얼'); 해당 매뉴얼은 ENFSI에서 발간하는 매뉴얼 시리즈 가운데 하나이다. 각각의 매뉴얼들은 작업 그룹에서 만드는 것이며, 일부 유사한 주제들은 하나로 합쳐져 나오기도 한다.

과정과 포렌식 조사를 위한 접근방법 등을 제시해 주고 있다. 특히 해당 매뉴얼은 국제적으로 표준화된 절차가 각 지역에 맞게 적용될 수 있도록 지원을 해 주고 있다. 따라서 매뉴얼을 살펴보면 목적과 범위, 용어 정의, 자원들, 방법들, 검증방법과 측정 도구의 불확실성에 대한 평가방법, 숙달정도 테스트 방법, 도구 사용방법, 현장에서의 사건 평가, 조사의 우선순위와 순서, 사건의 재구성 방법, 평가방법과 해석방법, 증거의 제출방법, 건강과 안전, 관련 문헌들 뿐 아니라 이전 매뉴얼과의 차이점 등에 대해서 상세히 설명하고 있다. 이처럼 ENFSI 회원 연구소에 대해 디지털 포렌식과 관련된 중요한 내용들을 제공함으로 해서 디지털 포렌식에 대한 회원 연구소들의 품질을 상향시키도록 노력하고 있다. 따라서 해당 매뉴얼은 사실상 유럽의 디지털 포렌식에 있어서 규범적인 역할을 수행하게 되므로 그 내용을 뒤에서 좀 더 자세히 살펴보고자 한다.

라. 유럽에 있어서 ENFSI의 의의

유럽에서의 ENFSI의 존재는 디지털 포렌식 분야에 있어서 크게 네 가지 의미에서 중요하다고 생각된다. 첫째로, ENFSI는 유럽의 공신력 있는 표준을 만들어 디지털 포렌식의 국가별, 연구소별 편차를 해소하고 있다. 디지털 포렌식 절차는 단순히 디지털 증거를 수집하여 법정에 제출하는 과정은 아니다. 그 절차 가운데는 과학이 자리잡고, 인력·도구·여러 물질·행정체계 등 다양한 요소들이 영향을 미치게 된다. 그러므로 아무리 우수한 디지털 포렌식 기술이 있더라도 해당 기술이 표준화 되지 못하고 공신력을 얻지 못한다면 결코 법정에서 증거로 사용할 수 없게 된다. 그런데 ENFSI는 유럽차원에서의 표준을 설정하는 역할을 통해 그와 같은 문제를 해결해 주고 있다.

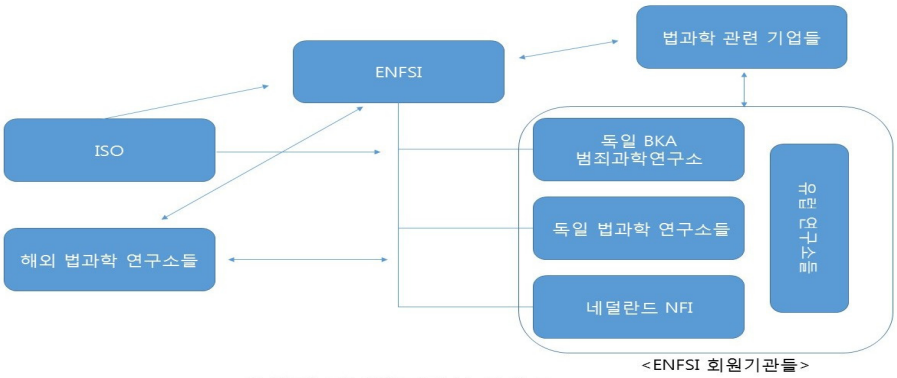
둘째로, 다른 지역의 디지털 포렌식 표준과 접목시키는 작업을 수행하고 있다. 디지털 포렌식은 한 국가, 한 지역에만 해당하는 것이 아니고 전 세계와 관련을 맺게 된다. 이는 현대의 글로벌 사회에서의 소송은 결코 한 국가 내에만 이루어지지 않고 있으며, 다국적 기업이 많아지고 있는 상황에서 소송절차와 증거절차는 매우 복잡하게 얽히게 된다. 그런 가운데 디지털 증거의 표준이 단지 유럽차원에서만 통용된다면 다른 국가나 지역에서는 증거로 사용될 수 없는 문제가 생긴다. 따라서 ENFSI는 다양한 모범 실무 매뉴얼이나 관련 문건들을 통해 국제적으로 통용되는 기준을 유럽차원

으로 이식하는 역할도 수행하고 있다. 예를 들어, 국제표준기구인 ISO의 연구소 관련 표준이나 법과학 관련 표준을 적극적으로 반영하고, 미국 등에서 통용되는 표준도 면밀하게 분석하여 적용하고 있다.

셋째로, 디지털 포렌식 절차에서 요구되는 인력·도구·장비·물질 등 세세한 부분에 있어 구체적인 지침을 제공해 주고 있으며, 최신의 기술을 소개해 주고 있다. 그로 인해 디지털 포렌식의 관련 요건들에 있어 최신의 기술이 적용될 수 있도록 도와주고 있다. 디지털 포렌식 기술은 하루가 다르게 발전하고 있기 때문에 비록 시스템이 잘 구축되어 있다고 하더라도 그 안에 적용되는 기술들이 이전 기술이라면 신뢰성을 잃게 된다. 그러므로 ENFSI는 관련 작업 그룹을 설치하고, 관련 전문가들을 참여시켜 최신의 기술이 반영될 수 있도록 노력하고 있다. 그를 위해 매년 정기 회의를 개최하기도 하며, 특별 프로젝트를 수행하기도 한다.

넷째로, 각 국가 및 연구소에 맞는 커스터마이징(Customizing) 작업도 수행하고 있다. 디지털 포렌식은 유럽 뿐 아니라 전 세계적으로 표준화가 요구되고, 사용된다고 하지만, 아직까지는 각 국가에서 요구하는 수준이나 정도가 상이한 실정이다. 그런 가운데 가장 진보적인 모범 실무 매뉴얼을 작성하고, 모든 국가들에 적용시킨다면 분명 해당 국가의 현실과 충돌하는 문제가 발생하게 된다. 그러므로 ENFSI는 구축된 표준이 각 국가들에 커스터마이징 되어 적용될 수 있도록 도와주는 역할도 수행하고 있다.

이처럼 ENFSI는 법과학과 관련해서 사실상 유럽의 컨트롤 타워의 역할을 수행하고 있다. 물론 이는 유럽연합이라는 지역적 특색으로 인해 구축된 것이기는 하지만 그 내용을 살펴보면 개별 국가에서도 그와 같은 메커니즘을 적용할 수 있을 여지가 있다.



[그림 12] EU내 디지털 포렌식 연구소

2. 디지털 포렌식 관련 지침 및 가이드라인

가. Best Practice Manual for the Forensic Examination of Digital Technology

1) 목적과 범위

이 Best practice Manual(BPM)[413]은 2015년에 ENFSI에 의해 발간된 것으로, 포렌식 조사절차에 관한 체계, 품질원칙, 교육훈련 프로세스와 포렌식 조사에 관한 접근방법을 제공하는데 목적을 두고 있다.[414] 이 BPM은 신뢰할 수 있는 결과를 산출하고, 확보한 정보의 품질을 최대화하며, 강력한 증거를 생산하는 포렌식 IT 조사분야에 있어서의 업무관행을 확립·유지하기 위한 것으로 ENFSI 회원 실험실과 다른 법과학 실험실에서 활용될 수 있다.[415] 즉 이 매뉴얼의 의도는 국제적 표준요건 그리고 국내 표준요건들과 각 회원들의 실험환경내에서의 실제적인 실행간에 도움이 되는 가교를 제공하고자 하는데 있으며, 국내 규제요건들과 국제적 기준에 따른 국내 표준운영절차(local standard operation procedure:SOPs)의 설계를 지원하기 위한 기술적 지침

413) BPM이란 과학적으로 승인된 practice를 반영한다는 의미이지 이 매뉴얼에 열거된 pracitce가 포렌식 분야에서 활용되는 유일한 good practice라는 의미는 아니라고 설명하고 있다. ; ENFSI, Best Practice Manual for the Forensic Examination of Digital Technology, ver.01, 2015, p.6.
414) ENFSI, Best Practice Manual for the Forensic Examination of Digital Technology, ver.01, 2015, p.6.
415) ibid.

을 제공하는 것이다.[416]

이 BPM은 이 분야의 전문가를 대상으로 하는 것이며, 우선적으로 컴퓨터와 전화에 기반한 포렌식 형식에 있어서 일반적인 정보기술 분야의 best practice에 초점을 맞추고 있는데, 이는 이러한 분야들이 압수전부터 최종보고서의 작성과 보존에 이르기 까지 포렌식 프로세스를 전체를 포함하는, 디지털 시스템의 획득과 분석을 다루고 있기 때문이다.[417]

2) 구성내용

가) 자원(Resources)

자원들(Resources)에서는 인적자원(Personnel), 사용장비(Equipment), 기준자료(Reference Materials), 시설과 환경조건(Accommodation and Environmental Conditions), 기록보관(Archive) 등에 관해서 요구되는 요건들과 구체적인 방법들을 서술하고 있다.

먼저 인적자원과 관련해서는 행정인력과 기술인력으로 구성되는데, 특히 모든 기술인력에 대해서는 그들에게 할당된 역할에 부합하는 기술적 능력을 보유할 수 있도록 정기적인 능력시험을 행할 것을 권고하고 있다.[418] 그리고 포렌식 기술직원들은 다음의 사항에 대해 직접적인 책임은 지닌다고 기술하고 있다. "ⅰ) 국내 법률상 요건의 준수, ⅱ) 현재의 기술적 발전과 절차에 대한 최신정보의 반영, ⅲ) 형사사법시스템에 대한 이해, ⅳ) 디지털 기술/디지털 증거를 수반하는 사건에의 관여를 입증하는 증거에 대한 포트폴리오 유지, ⅴ) 포렌식 디지털 증거조사와 관련한 적절한 정보를 제공하는 저널 및 문헌의 읽기, ⅵ) 분석하는 과정에서 직면한 문제들에 대해, 그리고 그것을 극복하기 위해 채택한 방법에 대해 동료들에게 공식적인 피드백 제공, ⅶ) 해당 지역의 절차와 표준의 개발을 돕고, 조사에 관한 기술적 진보를 향상시키는 것"등이 그것이다. 따라서 모든 기술직원들은 내외부 훈련프로그램을 활용하여 최신상태를 유지해야 하고, 포렌식환경내에서의 조사에 관한 기술적 발전을 개선하기 위하여 해당 지역의 절차와 표준에 대해 제안된 변화에 대하여 엄격한 동료심사와 개발을 통해 품질관리

416) ibid.
417) ENFSI, op.cit., p. 7.
418) ENFSI, op.cit., p. 9.

를 지원해야 한다고 기술하고 있다.[419]

장비와 관련하여서는 포렌식 실험실 안에 보유하고 있는 모든 포렌식 도구의 제조사·모델·고유일련번호, 구매일자와 서비스 설치 일자, 장비의 각 아이템 위치, 유지상태와 검증상태가 기록된 장비목록 기록부를 유지해야 하며, 기록안에는 관련된 위험분석의 결과와 인증된 프로세스내에 배치된 모든 기능들에 대한 정기적인 재검증의 결과를 포함해야 한다[420]고 되어 있다. 그리고 이 매뉴얼은 실험실내의 프로세스상 대체도구의 사용이 충분히 허용될 수 있어야 하지만, 그 도구의 사용이 공식적으로 승인·기록되었으며, 도구를 채용하기 전에 자격있는 직원에 의해 사용된 기능의 특성에 대한 공식적 분석이 테스트되었다는 것을 보장할 수 있는 충분한 정책을 가지고 있어야 한다[421]고 기술하고 있다.

기준자료와 관련하여서는 실험실내의 테스트 세트의 디자인과 운용의 중요성, 테스트 세트 결과의 한계와 오류가능성에 대한 인식의 중요성을 기술하고 있으며, 시설과 환경조건에 있어서는 국내 규제기준을 준수해야 한다는 것과 특히 데이터 처리시 오류를 초래하거나 증거물을 훼손시킬 수 있는 전원공급장치 관리 그리고 정전기 방전과 정전기 간섭표준 운용절차의 시행의 중요성을 기술하고 있다.[422]

마지막으로 기록보관과 관련하여서는 사건관리시스템이 지속적으로 그리고 정확하게 모든 기록보관된 자료에 대한 이용자의 접근과 이동을 추적할 수 있는 것이 절대적으로 중요하므로, 기록보관 솔루션을 선택할 때 선택한 포맷이 기록보관 유지정책 및 절차 그리고 해당 솔루션 제조업체의 명세서 양자에 모두 적합해야 한다고 기술하고 있다.[423] 그리고 기록보관 정책과 절차에 관한 평가와 위험분석시 보관자료의 손상가능성을 고려해야 하고, 특히 노후한 기록보관 기술로부터 자료를 복구하거나 읽어들일 수 있는 방법과 관련한 잠재적인 문제들을 검토하도록 권고하고 있다.[424]

---

419) ENFSI, op.cit., p. 10.
420) ENFSI, Best Practice Manual for the Forensic Examination of Digital Technology, ver.01, 2015, pp.10-11.
421) ENFSI, op.cit., p.12.
422) ENFSI, op.cit., pp.13-15.
423) ENFSI, op.cit., p.15.
424) ENFSI, op.cit., p.16.

나) 방법(Methods)

이 매뉴얼이 제시하는 방법은 디지털 포렌식의 신뢰성을 높일 수 있는 방법으로서, 동료심사 또는 전문가에 의한 평가(peer review), 조사 프로토콜(examination protocols), 연구(research)를 중심으로 기술하고 있다.

동료심사 또는 전문가에 의한 평가는 평가되어지는 세부사항의 근거와 효력을 확보하기 위한 입증수단으로서, 그 분석에 참여하지 않은 사람에 의해서 그리고 그렇게 할 자격이 있는 사람에 의해서 행해져야 한다.[425] 이러한 동료심사 또는 전문가에 의한 평가의 결과로서 전문가들간의 의견차이가 해결되지 못한 경우에는 보다 심층적인 심사가 고려되어야 한다.[426]

조사 프로토콜과 관련하여서 이 매뉴얼은 정확한 조사 프로토콜을 상세히 기술하고자 하는 것이 아니라, ENFSI 회원들간의 핵심적인 공통사항을 공유하면서도 각자 자체적인 요건들에 맞추어진 실험 프로토콜을 개발하는데 활용되고자 하는 것이다. 따라서 각 실험실들은 그들이 채용한 모든 프로토콜이 그들의 요구사항 그리고 인증을 확보하기 위해서 규제기관에 의해 요구되는 요구사항들에 모두 부합한다는 것을 보장할 책임이 있다.[427]

마지막으로 포렌식조사의 신뢰성을 높이는데 있어서 연구는 새롭고 참신한 개발에 있어서 본질적인 역할을 하며 기존의 기술들을 합목적적인 것이 되도록 보장하는 것이라 할 수 있다.[428] 따라서 기초가 된 포렌식 기술에 대한 모든 best practice, 지침서, 연구논문, 표준운용절차들은 그들이 의도했던 구체적인 목적에 합당하게 활용되고 있는 승인된 방법들에 대한 공리를 보장하기 위해 지속적으로 면밀히 조사되어야 한다.[429] 특히 Best practice는 항상 엄밀하게 테스트되었거나 또는 보다 더

---

425) ibid.
426) ibid.
427) ENFSI, Best Practice Manual for the Forensic Examination of Digital Technology, ver.01, 2015, p.17.
428) ENFSI, op.cit., p.18.
429) 이 매뉴얼은 독자들에게 다음을 경계할 것을 권고하고 있다. "최종 출간된 문서안에는 발견되지 않은 오류들이 있을 가능성이 있다. 항상 해왔던 방식이고 현재 표준으로 추정되고 있기 때문에 또는 다른 모든 사람들이 하는 방식이기 때문에 하고 있는 것이 어떤 점에서는 명백히 결함을 안고 있는 것일 수 있다. 포렌식 기법에 있어서 패러다임의 전환이라고 하는 방법들이 단지 연구의 흠결 또는 기존의 활용가능한 방법에 대한 이해의 흠결로 인한 것일 수 있다"; ENFSI, op.cit., p.19.

엄격하게 증명된 공리에 의해 뒷받침되는 방법을 추구해야만 한다.[430]

다) 검증방법과 측정도구의 불확실성에 대한 평가방법(Validation and Estimaion of Uncertainty of Measurement)

모든 ENFSI 실험실들은 ENFSI 문서 QCC-VAL-002 "법과학에 있어서 도구와 사람에 기반한 방법에 대한 단일 실험실 검증에 관한 가이드라인(Guidelines for the single laboratory Validation of Instrumental and Human Based Methods in Forensic Science)"열거된 요건들을 숙지해야 하고, 이에 따른 검증이 행해질 것을 요구받게 된다.

도구의 기능에 대한 검증은 도구내의 모든 기능을 검증이 아니라 그 프로세스에 구체적인 것으로 제한되어야 한다. 즉 포렌식 IT 도구내에 존재하지만 사용되지 않은 다양한 기능들로 인해 그리고 결과를 산출해내기 위해 결합될 수 있는 포렌식 IT 도구내의 복합적인 방식들로 인해 검증은 맡겨진 구체적인 프로세스로 제한되어질 수 있는 것이다. 그리고 신뢰할 수 있는 프로세스를 만들기 위해서 검증은 개선된 프로세스를 증명하고, 사용자와 이용된 도구의 기능들이 알려진 위험과 오류의 범위 내에서 작동한다는 것을 실제 입증할 것을 요구하게 된다.[431] 따라서 검증 프로세스를 디자인할 때는 5가지의 핵심요소는 "알려진 오류와 불확실성에 대한 이해, 요구목록, 위험분석과 평가, 효과적인 인증 테스트 세트, 정기적인 검증"이다.[432]

다음으로 불확실성은 측정값과 참값의 알려지지 않은 차이로 완벽하게 정의되거나 제거될 수 없는 것이며, 주어진 신뢰수준 내에서 참값이 존재하는 한계영역으로 표현될 수 있다.[433] 따라서 시스템내의 불확실성은 본래 부가적인 것이며, 일반적으로 프로세스내에서 사용된 기능의 수에 따라 증가한다. 불확실성이 기능의 수준에서 계산될 수 있는 것인가 아니면 프로세스 수준에서 추출되는 것인가의 여부에 대한 판단은 각 실험실의 재량에 맡겨져 있다.[434] 오히려 불확실성을 갖고 있지 않다고 표명된 프로세스는 그렇게 말한 사람의 지식의 흠결로 인한 것이거나 진실된 정보를 혼란스

430) ENFSI, op.cit., p.19.
431) ENFSI, op.cit., p.21.
432) ibid.
433) ibid.
434) ENFSI, Best Practice Manual for the Forensic Examination of Digital Technology, ver.01, 2015, p.22.

럽게 만들기 위한 적극적인 시도로서 고려될 수 있다.[435]

디지털 포렌식 프로세스내의 불확실성은 모든 포렌식 기능들, 매체 식별 그리고 보호되거나 암호화된 영역들, 디스크 획득·보고서 기술과 독자 해석·기록보관 내에 존재하는 것이므로, 이러한 불확실성을 인정하고 기록하는 것이 중요하다.[436]

이와 함께 디지털 포렌식 프로세스내에서 통상 나타나지 않는 추가적인 위험에 대한 분석방법[437], 프로세스에 대한 지속적인 재검증[438], 도구와 장비에 기반한 기능검증 그리고 사용자와 인적자원에 기반한 기능검증[439]과 관련해서는 QCC-VAL-002와 best practice를 참고하도록 기술하고 있다.

라) 능력시험(Proficiency Testing)

능력시험은 IT 포렌식의 구체적인 품질을 테스트하고 확인하는데 이용되는 것으로, "ENFSI내 능력시험과 합동훈련의 시행에 관한 지침서"에서 그와 관련한 정보를 제공하고 있다.[440] 능력시험은 직원능력개발 요건을 공식적으로 실험실 적격성 심사의 일부로서 평가할 수 있는 매카니즘을 제공하는 것으로, 대외적인 능력시험과 실험실 내의 능력시험으로 나뉘어질 수 있다. 이 가운데 내부 능력시험은 허용가능한 범위내에 있는 기존 실험실 프로세스의 인적 자원에 기반한 위험을 지속적으로 검증할 수 있도록 효과적인 피드백을 제공할 수 있는 방식으로 디자인될 필요가 있다

그리고 직원개발에 있어서 중요한 직원훈련은 그 자체만으로 직원능력에 대한 평가를 구성하지는 않으므로, 훈련이 종료되는 시점에서 공식적으로 배운 것에 대한 평가, 적절한 자격을 가진 구성원에 의한 동료심사, 훈련코스의 결과로서 생긴 새로운 국소적인 기법 등에 대한 평가가 행해진다.[441]

마) 취급 항목(handling items)

이 매뉴얼의 맥락내에서 취급항목은 물리적인 압수, 보호, 전송, 현장 또는 실험실에서 차후의 분석을 위한 보존에 관한 것이다. 먼저 현장에서의 취급항목은 현장

435) ibid.
436) ibid.
437) ENFSI, op.cit., pp.23-24.
438) ENFSI, op.cit., p.25.
439) ENFSI, op.cit., pp.25-26.
440) ENFSI, op.cit., p.27.
441) ENFSI, op.cit., p.28.

참여전 사전준비와 현장요구사항에 대한 평가 관련 절차의 숙지, 압수·수색에 관한 경찰 가이드라인 준수, 증거의 오염 및 파괴가능성 배제를 위한 증거물 접근차단, 포렌식 프로세스의 중요성 및 파괴적 성질 여부에 따른 다른 포렌식 부서와의 작업 순서 협의, 압수시 현장복구항목 및 취급자·장소에 대한 정확한 기록 작성, 네트워크 및 전원 차단 그리고 Anti-ESD 조치와 RF차단 케이스내 봉인시 실험실 표준절차 준수 등이 있다.[442] 실험실에서의 취급항목은 조사 시작전 증거물의 연속성과 봉인에 의한 무결성 점검 및 입증, 증거물 최초 수령시 증거물 저장으로 인한 데이터 손실가능성 평가 및 예방조치 고려, 무선통신으로 인한 데이터 손실가능성 제한, Anti-ESD 수단 및 오염방지 예방조치에 대한 라벨링 등이 있다.[443]

바) 사건 평가(Case assessment)

사건 평가는 현장 이전 단계에서의 준비, 현장평가, 실험실 평가, 원격시스템에 대한 실시간 분석, 초기사건 평가방법, 사건자료 수집 등으로 구성되어 있다. 먼저 현장 이전단계에서의 준비에 있어서는 메모리상 실시간 동적 데이터·실시간 암호화·원격에 의한 시스템 리셋 방지의 확인과 캡쳐 관련 지식의 평가가 필요하며,[444] 현장평가는 제출된 증거물이 나중에 실험실내에서 효과적으로 처리될 수 있도록 현장에 있는 사람들에게 원격으로 제공된 지원과 조언에 대해서까지 행해진다.[445] 실험실에서의 평가는 현장평가와 유사한 가이드라인을 준수해야 하며, 다수 증거물이 제출된 사건의 경우에는 증거물 조사의 우선순위를 정하는데 신중해야 한다.[446] 원격 라이브 시스템에 대한 분석시에는 데이터 접근을 위한 법률상 제약과 국가간 제약이 있음을 인식해야 하고, 데이터의 전부 또는 일부가 국내 법률상 차단규제의 대상이 되는 통신데이터인 경우에는 추가적인 제약이 있을 수 있다는 점을 고려해야 한다.[447]

사) 조사의 우선순위와 순서(Prioritisation and Sequence of Examinations)

디지털 증거에 대한 조사를 시작하기 전에 비례적으로 고려해야 할 사항과 분석순

442) ENFSI, Best Practice Manual for the Forensic Examination of Digital Technology, ver.01, 2015, pp.29-30
443) ENFSI, op.cit., p.30.
444) ENFSI, op.cit., p.31.
445) ibid.
446) ENFSI, op.cit., p.32.
447) ibid.

서를 결정하기 위한 리뷰가 행해져야 한다.[448] 조사 프로세스 전체에 걸쳐 고객(경찰)과의 소통이 유지되어야 하는데 이는 그 자료가 조사에 도움이 될 수 있을지 없을지는 고객(경찰)이 가장 알고 있기 때문이다. 이 경우 증거물 추출의 교차오염이 생기지 않도록 해야 한다.[449]

아) 사건의 재구성

분석은 제출된 항목이 제안된 가설을 입증할 수 있거나 입증할 수 없는 정보를 포함하는가의 여부를 판단할 수 있게 설계되어야 한다. 이것은 각각의 명제가 옳은 경우에 발견되어질 것으로 예측되는 바를 설명하는 정보와 예측된 결과의 입증가치에 대한 평가를 포함해야 한다. 이와 같이 조사에서 명제 방법론을 활용할 경우 ENFSI MP2010 문서를 참고해야 한다.

자) 평가와 해석(Evaluation and Interpretation)

원본 애플리케이션과 포렌식 도구가 데이터를 해석하는 방법에 대한 이해는 분석된 결과를 과학적으로 평가하고 해석하는데 있어서 필수적인 것이다.[450] 분석에서 나타난 오류의 잠재적 규모는 수학적으로 산출된 값을 이용하여 명시하거나 또는 발견된 정보와 관련하여 알려진 한계를 상세히 설명하는 문장이나 구절로 명시해야 한다.[451] 해석이 요구되는 경우, 분석관은 고객에 의해 제시된 명제가 어느 범위까지 테스트될 수 있으며, 복구된 데이터가 다른 상황을 이유로 제출될 수 있는가의 여부를 평가해야 한다.[452]

분석과정에 있어서 공식적으로 증명된 기능을 활용할 수 없는 경우 증명되지 않은 기능이 활용될 수도 있는데, 이 경우 분석관은 제출된 결과의 특성을 연구할 충분한 능력이 있어야 하고, 그 결과들이 실험실내에서 채택된 표준 검증방법의 기준에 부합할 수 있어야 한다.[453] 만약 증명되지 않은 기능이 정기적으로 사용되는 경우에는 공식적인 검증을 거쳐 실험실의 승인목록 안에 추가되어져야 할 것이다.

---

448) ENFSI, op.cit., p.33.
449) ENFSI, op.cit., p.34.
450) ENFSI, Best Practice Manual for the Forensic Examination of Digital Technology, ver.01, 2015, p.36
451) ibid.
452) ENFSI,op.cit., p.37.
453) ibid.

이 외에도 파일과 원본 데이터 맵핑 평가방법, 디스크와 파티션 및 볼륨 맵핑을 평가하는 방법, 파일 시스템 맵핑을 평가하는 방법, 포렌식 필터의 결과를 평가하는 방법, 평가와 해석에서 발생하는 오류를 찾아내는 방법 등이 기술되어 있다. 특히 평가와 해석에 있어서 발견된 오류들은 그 편차가 기존의 프로세스를 위태롭게 하지 않고 수용가능한 제약 내에서 존재하도록 동료심사의 일부로서 모니터링 되어야 한다.

아) 증거의 제출

전문가 증언을 제공하는 사람들의 가장 중요한 의무는 법원과 사법의 집행에 대한 것으로 증거는 정직, 진정성, 객관성, 공평성을 가지고 제공되어야 한다.[454] 증거의 제출은 명확하게 모든 평가의 결과 그리고 그 조사에 대한 해석을 명시해야 하며, 수행된 조사에 의해 뒷받침되는 정보만 제출해야 한다.[455] 서면보고서는 동료심사를 거쳐서 제출해야 한다.

전문가 증언은 특별히 법원에 의해 명령되지 않는 한, 그들의 전문영역 밖에서 행해진 질문에 대해서는 대답해서는 안되며, 심지어 자신의 전문지식의 한계에 대한 선언이 행해져야 한다.[456] 보고서에서 가장 중요한 것은 잘못된 해석을 피하기 위해 알려진 한계와 오류들을 분명히 하는 것이며, 데이터의 맥락이 정확하게 이해되고 표현되는 것이다.[457]

법원에서 디지털 조사의 결과물을 활용하는 일반적인 두가지 방법은 기술보고와 평가의견인데, 기술보고는 조사과정에서 정확히 찾아낸 증거와 개인의 숙련도를 토대로 한 분석에 대한 사실에 기반한 보고이며, 평가의견은 증거로 활용하기 위해 제공된 명확하게 조건지워진 정보와 사건의 구체적인 문제에 기반을 둔 증거적 가치에 대한 의견이다. 보고서는 이 두가지 요소 가운데 하나 또는 둘다 포함할 수 있다.[458]

---

454) ENFSI,op.cit., p.40.
455) ENFSI, Best Practice Manual for the Forensic Examination of Digital Technology, ver.01, 2015, p.40.
456) ibid.
457) ibid.
458) ENFSI, op.cit., p.41.

자) 기타

이 매뉴얼은 위에서 열거된 항목 외에도 '14. 건강과 안전'에서는 포렌식 과정에 있어서 발생할 수 있는 작업자의 건강과 안전과 건강에 해로운 물질의 제어(COSHH)에 대한 국가적 요구를 충족시킬 것을 서술하고 있다.[459] 또한 '15. 관련 문헌들'에서는 디지털 포렌식과 관련된 ISO, ENFSI의 관련 문건들을 열거해 놓고 있다. 그와 함께 국제적인 기준과 지침들, 일반적인 포렌식 및 기술관련 자료들, 관련 링크들을 알려주고 있다.[460] '16. 이전 버전에 비해 추가된 부분(Amendments Against Previous Versions)'에서는 버전의 역사에 대해 소개하고 있다.[461]

그 뿐 아니라 부록에서는 실무에서 실재적으로 검토해야 할 내용들을 기술해 놓고 있다. 부록 A에서는 컴퓨터 환경설정, 부록 B에서는 커스텀 개발방법, 부록 C에서는 데이터 매핑방법, 부록 D에서는 필터링 방법, 부록 E에서는 요구목록 작성법, 부록 F에서는 도구들에 대한 최소한의 요구사항, 부록 G에서는 리포트 작성시 요구사항, 부록 H에서는 위험도 평가 샘플 등을 상세히 제공해 주고 있다.[462] 이처럼 모범 실무 매뉴얼에서는 디지털 포렌식을 수행함에 있어 필요한 모든 절차와 과정에서 필요시되는 요건들을 상세하고 최신의 기준과 기술이 적용되도록 설명해 주고 있다. 물론 해당 매뉴얼은 각 국가의 실정에 맞추어서 수정되는 부분이 있지만, 그 자체로도 완결된 매뉴얼 역할을 하게 된다. 특히 유럽차원에서는 매뉴얼에 대한 공신력을 담보해 주고 있기 때문에 단순한 매뉴얼 이상으로 디지털 포렌식의 규범으로서의 역할도 수행한다고 할 것이다.

나. Guidelines on Digital Forensic Procedures for OLAF[463] staff

1) 목적

OLAF는 EU 펀드의 사기나 부패와 관련된 수사업무를 독자적으로 수행하고 있으

459) ENFSI, op.cit., pp.41-42.
460) ENFSI, op.cit., pp.42-43.
461) ENFSI, op.cit., p.44.
462) ENFSI, op.cit., pp.45-65.
463) OLAF는 유럽연합의 재정적 이해관계를 보호하기 위하여 유럽연합으로부터 위임을 받은 유럽위원회의 사기방지사무국이다.

며, EU와 관련된 사기방지정책도 수행하고 있다.[464] 이처럼 OLAF는 EU의 막대한 자금에 대한 EU내의 수사 뿐 아니라 EU 밖에서의 수사, 그리고 사안별로 EU회원국 내에서의 수사에 대한 조화를 위해서 수사업무를 수행하고 있는데, 재정에 관한 흐름은 대부분 사이버공간을 통해서 이루어지고 있다. 그러므로 OLAF에게 디지털 포렌식은 필수이자 매우 중요한 역할을 하기 때문에 그에 대한 직원들을 위한 지침을 마련하고 있다.[465] 물론 수사업무를 수행하고 있는 OLAF의 경우 'OLAF 직원을 위한 수사절차 지침(Guidelines on Investigation Procedures for OLAF Staff)'이 마련되어 있고, 해당 지침의 제15조에 디지털 포렌식에 대한 규정이 되어 있지만 매우 선언적인 내용만을 담고 있으며,[466] 그 중요성으로 인해 디지털 포렌식과 관련된 절차지침을 따로 두고 있는 것이다.

디지털 포렌식 절차에 관한 OLAF 가이드라인은 디지털 증거의 식별·획득·이미징·수집·분석·제출과 관련하여 OLAF 직원들이 따라야 하는 내부규칙으로, 행정절차·징계절차·사법절차에서 허용될 수 있는 증거의 연속성과 무결성을 보장하기 위한 방식으로 디지털 포렌식을 운용하기 위한 규칙을 확립하고자 마련된 것이다.[467]

이 지침서는 2012년에 채택된 '디지털 증거의 식별, 수집, 획득, 보존을 위한 가이드라인"에 관한 ISO 27037, 그리고 2012년 영국의 ACPO 에 의해 출간된 '디지털 증거에 관한 모범실무지침'과 같은 국제적으로 승인된 표준과 모범실무를 고려하여 제정된 것이다.[468]

2) 구성내용

가) 정의(Definitions)

정의 규정(제1조)에서는 EU 직원, 디지털 포렌식, 디지털 증거 전문가, 디지털 포렌식 작업 등 디지털 포렌식과 관련된 용어들을 정의하고 있다.[469] 특히 눈에 띄는

464) http://ec.europa.eu/anti-fraud/about-us/mission_en; 2016.9.30
465) ibid.
466) https://ec.europa.eu/anti-fraud/sites/antifraud/files/docs/body/gip_18092013_en.pdf.; 2016.9.30
467) OLAF, Guidelines on Digital Forensic Procedures for OLAF Staff, 2016, p.1.
468) OLAF, Guidelines on Digital Forensic Procedures for OLAF Staff, 2016, p.1.
469) ibid.

것으로 클라우드 서비스 제공자(제1조 제18항)에 대한 정의규정을 두고 있는 것이다.[470] 이는 이미 해당 디지털 포렌식에서는 최신의 동향인 클라우드 컴퓨팅 환경까지 고려하고 있다는 것을 알 수 있다.

나) 포렌식 실험실(OLAF's Forensic Laboratory)

OLAF의 법과학 연구실(제2조)에 대한 규정을 두고 있다. 여기서는 OLAF 법과학 연구소가 물리적으로 분리되어야 하고, 사무실은 보안이 철저해야 하며, 분석망은 분리되어야 하고, 해당 연구소의 출입이 엄격히 제한되어야 한다는 등의 내용을 담고 있다.[471]

다) 디지털 포렌식 작업의 준비(Prepartaion of a digital forensic operation)

디지털 포렌식 작업의 준비(제3조)에 대한 내용에서는 업무수행자가 디지털 포렌식 작업을 위한 준비 체크리스트를 작성하도록 하고 있으며, 디지털 포렌식 작업 수행을 위한 권한요청서가 필요하며, 사건관리시스템 가운데 해당 업무와 관련된 파일에만 접근하도록 해야 한다는 내용이 규정되어 있다.[472]

라) 디지털 포렌식 작업의 수행 - 일반적 절차

제4조에서는 디지털 포렌식 작업 수행과 관련해서 일반적인 절차들을 규정하고 있다. 확보된 증거가 차후 법적 절차에서 허용될 수 있도록 디지털 포렌식 작업은 반드시 OLAF의 허가받은 분석 전문가에 의해 수행되어야 하며, 수사관과 전문가는 서로 협력 하에 해당업무를 수행하도록 하고 있다. 디지털 포렌식 전문가는 포렌식 작업을 시작할 때 첫째, 포렌식 작업의 대상이 되는 모든 디지털 매체 뿐만 아니라 물리적인 환경과 배치상태를 기록하고 사진을 찍어야 하며, 둘째, 디지털 매체의 목록을 작성해야 한다.

그리고 디지털 포렌식 작업은 정해진 절차에 따라 이루어져야 하며, 수사관이 임의로 어떤 조치를 취하는 것은 금지되어 있다. 그리고 디지털 포렌식 작업에 관여했던 모든 사람의 명단이 작성되어야 하며, 디지털 포렌식 작업을 수행한 전문가의 서명이 보고서안에 포함되어야 한다. 그리고 디지털 포렌식 과정에서 수집된 모든 장치안에

---

470) OLAF, op.cit., p.3.
471) ibid.
472) OLAF,op.cit., pp.3~4.

포함된 정보는 안전한 방식으로 전송되어야 하며, 증거 연계성에 있어서 무결성 보장을 위해 전송과정 중에 항상 OLAF 직원의 물리적 통제하에 있어야 한다.[473]

마) 디지털 포렌식 작업의 수행- 내부 조사

디지털 포렌식 수행에 있어 내부 수사관들에 대한 내용도 규정되어 있다(제5조). 수사관은 EU 직원 또는 구성원이 EC 883/2013 규정 제4조 제7항에 따라 그리고 관련 기관에 의해 채택된 결정에 따라 OLAF과 협력할 의무가 있다는 점을 설명해야 한다. 디지털 포렌식 작업을 수행하기 전에 수사관은 디지털 포렌식 작업의 대상이 되는 개별적인 장치가 기관의 BYOD 프로그램에 등록되어진 것인가의 여부를 판단하기 위해 관련 기관과 접촉해야 하고, 만약 그렇다면 그 개별적 장치들은 기관에 의해 보유된 것과 마찬가지로 취급되어야 한다.[474]

그 건물에서 발견된 장치가 전적으로 개인적인 것이라고 주장되는 경우, 전문가는 그것이 그 기관에 의해 보유된 데이터를 포함하고 있는가의 여부를 검토하기 위해 그 개인 소유의 장치를 미리보기할 수 있도록 허가를 요청해야 한다.[475] 만약 그 건물에서 발견된 장치가 기관에 의해 보유된 정보를 포함하고 있거나 또는 그 기관에 의해 보유된 것인가의 여부를 확인하는 것이 불가능한 경우, 전문가는 그 데이터를 확보해서 그 포렌식 이미지를 봉인된 봉투안에 보관해야 한다. 그리고 OLAF 직원이 그 사람의 참여하에서 그 장치에 대한 미리보기를 하기 위한 회의를 위해 포렌식적으로 획득된 데이터의 소유자를 방문하게 된다.

OLAF는 EU 직원이나 그 구성원이 없는 동안 디지털 포렌식 작업이 수행되는 상황에서는 5.5조에 규정된 절차를 준수해야 하며, 사적인 것으로 표시된 데이터나 폴더, 이메일을 포함하고 있다는 사실이 전문가로 하여금 포렌식 작업을 하는 것을 막지는 못한다. 그리고 디지털 포렌식의 객체가 된 디지털 미디어의 주인에게 디지털 포렌식 작업 보고서의 관련 부분을 제공하도록 하고 있다.[476]

---

473) OLAF, op.cit., pp. 4~5.
474) OLAF, op.cit., p.5.
475) ibid.
476) OLAF, op.cit., pp. 5~6.

바) 디지털 포렌식 작업의 수행 - 외부 조사

제6조는 외부 수사관들에 대한 규정이다. 기본적으로 OLAF는 외부 기관들과 협력작업을 수행할 수 있도록 되어 있으며, 그에 따라서 회원국 및 다른 국가들과의 협력작업이 가능한지 여부를 현장 체크를 통해 확인하고 그에 따라 행동하도록 하고 있다.[477] 이는 기본적으로 OLAF에서 취급하는 정도의 디지털 포렌식 작업이 여러 회원국이나 제3국과 연관되어 있기 때문에 발생하는 필연적인 절차라고 할 것이다.

사) 원격 디지털 장치에 저장된 데이터의 수집

원격지의 디지털 장치로부터 데이터를 수집하는 규정도 두고 있다(제7조). 따라서 분석 전문가는 EC 883/2013 제4조 제2항, EC 2185/96 제5조, EC 8285/96 제5조 등의 규정에 따라 해당 작업을 수행할 수 있다. 특히 해당 규정을 통해 획득된 정보는 그 객관성과 신뢰성 보장을 위해 반드시 분석 전문가 면전에서 행해져야만 한다.[478]

아) 디지털 포렌식 작업과정에서 수집된 데이터에 대한 조사

제8조는 디지털 포렌식 작업 중 수집된 데이터의 검색방법에 관한 규정이다. 디지털 포렌식 작업을 위해 분석 전문가는 두 개의 복제본을 만들고 밀봉하여 보관하여야 하며, 그 중 하나를 OLAF의 내부 서버(법과학 연구소 서버)에 저장하고 디지털 포렌식을 수행한다. 그리고 필요 없게 된 파일들은 철저하게 삭제하도록 하고 있으며, 수사관은 OLAF의 법과학 연구소의 서버에 올려진 복제파일을 통해 검색을 수행하도록 하고 있다.[479]

자) 특별한 주의를 요하는 데이터 확보

제9조는 특별한 주의가 필요한 정보의 획득에 대한 규정이다. EC 45/2001 제10조 제1항에 따른 개인정보와 관련된 데이터를 수집하는 경우에는 EC 45/2001 제10조 제2항 규정에 따라 수행할 수 있으며, 배우자나 아이들과 관련된 데이터는 사건과 관련된 한에서만 검색할 수 있고, 트래픽 데이터 등은 특별한 기한을 정해서만 가능하게 되며, 해당 트래픽 정보에서 특정인을 식별할 수 있는 정보는 제외된다.[480]

---

477) OLAF, op.cit., p.6.
478) OLAF, op.cit., p.7.
479) ibid.
480) OLAF, op.cit.,p.8.

차) 다른 조사의 맥락에서 획득된 디지털 포렌식 이미지의 재사용

다른 수사와 연관된 디지털 포렌식 이미지의 재사용에 대한 규정도 두고 있다(제10조). 다른 수사와 관련해서 디지털 포렌식 이미지를 재사용하기 위해서 수사관은 해당 사건과 이미지의 관련성에 대한 면밀한 판단을 해야 하고, OLAF는 디지털 포렌식을 당하게 되는 개인이나 경제주체에게 다시금 그 사실을 알려야하며, 본래 디지털 포렌식을 요구한 기관에게도 새로운 수사가 시작되었음을 알려야 하고, 그것은 EC 883/2013 제9조 제3항 및 EC 45/2001 제20조를 충족시켜야 한다.[481]

카) 결과에 대한 최종적인 백업

디지털 포렌식에 대한 더 이상의 요구가 없는 경우 디지털 포렌식은 종결되고 디지털 포렌식 증거와 작업 파일에 대한 복제를 두 개 만들고는 밀봉하여 보관한다(제11조). 그리고 분석 전문가는 그 중 하나의 복제본을 OLAF 포렌식 보관소에 전달하여 보관토록 하고, 두 개의 복제본을 제외한 모든 파일들은 서버에서 삭제하여야 한다.[482]

타) 기타

제12조는 EU 뿐 아니라 EU내의 각 기관 및 회원국들, 제3국의 사법기관, 국제기구 등은 OLAF에 협조를 요청할 수 있으며, OLAF는 절차에 따라 디지털 포렌식을 수행하고 디지털 포렌식 작업 리포트와 분석 리포트를 제공해 줄 수 있으며, OLAF는 해당 데이터를 일정한 기한동안 보관 및 활용할 수 있다고 규정하고 있다.[483] 그리고 제13조는 법원 절차를 위해 디지털 포렌식 증거 파일을 사용하기 위해서는 CMS Intelligence Request Module을 통해서 요청하도록 하고 있으며, 전송은 반드시 암호화 하도록 하고 있다.[484] 제14조는 디지털 포렌식 증거와 워크 파일을 보유할 수 있는 기간은 다른 경우와 같은 원칙에 따라 결정됨을, 그리고 제15조는 해당 지침의 효과는 2014년 1월 1일 지침을 대체해서 2016년 2월 15일 부터로 정하고 있다.[485]

---

481) OLAF, op.cit.,p. 9.
482) OLAF, op.cit.,pp. 9~10.
483) OLAF, op.cit.,pp. 10~11.
484) OLAF, op.cit.,p. 11.
485) ibid.

다. Electronic evidence - a basic guide for First Responders

1) 목적

ENISA는 유럽에서 사이버 시큐리티를 담당하고 있는 기관으로 유럽에 대한 다양한 권고와 정책지원 및 구현, 관련 문제에 대한 직접적인 대응을 수행하고 있다.[486] 이러한 ENISA의 지침은 증거수집에 특별히 중점을 두면서 초동수사를 담당하는 사람들에 대한 지침을 제공하는데 목적을 두고 있다. 즉 법 집행의 관점에서 쓰여진 대부분의 경우와 마찬가지로 디지털 포렌식과 디지털 증거수집이라는 주제에 관한 기존의 방대한 자료들을 보완하는데 목적을 두고 있는 것이다.

이 지침서는 초기 대응자에게 증거에 접근하는 방법에 관하여 전체적인 단계별 지침을 제공하는 것이 목적이 아니라 유효한 증거수집원칙을 설명하고, 증거수집에 참여하기 전에 초기 대응자들이 적절한 질문을 할 수 있도록 하는데 있다고 설명하고 있다.[487]

2) 구성내용

ENISA의 지침은 크게 도입부(Introduction), 전자증거 수집(Electronic evidence gathering), 전자증거 수집원칙(Principles of eletronic evidence gathering), 범죄현장 도착 이전 작업(Before arriving at the crime scene), 현장도착 후 작업(Arriving at the scene), 압수(Seizure), 메모리 포렌식(Memory forensics), 증거 검토(Evidence examination), 증거평가 및 제출(Evaluating and presenting the evidence), 맺음말(Final remarks)로 되어 있다.

가) 개요

도입부에서는 범주와 목적, 배경, 그리고 대상 등에 대한 내용을 담고 있다. 본 지침의 범주에는 특별한 임무를 수행하는 CERTs(Computer Emergency Response Teams) 뿐 아니라 커뮤니티나 국가, 정부의 CERTs, 법집행 기관 및 국제 연구소 및 기관 등이 속한다.[488] 지침의 목적은 초동수사에 있어서 디지털 증거를 올바르게

---

486) https://www.enisa.europa.eu/about-enisa; 2016.9.30.
487) ENISA, Electronic evidence - a basic guide for First Responders, 2014, p.1.
488) ENISA, op.cit., p.2.

수집하도록 하기 위해 증거수집 원칙을 설명해 주기 위한 것이다.[489] 특히 CERTs는 컴퓨터 보안사고와 관련된 조사업무를 수행하고 있는데, 사실상 초동수사의 직무를 수행하게 된다. 그러므로 CERTs 업무 수행자가 초동수사를 하는 단계에서 어떤 절차를 거치고, 어떤 부분에 중점을 두어야 하는지를 목적으로 하고 있다.[490] 다만, 본 지침은 CERTs에게 구체적으로 규정을 정해서 지키도록 하는 것이 아니라 안내서의 역할을 수행하고 있다고 할 것이다.

나) 전자증거 수집

전자 증거의 수집에 있어서는 전자증거와 전자증거의 수집이 어떤 것인지, 증거의 저장매체의 다양성 등을 고려하도록 하고 있다. 그에 따르면 전자증거는 "법원에서 신뢰할 수 있는 이진수 형태로 저장 또는 전송되는 정보"를 의미하며, 전자증거 수집은 수사과정에서 증거적 가치가 있다고 판단되는 범죄와 관련된 데이터를 인식하고, 복구하며, 주어진 상황을 평가하는 것과 관련된 절차를 의미한다.[491] 전자증거의 저장매체는 개인컴퓨터나 랩톱, 서버 등 컴퓨터, 컴팩트 디스크, USB, 메모리 카드 등 저장장치, 스마트폰이나 디지털 카메라와 같은 모바일장치, 허브나 스위치, 라우터 등과 같은 네트워크 장치 등이 있기 때문에 그에 맞는 방법이 필요하다고 한다.[492] 이는 CERTs에게 전자증거 수집을 위한 초동수사에 대한 기본 개념을 알려주고 있는 것으로 보인다.

다) 전자증거 수집의 원칙

전자증거 수집의 원칙으로는, 제1원칙으로 데이터 무결성(Data Integrity), 제2원칙으로 감사추적(Audit Trail),[493] 제3원칙으로 전문가 지원(Specialist Support), 제4원칙으로 적합한 훈련(Appropriate Training), 그리고 제5원칙으로 적법성(Legality)를 제시하고 있다.[494] 이와 같은 원칙들을 제시하는 이유는 CERTs의 경우 초동단계에서

489) ibid.
490) ENISA, op.cit., p.3.
491) ENISA, op.cit., p.4.
492) ibid.
493) 감사추적이란 "감사를 위해 입력된 데이터가 어떤 변환 과정을 거쳐 출력되는지의 과정을 기록하여 추적하는 방법"을 의미한다. 하드웨어의 고장이나 입축력 오류 등을 추적하고, 비인가된 접근이나 사용 등을 알 수 있다(http://terms.naver.com/entry.nhn?docId=842713&cid=42346&categoryId=42346〈2016.9.30 최종방문〉).
494) ENISA, op.cit.,p.5.

그와 같은 원칙을 생각하지 않고 업무를 수행할 수 있기 때문인데, 그와 같은 경우 수집된 증거가 법정에서는 증거로 사용될 수 없기 때문이다. 그러므로 지침에서는 ISO 27037이나 OLAF 직원을 위한 디지털 포렌식 가이드라인, 디지털 기술의 법과학적 검토에 있어 모범 사례를 위한 지침 등에서 관련 내용을 볼 수 있다는 것과 함께 무결성이나 감사추적, 전문가 지원, 적합한 훈련, 적법성 등에 대한 설명을 해 주고 있다.[495]

라) 범죄현장 도착 이전

범죄현장 도착 이전 작업에서는 초동수사를 위해 어떤 준비들이 필요하지를 설명해 주고 있다. 초동 수사에서 먼저 툴킷(Toolkit)을 잘 준비해야 한다. 툴킷에는 현장 촬영을 위한 카메라, 시간을 기록할 수 있는 디지털 시계, 증거를 가져가기 위한 상자 또는 가방, 기록을 위한 필기구, 절차를 적어놓은 플로어 차트, 장갑, 증거의 무결성을 위한 증거목록 로그/증거 테입/스티커/라벨/테그 등, 정전기 방지 가방과 장비 및 비자성(non-magnetic) 툴킷, 고려해야할 법적 문제점을 기록한 체크 리스트 및 적절한 법적 조언이 기록된 리스트 등이 포함된다.[496] 그와 함께 포렌식을 위한 랩톱, 쓰기 방지 장치, 메모리 덤프를 위한 장치, 필요한 케이블, 그리고 아무것도 저장되지 않은 저장매체가 필요하다.[497] 특히 초동수사에서 사용되는 랩톱은 CPU가 인텔i7이나 i9 또는 그와 동급인 AMD 제품, 램은 8기가 이상, 메인보드는 USB포트 및 파이어월 포트 장착 필요, 하드디스크는 높은 용량, 그리고 스페어 디스크를 준비하도록 하고 있으며, 운영체제인 윈도우나 리눅스에서 사용할 수 있는 각종 명령어들을 제시해 주고 있다.[498] 이는 전자증서 수집에 있어 해당 컴퓨터 등의 운영체제의 다른 프로그램을 사용하지 않고 운영체제 자체에서 사용되는 명령어들을 통해서 검색과 수집이 가능하도록 하기 위해서이다.

마) 범죄현장에의 도착

여기서는 범죄현장에 도착한 이후의 작업에 대해 설명하고 있다. 알려지지 않은

495) ENISA, op.cit.,pp.6~8.
496) ENISA, op.cit.,pp.9~10.
497) ENISA, op.cit., p.10.
498) ENISA, op.cit.,pp.11~13.

곳에는 가급적 혼자 가서는 안되며, 현장에 도착해서는 자신의 안전을 확보하고, 주변 환경이나 주요 증거 영역, 범죄 연루자 등을 파악하고, 범죄 연루자가 디지털 장치가 있는 장소에 영향을 주지 못하도록 해야 한다.[499] 현장에서는 영국의 ACPO 컴퓨터 기반 전자 증거를 위한 모범 지침이나 OLAF 직원을 위한 디지털 포렌식 절차 지침과 같은 지침에 따라 행동하는 것도 필요하다.[500] 무엇보다 카메라나 동영상을 통해 디지털 장치를 촬영할 필요가 있는데, 거기에는 범죄현장에 들어간 일시·디지털 장비와 주변기기가 표시된 현장의 평면도, 현장에 있는 직원들, 들어갈 때의 현장사진, 모든 디지털 표현물의 원위치에서의 사진 등을 촬영해 놓아야 하고, 모든 디지털 증거는 개인적 접근을 차단하고, 보안이 유지되도록 하여야 한다.[501]

바) 압수

디지털 증거는 피의자의 장소에서 수집되기 때문에 장시간이 걸리는 데이터를 분석하기 위해서는 압수가 필요하게 된다. 그럴 경우 이미징을 통해 분석장소로 가져가는데, 그 때 고려해야 할 요소로서 컴퓨터가 동작하고 있는지, 컴퓨터가 네트워크에 연결되어 있는지, 메모리의 휘발성 데이터를 보존해야 하는지, 전체디스크가 암호화되어 있는지, 콘솔이 잠겨져 있는지 등 이다.[502]

사) 메모리 포렌식

컴퓨터의 경우 일반적으로 메모리에 있는 데이터들은 전원이 연결되어 있는 경우에만 획득이 가능하다. 그리고 하드디스크나 USB에 저장되지 않은 메모리에 올려져 있는 휘발성 정보들은 전원이 차단된 이후에는 복구가 불가능 하다. 그러므로 초동수사에 있어 메모리에 있는 정보를 획득하는 것은 매우 중요하다. 그러므로 메모리에 있는 정보의 내용들이 변경되지 않도록 획득하되, 경우에 따라서 해당 컴퓨터로 작업하는 것이 용이하지 않을 경우 네트워크를 통한 작업으로 획득하기도 한다.[503] 메모리에 있는 정보들은 USB와 같은 외부저장매체에 저장하여야 한다.

---

499) ENISA, op.cit.,pp.14.
500) ibid
501) ibid
502) ENISA, op.cit., p.15.
503) ENISA, op.cit., p.16.

아) 증거조사

조사 절차 그 자체는 원시 데이터의 해석과 사건의 재구성을 의미하는 것이다. 이러한 증거의 검토 작업은 원본이 아닌 복제본을 통해 이루어져야 한다. 그리고 수집된 정보 가운데 증거를 추출함에 있어서는 해시값 설정, 키워드 검색, 파일의 확장자 검색, 레지스트리 등 정해진 저장장소의 데이터 검색, 헤더와 풋터 사이의 데이터 검색, 압축파일 검색, 숨겨진 파일 검색 등을 통해 증거를 확보해야 한다.[504] 또한 인터넷 브라우저나 인터넷 캐쉬 또는 임시파일, 쿠기 파일, 타임라인 분석 등을 통해서도 증거를 수집할 수 있다.[505]

자) 증거의 평가와 제출

디지털 증거에 대한 평가보고서는 관련 전문가들을 상대로 하는 것이 아니고, 일반인들과 법원을 상대로 작성되어진다. 그러므로 보고서는 해당증거에 대한 진정성, 신뢰성, 증거능력이 인정될 수 있도록 기술되어야 한다.[506] 각 단계와 참조된 프로토콜·사용된 방법, 주요 증거의 압수·기록·수집·보관·복구·재구성·조직 및 수색 등과 관련 된 내용들이 포함되어 있어야 하고, 해당 절차가 모범 절차에 따라 수행되었는지도 검토하도록 하고 있다. 다른 디지털 포렌식 리포트 지침에도 부합하는지를 살펴보아야 한다.[507]

본 지침의 서두에서도 밝히고 있지만, 해당 지침은 CERTs의 초동수사 담당자에게 구체적이고 규범적인 지침을 제공해 주는 것은 아니다. 초동수사를 통해 전자증거를 처리하면서 해당 증거가 법적으로 가지게 되는 의미나 가치, 절차 등에 대한 내용을 대략적으로 나마 이해할 수 있도록 정보를 제공해 주공 있는 것이다. 그러므로 해당 지침에서는 다른 지침의 내용들을 함께 살펴볼 것을 권하기도 한다. 따라서 CERTs의 초동수사 담당자는 해당 지침을 살펴보고, 좀 더 구체적이고 규범적인 부분에 있어서는 우리가 앞서 살펴본 OLAF 직원을 위한 디지털 포렌식 지침 등을 살펴볼 필요가 있게 된다.

---

504) ENISA, op.cit., pp.17~18.
505) ENISA, op.cit., p.18.
506) ENISA, op.cit., p.19.
507) ibid.

제4절 독일의 디지털 포렌식 시스템

1. 독일의 디지털 포렌식 모델 구축 현황 분석

앞서 살펴본 바와 같이 유럽은 ENFSI를 중심으로 각 국가의 포렌식 관련 연구소가 연결되어 있다. 독일의 경우 유럽연합의 다른 국가들 보다도 월등하게 많은 9개의 기관이 ENFSI의 회원으로 참여하고 있다. 물론 그 기관들 가운데 가장 중요한 것은 독일 연방형사청(Bundeskriminalamt)에 설치되어 있는 법과학 연구소(Foresic Science Institute)일 것이다. 하지만 그 외에도 뮌헨의 Bavarian State Bureau of Investigation Forensic Science Institute, 비스바덴의 Forensic Science Institute, 함부르크의 Landeskriminalamt Hamburg LKA 3(Department of forensic science), 킬의 LKA Schleswig-Holstein(Forensic Science Institute), 수투트가르트의 State Criminal Police Office Baden-Wurttemberg(Forensic Science Institute), 베를린의 State Criminal Police Office Berlin(Forensic Science Institute), 하노버의 Forensic Science Institute, 뒤셀도르프의 State Criminal Police Office Northrhine-Westfalia(Department of Forensic Science) 등이 회원으로 참여하고 있다. 그러므로 아래에서는 독일 연방형사청을 중심으로 ENFSI의 회원으로 속해있는 기관들 가운데 주요 기관을 대상으로 독일의 디지털 포렌식 현황을 살펴보고자 한다.

가. 연방형사청의 범죄과학 연구소

독일에서 디지털 포렌식과 관련된 가장 대표적인 조직으로는 독일 연방형사청(BKA)에 소속되어 있는 '범죄과학연구소(Kriminaltechnisches Institut)'가 있다.[508] 우리나라의 경우에는 검찰청에 디지털 포렌식 센터를 두고 있고, 경찰에도 디지털 포렌식 센터를 두고 있으며, 국립과학수사연구원에 디지털 포렌식 관련 조직을 두고 있어 각각의 조직이 자체적으로 디지털 포렌식 업무를 수행하고 있는 것에 반하여 독일 연방형사청의 범죄과학연구소는 경찰조직을 포함해서 검찰과 법원에 대해서도 디지털 포렌식 서비스를 제공하고 있으며, 앞서 살펴본 바와 같이 ENFSI의 회원으로

508) https://www.bka.de/DE/DasBKA/OrganisationAufbau/Fachabteilungen/KriminaltechnischesInstitut/kriminaltechnischesinstitut_node.html:2016.9.30.

도 참여하여 유럽차원에서의 디지털 포렌식 기술 향상을 위해 많은 기여를 하고 있다.[509]

독일의 범죄과학연구소는 형사사건을 규명하고, 과학적인 방법으로 증거를 확보해야 한다는 필요성에 따라 설치되었다. 그를 위해 다양한 연구방법과 최신 과학 장비를 사용하고 있으며, 그들을 통해 발견된 증거들이 증거물로서 법원에 제출될 수 있도록 최대한 객관성을 담보하여 생성하도록 하고, 그를 보고서로 작성하여 법원에 제출될 수 있도록 지원해 주는 역할을 수행하고 있다.[510] 따라서 범죄과학 연구소는 연방형사청에 소속되어있으며, 경찰뿐 아니라 검찰이나 법원의 요청에 따라 형사절차에서 사용될 수 있는 과학적 방법을 통해 만들어진 감정서 등을 제공하고 있다.[511] 이런 측면을 보면 범죄과학 연구소는 우리나라의 국과수와 같은 지위를 가지고 있지만, 연방형사청에 속해 있는 것과 유사하다고 할 것이다.

범죄과학 연구소의 주요 업무들은 범죄현장지원이나 범죄증거분석회의, 수집된 증거의 전산화 등 여러 가지이지만,[512] 그 가운데 하나는 법과학적인 방법을 통하여 증거가치를 향상시키고, 새로운 디지털범죄에 대응하여 혁신적인 대응을 할 수 있는 방법을 마련하는 것이다. 따라서 아래에서 설명하겠지만, 기존의 조직에서 나누어져 있던 업무들을 모아서 디지털 포렌식과 관련된 새로운 전문그룹을 만들었다. 무엇보다 독일에서는 연방형사청이 디지털 포렌식과 관련해서 허브의 역할을 수행하고 있는 것과 함께 조정자의 역할을 수행하고 있는 것으로 보이는데, 이는 범죄과학 연구소의 소속과 지위를 통해서 잘 나타나고 있는데, 우선 각 주의 경찰들과 긴밀한 협조를 하는 것 뿐 아니라 해외의 디지털 포렌식 관련 연구소들과도 긴밀한 네트워크를 형성하고 있기 때문이다.[513] 이는 앞서 살펴본 ENFSI에서도 잘 나타나고 있는데, 범죄과학 연구소의 경우 ENFSI의 회원으로 참여하면서 지속적으로 유럽의 여러 관련 기관들과 협력을 하고 있다.

---

509) 이원상/탁희성/송봉규, 디지털 포렌식 역량강화방안, 2012년 경찰청수탁과제, 2012, 59면.
510) https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Kriminaltechnik/kriminaltechnik_node.html:2016.9.30.
511) ibid.
512) https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Kriminaltechnik/Kernkompetenzen/kernkompetenzen_node.html:2016.9.30.
513) 이원상/탁희성/송봉규, 앞의 글, 59면.

범죄과학 연구소는 앞서 언급한 바와 같이 증거물 수집 및 전문가·정보시스템을 문서화 작업을 하는 것에 도움을 주는 것이다. 그런데 가장 중요한 기능으로는 수집한 증거를 바탕으로 정보시스템을 구축해 주는 것이다. 예를 들어, 범죄에 사용된 탄환을 수집하거나, 문서정보화시스템(Informaionssystemen Urkunden(ISU)),[514]을 통해 디지털 포렌식이 원활 할 수 있도록 해주고, 유럽자동차라커 데이터뱅크(Autolackdatenbank) 등과 관련된 정보들을 제공해 줌으로서 수사관들의 업무를 지원해 주는 것이다. 특히 정보시스템 문서는 형사절차의 여러 단계에 있어 연방형사청 뿐 아니라 다른 관련 기관들에게 도움을 주고, 받으며 협력을 하기 때문에 다른 기관들과도 연관을 맺게 된다.

문서정보화시스템을 통해 형사소송과 관련된 여러 기관들이 소송절차와 관련된 다양한 문서들을 데이터베이스화 하여 저장 및 사용하게 되고, 그를 활용하여 예를 들어 진정 문서와 위조·변조 문서를 비교하여 식별하는 것과 같은 업무들도 쉽게 수행할 수 있게 된다. 또한 유럽자동차라커 데이터베이스를 사용하게 되면 범죄장소에서 발견된 페인트를 통하여 범죄와 관련된 차량의 종류와 생산연도 등을 손쉽게 알 수 있다. 이와 같은 시스템은 유럽차원에서만 국한되는 것이 아니라 미국이나 캐나다, 일본 등 해외의 법과학 연구소와도 협력되어 운영되고 있다. 또한 최근 유럽에서도 총기와 관련된 사건들이 많이 발생하고 있는데, 범죄과학 연구소는 5000종이 넘는 탄피와 탄환을 보유하고 있기 때문에 그를 통하여 범행에 사용된 무기가 어떤 것이었는지도 용이하게 식별할 수 있다. 이전까지 범죄과학 연구소는 총 20가지의 전문영역(무기, 탄환, 위조·변조문서, 혈액 및 타액과 같은 체액, 마약, 폭발물 등)에서 매년 10,000건 이상의 사건을 다루어 보고서를 제출하고 있었꼬, 60여개의 전공과목

514) 문서정보화시스템(ISU)은 "정보화에 의해서 생성, 결합 그리고 유포되는 일련의 문서를 총칭한다. 문서정보화시스템의 주요부분은 연방형사청에 의해 관리되는 데이터뱅크인데, 거기에는 위조, 변조 문서(예를 들어 여권, 면허증 등)들이 저장되어 있다. 문서정보화시스템으로 인해 관련 사안에 대해 빠른 대응이 가능해졌고, 관련 범죄의 대조 등을 통해 범죄에 대해 효과적으로 대응할 수 있는 기반이 마련되었다. 특히 문서에 있어서 최근 기술을 발달로 인해 원본문서를 보호하기 위한 보호장치가 마련되는 것에 비례해서 위조·변조 기술도 함께 진화하고 있다. 이로 인해 위조·변조된 문서를 확인해야 하는 여러 기관들에 있어서는 이를 대조할 수 있는 시스템에 대한 요청이 점차 증가하고 있다. 그러므로 위조·변조된 문서에 대한 정보를 각 기관들에 제공해주는 것은 매우 중요한 일이 되었다(http://www.bva.bund.de/DE/Organisation/Abteilungen/Abteilung_S/ISU/ISU.html〈2016.9.30 방문)"; 이원상/탁희성/송봉규, 앞의 글, 각주 70 참조.

의 325명의 전문가들이 업무를 수행하고 있었다.[515]

그런데 최근 독일 법과학연구소의 최근 조직도를 보면 이전이 조직과 상당부분 바뀐 것을 볼 수 있다. 이전의 조직이 아날로그 증거에 중점을 맞추고, 이제까지 범죄에서 중요시 되었던 증거들을 중심으로 조직되어 있었다면, 새로운 조직에서는 디지털 포렌식을 강조하고 있는 것이 눈에 띈다. 과거의 조직에서는 전문그룹이 물리/화학, 총기류/재료기술, 생물학, 문서/미디어 기술, 필체/언어/음성정보기술로 구분되어 있었다. 이처럼 과거 조직에서는 디지털 포렌식을 중점으로 하는 전문조직이 없었지만 새로운 조직에서는 '전문그룹 5'를 디지털 포렌식 전문 조직으로 운영하고 있는 것을 알 수 있다. 이는 디지털 포렌식의 필요성과 중요도가 높아짐에 따라 전문그룹도 그에 맞추어 새롭게 구성한 것이다.

나. 기술개발·서비스 및 혁신 기술센터(TESIT)

연방형사청의 조직가운데 법과학과 관련해서 눈에 띄는 조직이 있다. 바로 기술개발·서비스 및 혁신 기술센터(Technisches Entwichluns- und Servicezentrum, Innovative Technologien(TESIT))이라고 할 수 있다. 범죄과학연구소가 연방형사청 내에 소속되어 우리나라의 국립과학수사연구원과 같은 역할을 하고 있는 것에 비해 TESIT은 범죄과학연구소 내에서 기술개발 등과 관련된 업무를 수행하고 있다. 이는 범죄과학 연구소의 업무 가운데는 형사정책 및 범죄학적인 연구, 기술개발 및 서비스, 혁신 기술, 훈련 및 심화교육 등도 포함되는데, 그 가운데 TESIT은 범죄수사 등과 관련된 기술에 대한 분석 뿐 아니라 다양한 가치판단 등도 수행하고 있다.

그와 같은 업무가 가능한 이유는 TESIT의 구성원들이 단순히 한 분야의 전문가로만 되어 있는 것이 아니라 학자, 기술자, 엔지니어, 기술능력을 지는 경찰관 등 범죄와 관련된 다양한 분야의 전문가들로 구성되어 있기 때문이다.[516] TESIT의 기능은 여러 가지가 있지만 디지털 포렌식과 관련해서는 크게 세 가지의 기능이 눈에 띈다. 우선 TESIT는 빠르고 복잡하게 변화되는 기술에 대해서 선제적으로 분석하고 그 영향에

515) 이원상/탁희성/송봉규, 앞의 글, 60면.
516) https://www.bka.de/SharedDocs/Downloads/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/ki2Flyer.html〈2016.9.30. 최종방문〉.

대해 판단한다.[517] 그리고 새로운 기술에 대해서 지속적으로 분석하고, 지속적으로 기능을 검토해 가면서 실무에 적용할 수 있는지 여부를 판가름한다.[518] 또한 마지막으로 새로운 기술을 어떻게 수사절차에 적용시킬 수 있을 지에 대해 고민을 하고, 기술을 적용시킬 수 있도록 하고 있다.[519] 이와 같은 것이 가능한 이유는 TESIT가 간학문적인 인적구성과 함께 특정된 임무를 지속적으로 수행할 수 있는 환경이 조성되어 있기 때문이다. 특히 디지털 포렌식과 같이 하루밤을 자고 일어나면 새로운 기술이 개발되고, 상용화 되고 있는 현대의 상황에서 수사기관도 지속적으로 신기술에 대한 유입과 적용을 게을리 할 수 없기 때문에 이와 같은 조직은 상당히 의미있다고 생각된다.

다. 니더작센주의 포렌식 과학 연구소

1) 범죄기술연구소 개요

독일은 연방국가이기 때문에 기본적으로 경찰업무에 대해서는 각 주의 경찰이 해당 주와 관련된 업무를 수행하는 구조이다. 그러므로 경찰업무에 속하는 디지털 포렌식의 경우에도 각 주의 경찰 또는 연구소들은 자체적인 체계를 가지고 있다고 하겠다. 이는 앞서 살펴본 ENFSI의 회원에서도 살펴볼 수 있다. 뮌헨이나 비스바덴, 함부르크, 킬, 스튜투가르트, 베를린, 하노버, 뒤셀도르프 등에서는 ENFSI의 회원으로 활동하고 있는 법과학 기관들이 있다.[520] 그런데 그에 속하지 않은 법과학 기관들도 존재하고 있다. 그러므로 ENFSI에 속해있지 않은 기관의 경우에는 어떤 체계를 가지고 있는지를 살펴볼 필요가 있다. 따라서 ENFSI에 속하지 않은 기관 가운데 니더작센주 주경찰청의 범죄기술연구소(Kriminaltechnisches Institut)의 체계를 한 번 살펴보고자 한다.[521] 범죄기술연구소는 대학이나 전문대학 등에서 자연과학을 전공한 전공자들뿐 아니라 기술자 및 범죄전문가 등으로 니더작센 주경찰청에 설치되어 있는 법과학 기관이다.[522] 현재 약 200명의 인원이 연간 250,000건의 증거관련 자료 분석과 함께

517) ibid.
518) ibid.
519) ibid.
520) http://www.enfsi.eu/about-enfsi/members〈2016.9.30. 최종방문〉.
521) http://www.lka.polizei-nds.de/kriminalitaet/kriminaltechnik/-856.html 〈2016.9.30. 최종방문〉.
522) http://www.lka.polizei-nds.de/download/71669/Allgemeine_Info.pdf.

45,000건의 조사보고서를 작성하며 일선 경찰업무를 지원해주고 있다.[523]

2) 정보통신기술 관련 포렌식

그 가운데 특히 주목할 만한 것으로 정보통신기술 관련 포렌식(Forensische Informations- und Kommunikationstechnik(IuK))과 관련된 법과학 업무이다. 무엇보다 범죄기술연구소는 2008년 11월 21일 ISO/IEC 17025 인증을 획득하였으며, 이후로도 계속해서 디지털 포렌식 절차들에 대한 표준화작업을 수행하고 있고, 또한 정기적으로 독립된 업체에게 검토를 받고 있다.[524] IuK의 업무내용을 보면 지속적으로 발전하고 있으며 그 종류도 매우 다양한 하드웨어 및 소프트웨어로 인해 그 업무 영역도 지속적으로 변하고 있으며, 특히 기술의 따른 경찰들의 압수·수색업무를 지원해 주는데 많은 노력을 기울이고 있다. 이는 일선 경찰들의 경우 날로 발전하는 디지털 저장매체와 소프트웨어에 대해 적절하게 대응하며 압수·수색을 수행할 수 없기 때문에 범죄기술연구소가 그것을 지원해 주면서 일선 경찰들의 어려움을 해소해 주고 있는 것이다. 무엇보다 아동포르노라든지 인종차별, 경제범죄 등과 관련된 범죄들이 사이버공간에서 발생하는 경우 해당 정보들이 저장된 위치를 확인하고, 해당 정보가 관련 법률을 저촉하였는지를 판단해 주는 것은 일선 경찰들에게 큰 도움이 된다.[525]

하지만 지속적인 하드웨어 및 소프트웨어 기술발전과 함께 모바일 환경의 변화에도 적응하기 위한 노력을 기울이고 있다. 특히 근래에는 데이터보안(Datensicherung)으로 인해 원본을 기술적인 문제없이 복제하는 것에 많은 어려움을 겪고 있으며, 암호화 기술로 인해서 데이터를 획득한다고 하더라도 분석하는 것이 쉽지 않은 상황이다. 특히 최근 독일에서는 카드소지자 몰래 카드 속의 정보를 복사해 가는 스키밍(Skimming)[526]이 문제가 되고 있어서 그 해결을 위해 다양한 방법을 찾고 있다.

3) 법과학 품질개선 노력

범죄기술연구소에서는 지속적으로 연구소의 법과학 품질개선을 위한 노력을 기울

523) ibid.
524) http://www.lka.polizei-nds.de/download/71674/Forensische_Informations-_und_Kommunikationstechnik.pdf.
525) ibid.
526) ibid.

이고 있다. 특히 범죄기술연구소는 ISO/IEC 17025:2005[527]의 인증을 획득함으로 인해서 국제적인 규격에 적합한 연구소의 운영을 하고 있다.[528] 범죄기술연구소는 품질향상을 위한 학문적 및 기술적 계획과 시행, 검토, 개선의 과정을 지속적으로 유지하면서 신뢰성 향상을 위해 노력하고 있다. 이는 기본적으로 연구소의 신뢰성 향상이 국제적인 차원이나 다른 기관과의 증거관련 업무관계에 있어서 가장 기본적이면서도 매우 중요한 역할을 수행한다는 인식 때문이라고 할 것이다. 특히 범죄기술연구소는 학제간 소통의 중요성과 내부 인력의 내적 및 외적 교육의 중요성을 인식하고, 내부 인력의 경쟁력이 향상될 수 있도록 노력하고 있으며, 정기적인 감사나 매년 경영평가를 통해 객관적으로도 품질개선이 보장될 수 있도록 하고 있다.[529]

4) 니더작센주 범죄기술연구소의 시사점

니더작센주의 범죄기술연구소의 경우에도 한 주의 한 경찰청 내에 속해있는 기관이지만, 해당 연구소의 경영방식이나 법과학 절차는 국제규격에 적합하도록 노력하고 있으며, 해당 절차의 신뢰성 확보를 통해 결과물을 다른 국가나 기관들과 교환하는 것에 있어 아무런 문제가 없도록 노력하고 있다. 디지털 포렌식과 관련된 기술변화 및 모바일 환경에 따른 사용환경의 변화, 암호화 등의 고도화를 통한 분석의 어려움 등 다양한 문제점들은 모든 법과학 기관에게 동일한 도전과제이다. 그럼에도 불구하고 중요한 것은 국제적으로 해당 문제에 대해 어떤 대비책을 마련하고 있으며, 어떤 노력을 하고 있는지에 대해 지속적으로 모니터링을 하며, 자신의 기관에 적용시키려고 노력하는 것과 내부적인 역량을 결집시키고 고도화 할 수 있도록 내부 프로세스를

527) ISO/IEC 17025는 크게 경영요구사항과 기술요구사항들을 충족하도록 다음과 같이 구성되어 있다; 강지현/김민지/김성규/Jane Goodman-Delahunty/Paula Saunders/Mandeep Dhami/Yvette Tinsley, 법과학을 적용한 형사사법의 선진화 방안(II), 한국형사정책연구원 연구총서, 2011, 226면.

경영요구사항	기술요구사항
4.1 조직; 4.2 경영시스템; 4.3 문서 관리 4.4 의뢰, 입찰 및 계약의 검토 4.5 시험 및 교정의 위탁; 4.6 서비스 및 물품 구매 4.7 고객에 대한 서비스; 4.8 불만사항 4.9 부적합 시험 및 교정작업의 관리 4.10 개선; 4.11 시정 조치; 4.12 예방 조치 4.13 기록의 관리; 4.14 내부 심사; 4.15 경영 검토	5.1 일반 사항; 5.2 직원 5.3 시설 및 환경 조건 5.4 시험 및/또는 교정방법과 방법의 유효성 확인 5.5 장비; 5.6 측정 소급성; 5.7 샘플링 5.8 시험 및/또는 교정 품목의 취급 5.9 시험 및/또는 교정 결과의 품질보증 5.10 결과보고

528) http://www.lka.polizei-nds.de/download/71730/Qualitaetsmanagement.pdf.

529) ibid.

객관화 하려는 노력에 대해 주목해 볼 만 하다.

특히 해당 기관은 ENFSI에 속하지 않음에도 불구하고 ENFSI에 속한 기관들과 별다른 차이점이 보이고 있지 않다. 이는 비록 유럽에서 허브역할을 수행하는 ENFSI의 회원으로 참여하고 있지만, 기본적인 운영체계는 회원기관과 거의 유사하므로 유럽의 경우 기관들과의 증거공유에서 신뢰성은 계속해서 유지될 수 있는 것을 의미한다

라. 독일의 디지털 포렌식 관련 판결

독일의 경우 디지털 포렌식과 관련된 판결의 발견이 쉽지 않다. 물론 미국이나 우리나라의 경우에도 매우 많다고 볼 수는 없지만 독일의 연방헌법재판소의 몇몇 결정이 디지털 포렌식과 연관이 될 수 있기 때문에 간략하게 소개하고자 한다.

1) 이메일 압수·수색 관련 연방헌법재판소 결정

독일에서도 정보의 압수·수색과 관련해서 다양한 문제점들이 논의되고 있다.[530] 그 가운데 하나가 이메일을 압수·수색하는 문제이며, 그와 관련된 사건으로 인해 많은 논란이 있었다. 사건의 내용을 보면 피의자들과 관련된 사기 및 배임사건에서 수사관이 압수·수색영장을 발부받아 피의자들의 주거지를 압수·수색하였다. 그런데 수사관이 피의자의 주거 내에 있는 컴퓨터 뿐 아니라 인터넷 상에서 메일 서비스를 제공하는 Provider의 메일 서버에 있는 이메일에 접근하고자 하였지만, 피의자는 수색결정에 인터넷상의 이메일에 대한 접근을 거부하였다. 따라서 해당 지방법원은 결정으로 인터넷상의 이메일 계정에 저장된 데이터 압수를 명하였고, 수사관이 해당 서비스 제공자로부터 피의자의 메일서버에 있는 2,500개의 이메일을 제출받았고, 피의자는 그에 대해 항고하였다.[531]

해당 사안에서 독일 연방헌법재판소는 서비스 제공자의 메일 서버에 저장되어 있는

---

530) 우리나라처럼 독일에서도 저장매체의 압수, 데이터의 압수, 커뮤니케이션 데이터의 압수, 디지털 증거 수색, 전송되는 정보의 획득 등 디지털 증거를 압수·수색하는 여러 태양에 대한 문제점들에 대한 논의가 매우 뜨겁다; Eric Hilgendorf/ Brain Valerius, Computer- und Internetstrafrecht, 2. Auflage, 2012, 228면~240면.

531) BVerfG, 2 BvR 902/06 vom 16.6.2009. 그에 대한 상세한 설명으로 김성룡, "이메일 압수수색에 관한 독일 연방헌법재판소 결정의 주요 내요과 그 시사점", 경북대학교 법학논고 제32권, 2010, 186~187면.

이메일은 독일 기본법 제10조의 통신비밀보호법을 기준으로 해서 판단되어야 하고, 서비스 제공자의 서버에 저장된 피의자의 이메일을 압수하는 것은 해당 피의자의 통신비밀 기본권을 침해하는 것이지만, 독일 형사소송법 제94조에서는 그 압수를 허용하고 있고, 다만, 제94조에 따라 압수를 하는 경우에도 비례성원칙은 지켜져야 하며, 피의자의 헌법소원청구를 인용하지 않았다.[532] 이에 따르면 서비스 제공자의 서버에 있는 이메일을 획득하는 것은 일반적인 재산권 외에도 통신비밀을 침해하는 것이며, 법률에서 해당 압수·수색에 대해 허용하고 있다고 하더라도 반드시 해당 이메일을 압수·수색하는 것에 있어서는 비례성원칙을 준수해야 한다는 것이다.[533] 이 결정의 연장선상에서 보면 디지털 포렌식에 있어서도 비례성원칙이 요구된다는 것을 알 수 있다.

2) 온라인 수색 관련 연방헌법재판소 결정

또한 온라인 수색(Online-Durchsuchung)과 관련해서 제기되는 문제점도 살펴볼 필요가 있다. 디지털 증거에 대한 획득은 기존의 헌법적 가치인 자유권, 인격권, 정보의 자기결정권과 같은 기본권 뿐 아니라 자신의 정보에 대한 기밀성과 무결성이라는 새로운 기본권도 침해하게 된다.[534] 그런데 디지털 증거의 경우 그 증거를 확보하기가 쉬운 경우도 있지만, 그 물리적 저장장소가 어디인지 모르거나 장소를 알더라도 해외에 있는 경우가 문제될 수 있다. 따라서 독일의 경우 테러와 같은 중대한 범죄에 대한 증거획득의 방법으로 온라인 수색을 할 수 있도록 연방 형사청법률에 규정하고 있다.[535] 이미 국내 여러 문헌에서는 온라인 수색에 대한 내용을 다루고 있기 때문에 여기서는 상세히 다루지는 않겠다.

그런데 최근에 온라인 수색과 관련해서 독일 연방헌법재판소의 새로운 결정이 나왔다. 독일 헌법재판소는 연방 형사청법률의 온라인 수색과 관련된 사안에서 일부위헌

---

532) 김성룡, 앞의 글, 192면.

533) 이경렬, "디지털정보 관련 증거의 압수·수색 규정의 도입방안 연구", 홍익법학 제13권 제3호, 2012, 500면.

534) 즉, 독일 연방헌법재판소는 그동안에는 확인되지 않았던 정보와 관련된 새로운 기본권이 침해되는 것이라고 판단하였다. 그에 대해서는 이원상, "온라인 수색에 대한 고찰 - 독일의 새로운 논의를 중심으로, 형사법연구 제20권 제4호, 2008, 346면~347면.

535) 이에 대해서는 전현욱/윤지영, 디지털증거 확보를 위한 수사상 온라인 수색제도 도입 방안에 대한연구, 2012년 대검찰청 용역보고서, 2012, 51면~62면.

결정을 하였고, 그에 따라 2018년 6월 말까지 개정을 하게 되었다.[536] 독일 연방헌법재판소의 결정 요지를 보면, 국제적인 테러 등의 이유로 연방 형사청에게 온라인 수색과 같이 비밀리에 범죄자의 정보를 획득할 수 있도록 수권을 한 것은 헌법적으로 부합한다고 할 수 있지만, 해당 권한은 비례성원칙에 맞게 형성되고 수행되어야 한다는 것이다. 따라서 연방 형사청이 그와 같은 방법으로 수사를 함에 있어서는 개인의 삶의 영역을 충분히 보호해 주고, 중요한 보호법익이 침해되지 않도록 노력해야 한다. 특히 국가가 사용하거나 국가로 전송되는 데이터는 목적과 관련된 범위내에서만 가능하며, 입법자들도 목적의 범위 내에서 해당 데이터들이 사용될 수 있도록 허용하도록 할 수 있다. 특히 목적의 변경을 통해 해당 데이터를 사용하기 위해서는 위험한 상황에 대한 중요한 요청이 충족되는 경우에 한해서 가능하게 된다. 결론적으로 해외에서 국내의 국가기관으로 데이터를 전송하는 것은 목적관련성 및 목적변경가능성이라는 일반적인 헌법적인 원칙에 의거하여야 하며, 그 판단은 다른 규정을 살펴보아야한다. 그리고 해외에 있는 데이터를 국내로 전송하는 경구 그 해당 국가의 규정에 대한 고려도 하여야 한다고 보고 있다.

해당 결정에서도 비례성원칙의 중요성이 다시 한번 확인되고 있다. 이는 디지털증거의 경우 법률로서 구체적으로 제한하는 것에는 상당한 한계가 있고, 개인의 기본권의 침해 정도도 구체적으로 판단하기 어려운 측면이 있기 때문에 법률에 의해 규정이 되더라도 반드시 비례성원칙을 고려하여야 하며, 법률에 의한 수권을 받아 수행하는 경우에도 비례성원칙을 고려할 것을 요청하는 것이라고 할 것이다.

마. 독일 범죄과학연구소의 시사점

독일 범죄과학연구소가 주는 시사점은 크게 다섯 가지로 나누어 볼 수 있다. 첫째로, 디지털 포렌식에 대한 기술적인 부분을 지속적으로 모니터링하고, 현재의 디지털 포렌식 조직 및 기술에 접목시킬 조직이 필요하다. 독일의 경우 TESIT를 보면 그와 같은 업무를 잘 수행하고 있는 것으로 보인다. 디지털 포렌식 기술은 지속적으로 발전하고 있기 때문에 사실 실무에서 그것을 모두 따라가는 것이 쉽지 않다. 더욱이

536) 1 BvR 966/09.

휴대폰 기술이나 컴퓨터 기술, 암호 기술 등 다양한 분야의 기술들도 함께 발전하고 있기 때문에 지속적으로 관련 기술들을 모니터링하고, 해당 기술을 디지털 포렌식 기관에 접목시키는 것은 매우 중요하다. 그러나 그것은 단순히 기술적인 접목에만 그치지 않고, 법적인 부분, 조직적인 부분, 인력적인 부분 등 다양한 부분들에 걸쳐 있다. 그러므로 기술과 조직, 법학, 실무자 등 다양한 분야의 전문가들이 그와 같은 업무를 전문적으로 수행할 필요가 있다. 그것은 디지털 포렌식에 지속적으로 생명을 연장시켜 주는 것과 같다. 즉, 디지털 포렌식은 항상 현재와 함께 미래를 준비해야 한다. 그러므로 디지털 포렌식 기관 내에 TESIT와 같은 조직을 운영하는 것도 적극 고려할 필요가 있다.

둘째로, 국제적인 기관들과 연계가 되어야 한다는 것이다. 독일처럼 ENFSI를 통해 최신의 정보와 기술을 공유하는 것은 매우 중요하다. 이는 특히 사이버범죄의 경우 기술지배성이[537] 매우 크기 때문에 기술의 발전과 함께 빠르게 발전하고, 또한 전 지구적이기에 한 국가내의 디지털 포렌식 정보와 기술은 한계를 지니게 된다. 그러므로 디지털 포렌식 연구센터의 경우 단순히 국내의 디지털 포렌식을 전담하는 정도의 개념이 아닌 국제 디지털 포렌식 네트워크의 일원으로 참여할 수 있는 능력을 보유해야 할 것이다.

셋째로, 독일의 경우에도 ENFSI의 회원 기관들이 많기 때문에 국제규격을 준수하고 있다는 것이다. 앞서 니더작센주의 경우에 볼 수 있듯이 독일의 각 주의 디지털 포렌식 관련 기관들은 ISO/IEC 17025[538] 인증을 획득하였다. 이처럼 국제적인 규격을 준수하는 이유는 앞에서도 설명한 것과 같이 디지털 포렌식은 한 주나 한 국가에 국한되는 것이 아니고, 특히 유럽의 경우에는 협력 수사가 더욱 요구되는 환경이기 때문에 한 기관에서 디지털 포렌식을 통해 분석된 디지털증거는 다른 주나 국가의 법원에서도 인정되어야 할 필요성이 매우 크다. 더욱이 우리나라에는 디지털 포렌식 업무를 수행하는 기관이 많지 않기 때문에 그 몇몇 기관이 노력을 하게 되면 우리나라의 전체적인 기관이 국제규격을 준수할 수 있게 된다. 그러나 필자가 현재까지 아는 바에 따르면 아직까지 디지털 포렌식과 관련된 국제규격의 취득에는 큰 관심이 없는

537) 그에 대해서는 이원상, 사이버범죄에 있어서 형법의 역할과 시스템적 대처방안, 2003년 석사 학위논문, 2003, 18면 이하 참조.

538) ISO/IEC 17025는 테스트나 측정 연구실의 적격여부에 따라 주어지는 ISO 표준이다.

것 같은데, 이는 아직까지는 디지털증거의 사용이 우리 법원에 한정되기 때문이다. 그럼에도 불구하고 글로벌시대의 글로벌 범죄에 대응하기 위해서는 국제규격의 준수를 고려해 볼 필요가 있다.

넷째로, 범죄과학연구소의 조직을 보면 이전 조직에 비해서 현재의 조직에서 디지털 포렌식과 관련된 조직력이 강화된 것을 볼 수 있다. 이를 통해 우리가 알 수 있는 것은 우리 대검찰청에 디지털 포렌식센터를 두고 있는 것이나 경찰청에 디지털 포렌식센터를 두고 있는 우리의 체계가 이들보다 앞서 있다는 것을 알 수 있다. 즉, 우리나라가 디지털 포렌식과 관련해서 항상 선진국들의 모습을 따라가고 있는 것만은 아니라는 것이다. 다만, 이것이 조직체계에만 그치는 것은 안된다. 그러므로 디지털 포렌식 분야에 있어서 이제는 우리나라가 단순하게 선진국들을 따라가는 것만은 아니므로 해외의 사례를 보고 참고하는 것이 아닌 우리의 체계를 해외에 전파할 수 있도록 현행 체계를 잘 구축하는 것이 필요하다고 생각된다. 그릇은 잘 되어 있기 때문에 그릇 안을 무엇으로 채워야 할지를 계속해서 고민해야 할 것이다.

다섯째로, 유럽의 경우 니더작센주의 범죄기술연구소의 사례에서 살펴볼 수 있는 것과 같이 ENFSI의 회원여부는 디지털 포렌식 절차의 신뢰성 확보에 큰 요건은 아닌 것으로 보인다. 이는 해당 범죄기술연구소의 경우 ENFSI에 속하지 않았지만 ISO/IEC 17025:2005의 인증을 획득하고 있으며, 내부적으로도 전체적인 절차가 객관과 되어 신뢰성을 확보할 수 있도록 노력하고 있다. 따라서 범죄기술연구소에서 분석한 증거결과는 유럽의 다른 국가나 연구소와 교환하더라도 그 신뢰성이 보장될 수 있다. 이는 디지털 포렌식 관련 기관이 어떤 인식을 가지고, 어떤 의지를 가지고 있는지에 따라 디지털 포렌식 품질향상이 영향을 받을 수 있다는 것을 의미한다.

제5절 네델란드의 디지털 포렌식 시스템

1. 네델란드 디지털 포렌식 연구소((Nederlands Forensisch Institut: NFI)

가. 설립목적

디지털 포렌식과 관련해서 주의깊게 살펴볼 필요가 있는 나라가 바로 네덜란드이다. 네덜란드는 특히 우리나라의 경찰청과 밀접하게 교류를 하고 있으며,[539] 그로 인해 우리 경찰청에서는 네덜란드 과학수사 연구소((Nederlands Forensisch Institut: NFI)로 인력을 파견하여 그 기관의 프로세스에 대해 살펴보기도 하였다.[540] 무엇보다 NFI는 세계적으로 법의 원칙이 강화되는 것을 목적으로 삼고 있다. 이를 위해 법과학이 매우 중요한 역할을 하고 있는데, 법과학은 범죄에 대응하는데 있어 수사의 방향을 제시하고 증거를 제공하는데 결정적인 역할을 하기 때문이다. 무엇보다 NFI는 가장 유용하고 선진화된 법과학 결과물들을 발전시키며 이들을 자국 및 전 세계의 다양한 수요자들에게 제공하는 것을 추구하고 있다.[541] 따라서 NFI는 단순한 감정기관에 머물지 않고 형사사법에 관련한 정책방향을 제시하고, 법과학을 통한 정확한 증거확보를 위한 각종 기술 및 정책개발 노력을 하고 있다.[542]

이런 NFI의 목표의식은 최근에 생겨난 것이 아니다. NFI의 역사는 2차 세계대전 직후로 거슬러 올라간다. 1945년에 네덜란드 법무부는 W. Froentjes 교수의 주도하에 사법연구소(Justice Laboratory)를 설립했다. 이후 1951년 병리학자인 J. Zeldenrust를 중심으로 사법의학연구소(Judicial Medical Laboratory)가 설립되기도 하였다. W. Froentjes는 예술 작품 위조에, J. Zeldenrust는 이목을 집중한 살인 사건들과 관련해서 항상 미디어에 언급될 정도로 세간에도 많이 알려지게 되었다. 이후 이 두 개의 연구소는 1999년에 합병되어 NFI로 거듭나게 되었다. 하지만 NFI의 초기 시설 등은 현대적인 요건을 맞추기에는 너무나 부족하였다. 따라서 2004년 보다 적극적이고 활발한 업무추진을 위해 신축 건물로 옮기게 되었다. 그 결과 현재 40여

539) 2011년 경찰청은 NFI와 MOU를 체결하였따(http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=102&oid=003&aid=0003689147〈2016.9.30 최종방문〉.
540) 경찰청, 스마트폰 포렌식 기술 연구, 국외훈련보고서 2012 참조.
541) http://www.forensicinstitute.nl/
542) 김혜경/김택수, 선진국의 법과학 체계 및 입법례 비교, 2014, 113면.

개의 법과학 관련 학문분과들이 이 기관에 소속되어 있으며, 550여 명의 연구 및 지원 인력들이 여기서 업무를 수행하고 있다.[543]

나. NFI의 법과학 품질 보장 체계

우리가 NFI에서 관심을 가질만한 것으로 법과학 품질을 보장하는 체계에 관한 것이다. 이는 이미 앞서 독일의 사례에서도 확인하였지만, 디지털 포렌식 연구소의 품질 보장은 결과물에 대한 신뢰도와 직결되어 있기 때문에 국제규격에 맞고, 객관적인 품질보장 체계가 마련될 필요가 있다. 따라서 NFI의 경우에도 법과학 품질 보장을 매우 중요하게 생각하고 있으며, 그를 위해 확고한 체계를 구축하고 있다. 우선 NFI가 상정하고 있는 연구 품질이라는 개념은 '빠르고, 정확하고, 쉽게 사용될 수 있는 형태'로 수요자의 요구에 맞는 결과물 및 서비스를 공급해 주는 것이다.[544] 그러므로 NFI는 최선의 결과물 및 서비스를 제공하기 위해 무엇보다 객관적이고 과학적인 정합성을 유지할 수 있도록 노력하고 있다. 더욱이 최근 들어 복잡한 형사사건의 문제들을 해결하는 것에 법과학의 중요성이 증대되면서 NFI는 자신의 결과물 및 서비스의 신뢰도 제고를 위해 다양한 측면에서 노력을 기울이고 있다. 특히 내부적으로 품질관리를 수행하는 것에는 다소 한계가 존재하기 때문에 NFI는 과감히 외부 공인 품질관리시스템을 도입하기도 하였다.[545] 그에 따른 NFI의 품질관리시스템의 주요 체계를 보면 다음과 같다.

첫째로, 품질관리시스템 및 보고 시스템을 객관화하기 위한 노력을 하고 있다. 그로 인해 품질관리시스템에 세부적인 절차와 방법에 따라 업무를 수행하도록 하고 있는데, 해당 절차는 수요자의 요구를 수용하는 단계부터 시작해서 NFI의 연구결과에 따른 보고서 작성단계까지 전 과정에 적용된다. 물론 이와 같은 시스템은 웬만한 법과학 기관들이면 모두 가지고 있을 것이다. 그런데 NFI의 시스템에서 주목할 만한 것은 NFI의 품질관리시스템의 근간은 모든 연구활동에 대해 세밀하게 보고서를 작성하는 것에 있다. 그에 따라 세부적으로 명시된 절차에서 벗어나는 모든 활동들은

543) http://www.forensicinstitute.nl/about_nfi/organisation_profile/history/
544) https://www.forensicinstitute.nl/about_nfi/Organisation-profile/Quality.aspx; 2016.9.30.
545) ibid.

향후 개선을 위해서 측정되고 등록된다는 것이다.[546] 쉽게 말해 NFI의 품질관리시스템의 핵심은 추후 검증을 통해서 해당 품질의 객관성이 측정될 수 있고, 개선될 수 있도록 세밀하게 문서화 되는 것에 있다. 특히 NFI의 결과물 및 서비스는 주로 법정에서 사용되게 되는데, 그와 같은 엄격한 절차를 통해 산출된 결과물은 법정에서의 신뢰성을 높여 주는 것과 함께 법과학 절차에서의 문제점을 확인하는 것에도 큰 도움을 주게 된다. 결과적으로 법과학 절차의 투명성과 함께 신뢰성을 보장하는 것이라고 할 것이다.

둘째로, 인증과정을 통한 신뢰도 향상이 있다. NFI는 1994년 이래로 자신의 품질관리시스템에 대해 정기적으로 독립 단체인 네덜란드 인증협회(the Dutch Accreditaion Council)에게 인증을 받고 있다. 이는 해당 기관의 신뢰성을 객관적으로 외부기관에 의해 검증받는 것이다. 특히 해당 인증은 ISO/IEC 17025에 근거하고 있기 때문에 이는 앞서 살펴본 바와 같이 국제적인 규격을 준수하게 되는 것이다. 따라서 NFI는 국내에서의 인증 뿐 아니라 국제규격에 따른 인증을 받게 됨으로 인해서 그 결과물에 대한 국내 및 국제적인 공신력을 갖게 되었다.[547]

셋째로, NFI는 네덜란드 인증협회로부터 인증요건에 충족되는지 여부를 확인받기 위해서 매년 외부감사를 다고 있다. 그 뿐 아니라 NFI는 독자적인 자체감사와 관리검토 등도 매년 시행하고 있으며, 또는 파트너 기관들에게 정기적으로 추가적인 검토를 요청하기도 한다. 이처럼 자체감사, 동료 기관들에 의한 검토, 외부 협회에 의한 감사 등이 수행되면서 NFI의 인증은 단순히 일회적으로 끝나는 것이 아니라 지속적으로 이루어지기 때문에 지속적인 품질관리 뿐 아니라 신뢰도 유지가 가능하게 되는 것이다. 그와 함께 NFI는 외부의 벤치마킹 조사에도 참여하여 자신의 연구소의 역량이 다른 연구소들과 비교하여 어느 정도의 수준에 도달해 있는지도 측정하고 있다.[548]

그리고 넷째로, NFI의 법과학 수사의 과학적 및 법률적 콘텐츠들이 정기적으로 검토를 받고, 해당 내용들이 최신의 내용들을 담고 있는지에 대해서도 평가를 받고 있다. NFI의 이와 같은 노력은 연구결과물이 언제나 최신의 상황에 맞게 유지될 수 있도록 하여 신뢰도를 유지하도록 만들고 있다.[549]

---

546) ibid.
547) ibid.
548) ibid.

이처럼 NFI의 법과학 품질보장 체계는 NFI의 존재이유를 보다 강조하고 있으며, 해당 기관이 네덜란드 국내 뿐 아니라 국제적으로도 공신력 있고 신뢰성 있는 기관이 될 수 있도록 하는 것에 높은 기여를 하고 있다. 물론 구체적으로 들어가게 되면 실제적으로 실무현장에서 체계에 적합한 노력을 하고 있는지는 확실하지 않지만, 적어도 NFI에서 구축하고 있는 품질보장 체계는 적어도 외부의 제3자들에게 해당 기관이 객관적이고 신뢰 높은 기관이라는 인상을 주기에 충분하다고 생각된다. 이와 같은 고품질의 체계를 바탕으로 NFI는 크게 네 가지 분야에서 자국 내 기관 뿐 아니라 국제적으로 서비스를 제공해 주고 있다. 첫째는 NFI의 법과학과 관련된 기본적인 결과물 및 서비스에 관한 것이고, 둘째는 조언과 관련된 서비스이며, 셋째는 교육프로그램이다. 그리고 넷째는 지속적인 연구와 획득된 지식을 체계적으로 저장하는 것이다.

다. NFI의 결과물 및 서비스

앞서 언급한 바와 같이 NFI는 수 십 개의 법과학 관련 분과에서 관련 전문 지식을 통해 발생한 사건에 대한 포렌식 뿐 아니라 잠재적 범죄사건에 대해서도 포렌식을 수행하고 있다. 특히 NFI는 자국의 정부, 자국의 각종 형사사법 관련기관, 자국의 법과학 연구기관에 대해 지원을 하는 것과 동시에 해외의 기관들에 대해서도 법과학 관련 결과물 및 서비스를 제공하고 있다.[550] 다만, 그와 같은 결과물 및 서비스에 대해서는 무상으로 제공되는 것은 아니며, NFI가 자체적으로 마련해 놓고 있는 규정에 따라 일정한 금액을 받고 있다.[551] 그렇게 보면 NFI의 경우 국가기관으로서의 성격과 함께 공공기관의 성격도 함께 가지고 있는 것으로 보인다. 국가기관의 업무를 수행하는 것과 함께 그 외의 업무도 함께 수행하면서 국가적인 법과학의 발전 뿐 아니라 다른 부분에서의 발전도 함께 꾀하고 있는 것으로 보인다.

---

549) ibid.
550) http://www.forensicinstitute.nl/products_and_services/index.aspx:2016.9.30.
551) https://www.forensicinstitute.nl/binaries/alg-leveringsvoorwaarden-diensten-(versie-mei-2015)-uk_tcm120-572668_tcm36-91104.pdf.:2016.9.30.

1) 법과학 결과물 제공

NFI는 해당 기관의 전문지식으로 해결할 수 있는 폭넓은 분야에 있어서 다양한 법과학 결과물들을 제공하고 있다.[552] 일단 해당 분야는 크게 6개로 나누어 볼 수 있다. 첫째로, 보나파르트(Bonaparte)가 있다. 대규모의 자연재해 등으로 희생자들이 발생하였을 경우 그 희생자들의 신원을 파악하는 것은 결코 쉽지 않게 된다. 따라서 NFI는 보나파르트라는 DNA 기술을 사용하여 신속하게 신원을 확인해 주고 있다.[553] NFI는 네덜란드의 라드부드(Radboud) 대학과 공동으로 이 보나파르트 기술을 발전시키고 있으며, 보다 발전된 소프트웨어를 개발하여 보다 신속하고 정확하게 업무가 수행될 수 있도록 노력하고 있다. 특히 2010년 5월 12일 트리폴리에서 있었던 비행기 사고로 103명이 사망한 사건에서 보나파르트를 이용하여 3개월이 걸릴 업무를 3주로 줄이고, 정확하게 희생자를 구분할 수 있었던 것은 큰 공적으로 평가되고 있다.[554]

둘째로, 패러데이 케이지(Faraday cage)가 있다. 페러데이 케이지는 외부의 정전기를 차단하기 위해서 기계장치 주위에 두르는 금속판을 의미한다.[555] 페러데이 케이지는 쉽게 말해 외부에서 원격으로 장치에 접근하여 해당 장치의 내용을 삭제하는 것을 방지하기 위한 기술이다. 예를 들어, 범죄자가 범죄현장에 휴대폰을 남기고 갔는데 그 휴대폰 안에는 범죄와 관련된 중요한 정보들이 있다. 수사관이 그 내용을 살펴보기 위해서는 휴대폰의 전원을 킨 상태에서 내용을 검색해야 하는데, 그와 같은 경우 범죄자가 외부에서 원격적인 방법을 통해 휴대폰의 내용을 모두 삭제할 수 있다. 그러므로 페러데이 케이지는 그와 같은 방법을 통해 디지털 저장매체에 있는 자료를 삭제하는 것을 방지하는 도구라고 할 수 있다. 네덜란드의 경우 특히 모바일 디지털 포렌식에 큰 강점을 가지고 있으며, 네덜란드 경찰도 모바일 기기에 대한 디지털 포렌식의 필요성을 강조하고 있다. 그런데 아래에서 살펴보겠지만 모바일 기기의 정보를 획득하기 위해서는 모바일 기기의 전원을 연결시켜야 하는데, 그 때 범죄자가

552) https://www.forensicinstitute.nl/products_and_services/forensic_products/index.aspx:2016.9.30.
553) https://www.forensicinstitute.nl/products_and_services/forensic_products/bonaparte.aspx:2016.9.30.
554) ibid.
555) 네이버 사전 참조(http://endic.naver.com/popManager.nhn?sLn=kr&m=miniPopMain:2016.9.30.

원격으로 해당 모바일 기기의 내용을 삭제할 수 있는 것이 늘 문제시 되었다. 따라서 네덜란드 경찰의 요청에 따라 NFI는 패러데이 케이지를 개발했으며, 지속적으로 그 기능을 발전시키고 있다.[556]

셋째로, 메모리 툴킷(Memory Toolkit)이 있다. 디지털 포렌식을 위해서는 디지털 저장매체 안의 내용을 읽을 수 있어야 한다. 그런데 디지털 저장매체에 저장된 정보는 물리적으로는 반도체소자의 변화에 따라 기록되고, 소프트웨어적으로는 0과 1의 기계어로 읽혀질 수 있다. 그러므로 해당 매체내의 정보를 읽기 위해서는 그와 같은 내용을 인간이 읽을 수 있도록 변환시켜주는 장치가 필요하게 된다. NFI 메모리 툴킷은 그와 같은 역할을 수행하는 것이다. 그러므로 메모리 툴킷을 사용하여 수사관들은 각종 모바일 기기 내의 메모리 칩에 저장되어 있는 정보를 추출하고, 읽을 수 있게 된다.[557] 특히 NFI 메모리 툴킷은 하드웨어와 소프트웨어로 구성되어 있으며, 모바일 기기의 손상이나 암호화로 인한 해독의 어려움, 삭제로 인한 추출의 어려움에도 대응하고 있기 때문에 디지털 포렌식을 위해 다양하게 사용되고 있다.[558]

넷째로, 디프레이저(Defraser)가 있다. 최근 동영상의 활용이 빈번해 지면서 동영상 등 멀티미디어 파일가 범죄의 증거로 사용되는 경우가 많아지고 있다. 하지만 경우에 따라서는 해당 파일이 손상되거나 삭제되어 사용하지 못하는 경우가 있는데, 디프레이저는 그와 같은 경우를 대비하여 만들어진 도구이다. 디프레이저는 포렌식 분석 도구로서 데이터 스트림 중에 있는 멀티미디어 파일을 전부 또는 부분적으로 복구할 수 있고, 필요에 따라서는 그것들을 원상태로 수정할 수 있는 장치를 의미한다.[559] 특히 이와 같은 방식은 디스크의 빈 공간이 없어서 복구할 수 없는 경우 스트림의 방법을 통해서 디지털 포렌식을 하는 것을 가능하게 해준다.

다섯째로, PRNU 컴페어 프로페셔널(PRNU Compare Professional)이 있다. 해당 기술은 모바일 기기 등의 카메라 기능과 관련된 기술이다. 모바일 기기 등에는 대개

---

556) https://www.forensicinstitute.nl/products_and_services/forensic_products/faraday-cage.aspx:2016.9.30.
557) https://www.forensicinstitute.nl/products_and_services/forensic_products/nfi-memory-toolkit.aspx:2016.9.30.
558) https://www.forensicinstitute.nl/binaries/brochure-memory-toolkit-mtk-en-ams-20110520-def_tcm120-448609_tcm36-21578.pdf.:2016.9.30.
559) https://www.forensicinstitute.nl/binaries/brochure-nfi-defraser_tcm120-563783_tcm36-21561.pdf.:2016.9.30.

카메라 기능이 장착되어 있는데 그를 통해 촬영된 영상이 범죄의 입증을 위해 필요한 경우가 많다. 하지만 해당 사진이 그 카메라를 통해 촬영되었는지, 서로 다른 사진이 동일한 카메라로 촬영되었는지를 밝힐 필요성이 존재하기도 한다.[560] 따라서 NFI는 PRNU 컴페어 프로페셔널이라는 도구를 통해서 그와 같은 문제를 해결하고 있다. 예를 들어, 유럽에서 많은 문제가 되고 있는 아동음란물 사진이 발견된 경우 해당 아동음란물이 범죄자의 카메라로 촬영되었는지를 입증하는 것은 매우 어렵다. 그러나 범죄자의 카메라에 저장된 다른 사진과 아동음란물 사진을 비교분석하여 동일한 카메라로 찍은 것이 입증된다면 해당 아동음란물 사진이 범인의 카메라로 찍었다는 것을 증명할 수 있게 된다. 따라서 PRNU 컴페어 프로페셔널은 외부 데이터베이스와 연동되어 5000개가 넘는 패턴을 신속하게 비교 분석하여 결과를 도출하고 있다.[561]

여섯째로, 한스켄(Hansken)이 있다. 한스켄은 이전의 XIRAF[562]의 발전모델이라고 할 수 있다. 2010년 10월 브터 NFI는 테라바이트(terabyte)가 넘는 엄청난 양의 디지털 데이터를 처리할 수 있는 디지털 포렌식 서비스(Digital Forensics as a Service)를 제공하고 있다. NFI는 엄청난 양의 디지털 정보에 쉽고, 안전하며, 빠르게 접근할 수 있는 체계를 구축하여 수사관이 간편하게 이용할 수 있는 서비스를 제공해 주고 있는 것이다.[563] 다만, 해당 기술의 경우 빅데이터를 다루고 있기 때문에 다양한 리스크(Risk)가 존재하게 된다. 그러므로 보안(Security), 프라이버시(Privacy), 투명성(Transparency), 다중공유(Multi-tenancy), 장래의 입증(Future proof), 데이터 유지(Data retention), 신뢰성(Reliability), 높은 가용성(High availability)을 대원칙으로 해서 해당 시스템을 운영하고 있다.[564]

---

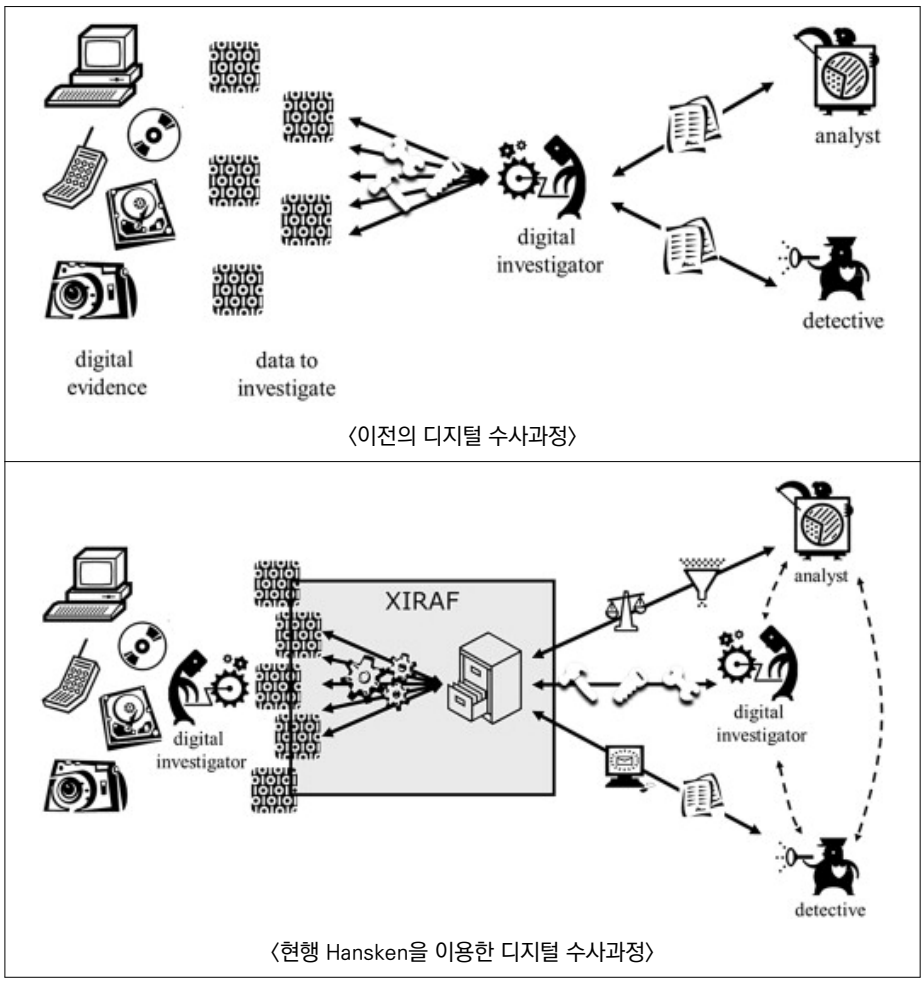
560) https://www.forensicinstitute.nl/products_and_services/forensic_products/prnu-compare-professional.aspx:2016.9.30.

561) https://www.forensicinstitute.nl/binaries/brochure-nfi-prnu-compare-professional_tcm36-21580.pdf.:2016.9.30.

562) XIRAF는 여러 장비에서 획득한 대량의 데이터들을 초고속으로 자동 분석하고, 데이터들을 검색할 수 있도록 해주는 첨단 소프트웨어 도구이다; 이원상/탁희성/송봉규, 앞의 글, 69면.

563) 해당 기술에 대한 구체적인 설명은 R.B. van Baar/H.M.A. van Beek/E.J. van Eijk, "Digital Forensics as a Service: A game changer", Digital Investigation 2014, vol. 11 Sup 1, 2014, pp.54~62 참조.

564) H.M.A. van Beek/E.J. van Eijk/R.B. van Baar/M. Ugen, J.N.C. Bodde/A.J. Siemelink, "Digital forensics as a service: Game on", Digital Investigation Vol. 15, 2015, p.23.



[그림 13] NFI 디지털 수사 절차[565]

이처럼 NFI가 제공하고 있는 여러 결과물들 가운데 가장 많은 것이 디지털 포렌식과 관련된 결과물들이다. 이는 최근 디지털 포렌식에 대한 중요성이 부각되고, 우리 사회의 곳곳에서 디지털 기기들이 사용되면서 나타나게 되는 현상에 대응하기 위한 것으로 이해된다. 이처럼 NFI는 변화하는 디지털 환경에 맞추어 지속적으로 관련 기술을 개발하고, 다양한 결과물들을 산출해 내고 있다.

565) R.B. van Baar/H.M.A. van Beek/E.J. van Eijk, op.cit., p.56, 59.

2) 법과학 서비스 제공

NFI가 제공하고 있는 서비스도 매우 다양하다. 그러나 그 가운데 CBRNe, 손가락 자국 식별, 핵보안 포렌식, 빅데이터 분석 포렌식, 모바일 데이터 복구, 야생환경 포렌식 등 크게 6가지의 서비스를 주목해 볼 필요가 있다.[566]

첫째로, CBRNe가 있다.[567] 최근 들어 테러리즘은 세계 곳곳에서 발생하고 있다. 특히 화학적 무기나, 생물학적 무기, 방사능 또는 핵 등을 사용하는 테러는 전 세계의 국가들과 시민들에게 크나큰 위협이 되고 있다. 그러므로 각 국 정부는 그와 같은 위협에 대응하기 위한 방안을 마련하고, 지속적으로 대응해 나가야 하는데, NFI에서는 그와 같은 각 정부들의 활동을 보조해 주기 위해서 CBRNe를 제공해 주고 있다. CBRNe는 크게 네 가지 영역에서 지원을 해 주고 있다. 하나는 CBRNe 사건 현장에서의 운영을 지원하는 것이고, 다른 하나는 CBRNe 사건 현장에서 전통적인 포렌식 수사를 수행하는 것이다. 그리고 다른 하나는 CBRNe 사고에 있어 사용되는 에이전트들을 프로파일링 하는 것이며, 다른 하나는 CBRNe 사고를 미연에 방지할 수 있도록 노력하는 것이다.[568] 즉, NFI CBRNe 팀은 사고나 공격발생시 즉시 배치될 수 있도록 준비하고 있으며, 해당 사건에 대한 정보 저장과 프로파일링을 통해서 각 국가의 정부들이 그 사건에 대응하는 것을 지원해 주고 있는 것이다.[569]

둘째로, 부분 손가락 자국 식별화(Fingermark Individualisation) 서비스를 제공해 주고 있다. 이는 지문식별에 대한 새로운 방식의 포렌식이라고 할 수 있다. 이제까지는 지문이 범죄 증거로 자주 사용되었지만 충분한 정도의 지문이 있어야 식별이 가능했다. 하지만 NFI는 확률적 접근방법(The probabilistic approach)을 통해서 충분한 정도의 지문이나 손바닥 모양이 없는 경우에도 식별이 가능하도록 하였다.[570] 즉, NFI는 수많은 불특정 다수에 대한 지문 데이터베이스를 구축하였고, 불분명한 지문을

---

566) https://www.forensicinstitute.nl/products_and_services/forensic_services/: 2016.9.30.

567) CBRNe란 "The use of chemical, biological, radiological and nuclear agents, possibly spread by means of explosives"의 약자를 의미한다.

568) https://www.forensicinstitute.nl/products_and_services/forensic_services/CBRNe/index.aspx:2016.9.30.

569) https://www.forensicinstitute.nl/binaries/brochure-cbrne-en-2011.def_tcm120-448796_tcm36-18845.pdf.

570) https://www.forensicinstitute.nl/products_and_services/forensic_services/Fingermark_Individualisation/index.aspx:2016.9.30.

비교대조 하여 전문가가 지문의 일치율을 판단하도록 하는 것이다. 그와 같은 방법을 통해 과거에는 쓸모없이 버려졌던 손자국들이나 부분 지문들이 매우 유용하게 사용될 수 있게 되었고, 수사에도 많은 도움이 되고 있다.

셋째로, NFI는 핵보안 포렌식 서비스도 제공해 주고 있다. NFI는 최근 핵 테러리즘의 문제가 높아져 가고 있는 가운데 핵보안 포렌식 프로그램을 제공해 주고 있다. 해당 프로그램의 목적은 핵과학과 법과학의 지식을 공유하고, 그것을 통해 방사능 또는 핵사고로 인한 주요 인프라의 보호 및 시민의 보호를 위해 사용하는 것이다.[571] 즉, 핵과학 기술의 경우 그 복잡성과 위험성으로 인해 문제가 발생하더라도 그 원인을 밝혀내기가 쉽지 않기 때문이며, 그러므로 문제가 발생하는 경우 핵과학기술과 법과학 기술을 이용하여 문제점을 파악하고 그에 대응할 수 있도록 해주기 위해서이다. 핵보안 포렌식의 경우 그 중요성과 위험성이 매우 크기 때문에 특별히 따로 관리하고 있기도 하다.[572]

넷째로, 빅데이터 분석을 통한 포렌식 서비스를 제공한다. 이는 최근 빅데이터의 중요성이 높아지면서 새롭게 추가된 서비스라고 할 것이다. 이를 위해 KECIDA (Knowledge and Expertise Centre for Intelligent Data Analysis)라는 부서를 만들고 해당 부서에 전문가들을 배치하여 다양한 빅데이터 분석활동을 수행하고 있다.[573] 빅데이터 분석은 크게 각종 텍스트에서 자동적으로 관련된 정보를 인식·분류·요약하는 텍스트 마이닝(Text mining), 해당 데이터들을 검토하고 데이터에 대한 통계와 패턴 등을 분석하여 사건을 예측하고 연관시켜주는 데이터 프로파일링(Data profiling), 금융정보의 흐름을 분석하여 사기나 부패범죄, 테러범죄등에 사용되는 돈의 흐름을 파악하는 금융 데이터 분석(Financial data analysis), 그리고 각종 소셜 네트워크 서비스 분석을 통해 사건 관계인들이 어떻게 연결이 되어 있고, 어떤 정보들을 나누었는지를 살펴보면 소셜 네트워크 분석(Social network analysis) 등으로 나누어진다.[574] 법과학에서 빅데이터 분석이 중요한 이유는 정형화된 데이터 외에 비정형

---

571) https://www.forensicinstitute.nl/products_and_services/forensic_services/Forensics_in_Nuclear_Security_Programme/index.aspx:2016.9.30.

572) 그러므로 핵보안 포렌식에 대해서는 따로 홈페이지가 마련되어 있다(http://www.nuclearforensics.eu/:2016.9.30.

573) https://www.forensicinstitute.nl/binaries/brochure-kecida-en-ams-20110525-def_tcm36-19563.pdf.:2016.9.30.

화된 데이터를 분석할 수 있다는 것이다. 그러므로 기존에는 분석할 수 없는 내용까지 분석이 가능게 된다. 그러므로 KECIDA에서는 구조화 되거나 구조화 되지 않은 다양한 유형의 데이터를 분석하고, 수요자가 데이터의 편차를 확인할 수 있는 프로파일링이나 인자 등을 제공하며, 네트워크를 확인하고, 빅데이터 분석기술을 보다 발전시키며, 현 시스템이나 새로운 시스템의 데이터 분석 설계에 대한 조언을 제공하고 있다.[575]

다섯째로, 모바일 폰 데이터 복구 서비스를 제공하고 있다. 앞서 언급한 바와 같이 NFI의 모바일 포렌식은 세계적으로도 알려져 있으며, 해당 기관도 그 부분을 특화시키고 있다. 그러므로 NFI는 범죄자의 모바일 폰에 있는 각종 사진이나 동영상, 메시지, 위치정보 등 증거로 사용될 수 있는 정보들을 데이터의 암호화나 훼손, 삭제, 모바일 폰의 손상 등의 어려운 조건을 이겨내고 획득하는 기술과 서비스 제공을 위해 지속적으로 노력하고 있다. 특히 모바일 폰의 메모리에서 정보를 획득하는 과정은 소프트웨어적으로만 가능한 것이 아니다. 하드웨어적인 작업을 통해서 모바일 폰에서 메모리를 분리하고, 분리된 메모리를 NFI 메모리 툴킷을 사용하여 하드웨어적인 작업을 거치면서 소프트웨어를 통해 획득하기도 한다.[576] 이와 같은 기술은 모바일 폰의 향상과 함께 보조를 맞추어야 하기 때문에 NFI는 관련 기술의 향상을 위해서도 많은 노력을 기울이고 있다.

여섯째로, 야생환경을 위한 포렌식 서비스도 제공하고 있다. 국제적으로 불법 밀렵 등이 성행하면서 보호되어야 하는 동식물들이 멸종 위기에 처해있다. 그러므로 NFI는 국제기구나 정부기관들에게 멸종 위기에 있는 동식물들의 불법 거래를 방지하도록 하기 위해 야생환경과 관련된 포렌식 서비스를 제공하고 있다. 따라서 DNA 프로파일링을 통해 각종 종에 대한 식별을 가능하게 하고, 각종 동식물을 사용한 생산품에 포함되어 있는 종들을 확인하며, 동식물에 해를 주는 도구나 약물들이 어떤 것이지에 대한 결정도 하고 있다.[577]

---

574) https://www.forensicinstitute.nl/products_and_services/forensic_services/Forensic_Big_Data_Analytics/index.aspx:2016.9.30.
575) ibid.
576) https://www.forensicinstitute.nl/products_and_services/forensic_services/Mobile_Phone_Data_Recovery/index.aspx:2016.9.30.
577) https://www.forensicinstitute.nl/products_and_services/forensic_services/Wildlif

라. 컨설턴트 서비스

법과학과 관련해서 그 중요성이 증대대고 있는 것은 세계 어느 국가에나 해당한다. 특히 각 국가의 법과학 기관들은 법과학의 처리과정과 경영, 품질확보, 거버넌스의 필요성 증대에 대응해야 할 뿐 아니라 기술의 변화와 법률의 변경, 그리고 주요 파트너인 법집행기관의 수요 변화에도 반응하여야 한다. 하지만 이런 모든 환경의 변화에 대한 대응이 단기간에 이루어지기는 쉽지 않다. 그러므로 NFI는 해당 기간이 이제까지 쌓아온 경험과 기술력을 바탕으로 다른 법과학 기관들이나 기구들에 대해 컨설턴트 서비스를 제공해 주고 있다.[578] NFI가 컨설턴트 서비스를 제공하는 내용을 살펴보면 법과학 기관들이 보다 효율적인 운영 절차를 담보할 수 있도록 해주는 것과[579] ISO 17025 또는 ISO 17020 등 국제규격을 획득할 수 있도록 준비할 수 있도록 해주는 것,[580] 법과학 관련 기관 등을 대상으로 적절한 매니지먼트 교육 제공,[581] 효율적이며 실제적인 법과학의 근무환경이 조성될 수 있도록 하는 것,[582] 그리고 초동조사자나 의학 실무자, 다른 범죄와 관련된 분야의 사람들에게 법과학적 인식이 만들어질 수 있도록 하고 있다.[583] 이와 같은 서비스는 NFI가 가지고 있는 노하우를 다른 기관 등에게 전파하여 법과학 분야가 전체적으로 높은 수준을 유지할 수 있도록 도와주고 있다.

---

e_Forensics/index.aspx:2016.9.30.

578) https://www.forensicinstitute.nl/products_and_services/consultancy_services/:2016.9.30.

579) https://www.forensicinstitute.nl/products_and_services/consultancy_services/Ensuring%20efficient%20operational%20processes.aspx:2016.9.30.

580) https://www.forensicinstitute.nl/products_and_services/consultancy_services/Preparing%20for%20Quality%20Assurance%20certification.aspx:2016.9.30.

581) https://www.forensicinstitute.nl/products_and_services/consultancy_services/Providing%20appropriate%20management%20training.aspx:2016.9.30.

582) https://www.forensicinstitute.nl/products_and_services/consultancy_services/Designing%20an%20efficient%20and%20practical%20working%20environment.aspx:2016.9.30.

583) https://www.forensicinstitute.nl/products_and_services/consultancy_services/Generating%20forensic%20awareness.aspx:2016.9.30.

마. 트레이닝, 워크숍 및 교육 제공

NFI가 중점을 두고 있는 것 가운데 하나가 바로 트레이닝, 워크숍, 교육 제공이다. NFI의 그와 같은 사고는 UN차원에서 늘 제기되는 Capacity Building와도 관련이 있다. 현대 사회의 특징으로 제기 되는 것 가운데 하나가 바로 '글로벌화(global)'와 '과학화(scientific)'라고 할 수 있다. 우리가 살고 있는 사회가 급속히 국제화 되어 가면서 국경을 초월하는 범죄들이 빈번하고, 또한 과학과 및 기술화 되면서 고도의 전문지식이나 기술이 요구되고 있다. 따라서 글로벌화 된 범죄수사, 법집행이라는 맥락에서 NFI는 고도의 법과학 전문지식을 수사에 접목하는 것과 개발한 기술과 경험을 여러 관련 기관들과 기구들에 보급하는 것이 매우 중요하게 된다. 이에 NFI는 자신들이 개발한 다채로운 트레이닝과 워크숍 및 교육 프로그램 등을 서비스하며, 자신들의 기술과 경험을 전파하고 있다.[584] 해당 서비스는 크게 세 부분으로 나누어 살펴볼 수 있다.

첫째로, 해당 서비스의 참가자는 이미 해당분야에 전문성을 가지고 있는 사람들 뿐 아니라 해당 분야의 전문가가 되기 위해 수련중인사람, 법집행기관 직원 등 매우 다양하다. 좀 더 상세히 살펴보면 의료분야의 초동대응을 하는 사람(First-responders in the medical sector), 포렌식 수사관(Forensic investigators), 형사(Police detectives), 재판관(Magistrates and judges), 변호사(Prosecution counsel), 포렌식 절차의 관리자 및 행정가(Managers and administrators in the forensic chain), 그리고 대학에서 법과학을 전공하는 학생(Students of Forensic Science at universities and colleges) 등이다.[585]

NFI에서 제공해 주는 해당 서비스의 장점은 크게 네 가지로 제시되고 있다.[586] 첫째, 이론과 실제의 조합에 의한 수업이 가능하다는 것이다. NFI는 사실상 세계적인 법과학 연구기관으로서 매 년 수만 건이 넘는 법과학 수사와 분석 업무를 수행하고 있다. 따라서 NFI의 아카데미 코스와 전문 교육은 이론적인 부분과 실무적인 부분을

584) https://www.forensicinstitute.nl/products_and_services/training_workshops_courses/: 2016.9.30.
585) https://www.forensicinstitute.nl/products_and_services/training_workshops_courses/participants.aspx: 2016.9.30.
586) https://www.forensicinstitute.nl/products_and_services/training_workshops_courses/key-benefits.aspx: 2016.9.30.

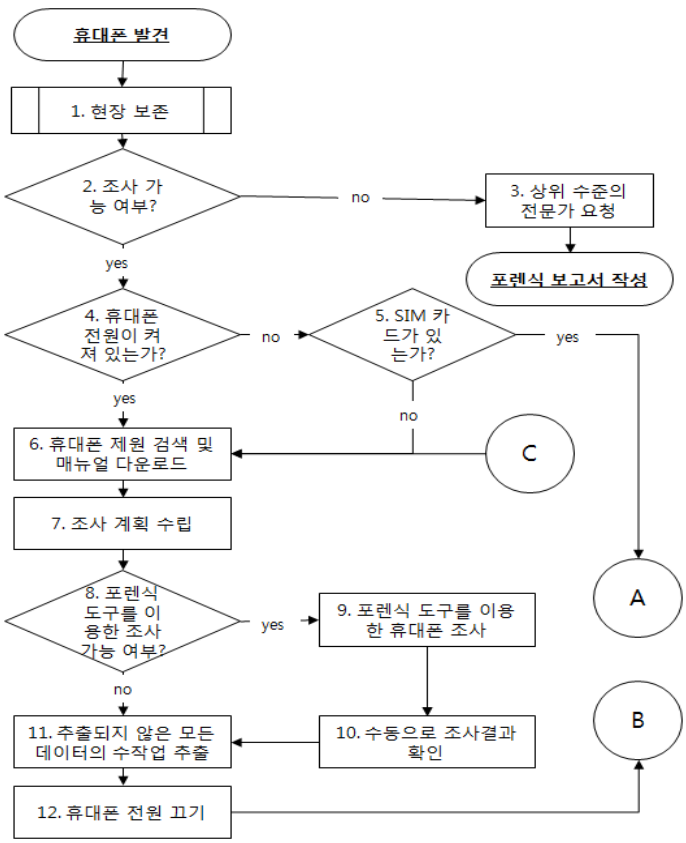
모두 아우르게 된다.[587] 둘째, 가장 최신의 기술이나 실무 등의 발전상황을 신속하게 반영할 수 있다. 앞서 언급한 것과 같이 법과학 분야는 매우 역동적으로 변화하고 있기 때문에 범죄수사 및 기소를 위해서는 끊임없이 새로운 기술이 요구된다. 그에 따라 NFI는 가장 최신의 기술이나 방법들을 아카데미 코스에 적용하고 있다.[588] 셋째, 기초적인 분야에서 부터 구체적인 연구분야까지 넓은 범위의 주제를 제공해 주고 있다. 따라서 NFI는 독성학 및 병리학에서 부터 디지털 기술 및 유전자 분석에 이르기까지 대략 40여 개의 법과학 연구 분야를 아우르는 실무를 담당하고 있다. 그러므로 몇몇 아카데미 코스에서는 기초적인 지식과 관련된 정보를 제공해 주고 있으며, 몇몇 코스에서는 보다 구체적이고 세밀한 주제를 다루기도 한다. 이는 일반적인 교육에서부터 특수한 교육까지 다양한 지식 수요자들의 요구에 부합하는 것이다.[589] 넷째, 코스를 담당하고 있는 인력이 풍부한 경험을 가지고 있는 현장 전문가 뿐 아니라 해당 분야에서 선도적인 역할을 수행하고 있는 과학자들이라는 것이다. 즉, NFI 아카데미 코스와 워크숍, 교육 프로그램은 범죄 현장 수사 및 분석 등에서 선도적으로 업무를 수행하고 있는 NFI 전문가들에 의해 진행된다. 그러므로 그들이 실무에서 경험한 내용 및 연구의 내용들이 직접적으로 전달될 수 있도록 하고 있다.[590]

바. NFI 모바일 포렌식 절차

우리나라 경찰청의 디지털 포렌식센터에서 주목할만 것으로 모바일포렌식과 관련된 조직을 두고 있는 것이다. NFI 모바일 포렌식 절차를 좀 더 상세히 살펴볼 필요가 있다. NFI의 경우 네덜란드 법원과 경찰청과 함께 제정한 모바일 포렌식 모델에 따라 모바일 포렌식을 수행하고 있다.[591] 해당 모델의 순서도에 따라 절차를 살펴보면 다음과 같다. 먼저 수사관이 휴대폰을 발견하였다면 우선 현장을 보존하고 조사가능 여부를 판단하게 된다. 만일 조사가 불가능하게 되면 상위수준의 전문가에게 요청을 하게 되는데, 그를 위해서는 포렌식 보고서를 작성해야 한다. 조사가 가능한 경우에는

587) ibid.
588) ibid.
589) ibid.
590) ibid.
591) 경찰청, 스마트폰 포렌식 기술 연구, 국외훈련보고서 2012, 43면.

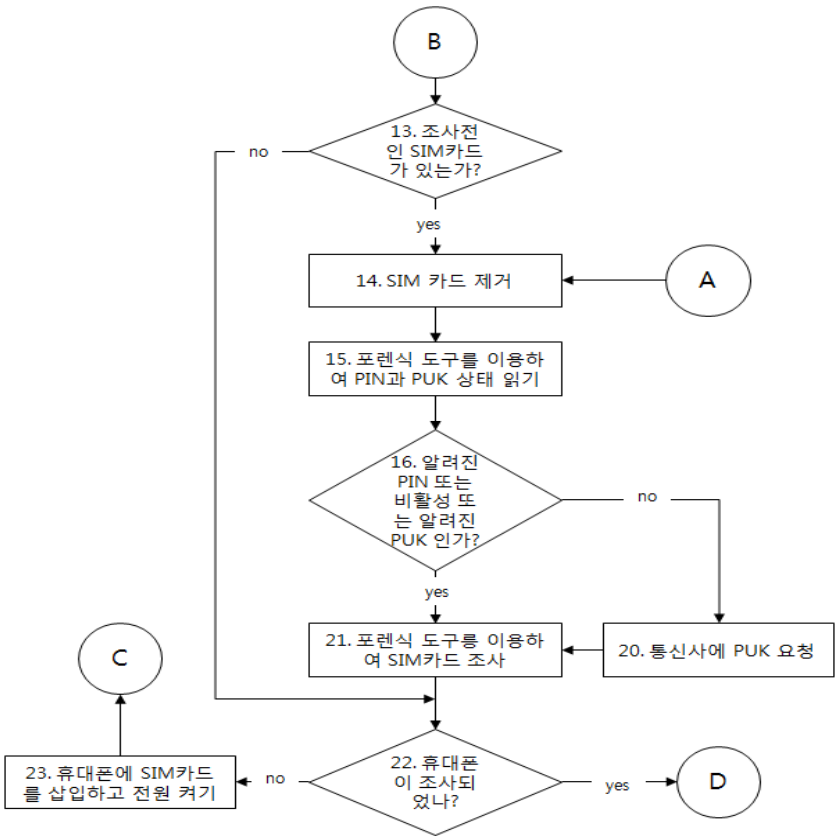
휴대폰의 전원이 켜져 있는지를 살펴보고, 그렇지 않다면 SIM카드 유무를 확인하고, SIM카드가 있는 경우에는 A절차를 진행하고, 그렇지 않은 경우에는 C절차를 진행한다. 휴대폰 전원이 켜져 있는 경우에는 휴대폰 제원을 검색하고, 매뉴얼을 다운받는다. 그리고 조사계획을 수립하고 포렌식 도구를 이용하여 조사 가능여부를 판단한다. 조사가 가능하다면 조사를 수행하고, 수동으로 조사결과를 확인한다. 조사가 가능하지 않는다면 추출되지 않은 모든 데이터를 수작업을 통해 추출한다. 그리고는 휴대폰을 끄고 B절차를 진행한다.



[그림 14] NFI 모바일 포렌식 순서도 1/3: (경찰청 국외훈련 보고서)

B절차는 다음과 같이 진행된다. 조사전인 SIM카드가 있는 경우 SIM 카드를 제거하고 포렌식 도구를 이용하여 PIN과 PUK 상태를 읽는다. 알려진 PIN 또는 비활성화

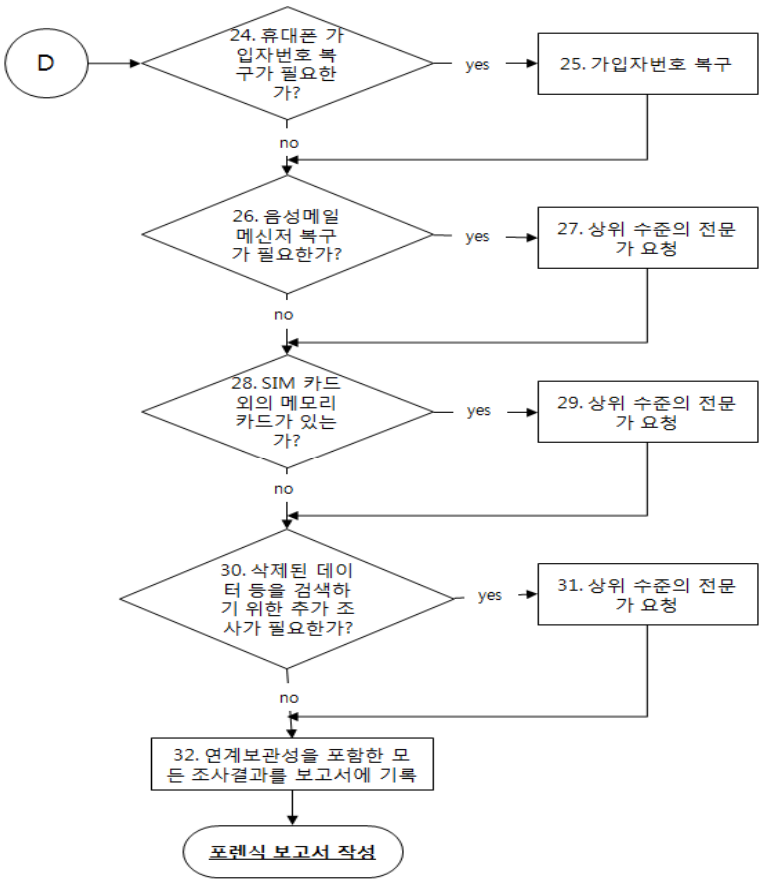
되었거나 알려진 PUK여부를 살펴보고, 그렇지 않다면 통신사에 PUK를 요청한다. 알려진 경우라는 포렌식 도구를 이용하여 SIM카드를 조사하고 휴대폰이 조사되었는지 여부를 판단해서 그렇다면 D절차를, 그렇지 않다면 휴대폰에 SIM카드를 삽입하고 전원을 켠 후, C절차를 진행한다.



[그림 15] NFI 모바일 포렌식 순서도 2/3: (경찰청 국외훈련 보고서)

D절차는 다음과 같다. 휴대폰 가입자번호복구가 필요한지를 판단하여 그렇다면 가입자번호를 복구하고, 그렇지 않다면 음성메일 메신저 복구여부를 판단한다. 복구가 필요하면 상위 수준의 전문가에게 요청하고, 그렇지 않다면 SIM카드 외에 메모리카드가 있는지를 살펴본다. 추가 메모리카드가 있다면 상위 수준의 전문가에게 요청하고, 그렇지 않다면 휴대폰에 삭제된 데이터가 있는지를 살펴본다. 있다면 상위 수준

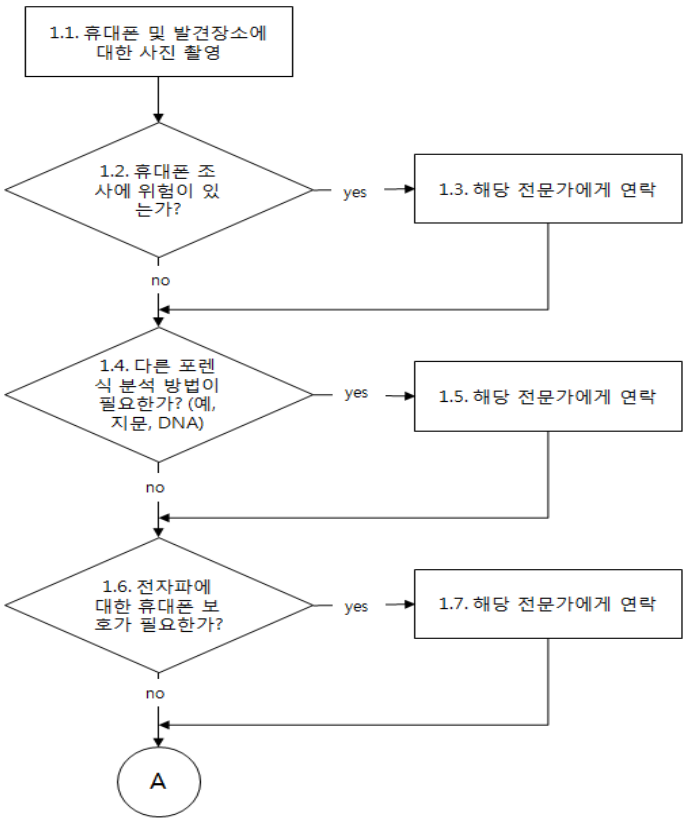
의 전문가에게 요청하고, 그렇지 않다면 연계보관성을 포함한 보든 조사결과를 보고서에 기록하고, 포렌식 보고서를 작성한다. 일선 수사관은 해당 순서도에 따라 기계적으로 수행하면 된다. 자신의 능력을 넘어서는 부분에 대해서는 상위 수준의 전문가에게 요청하면 그 뿐 이다.



[그림 16] NFI 모바일 포렌식 순서도 3/3: (경찰청 국외훈련 보고서)

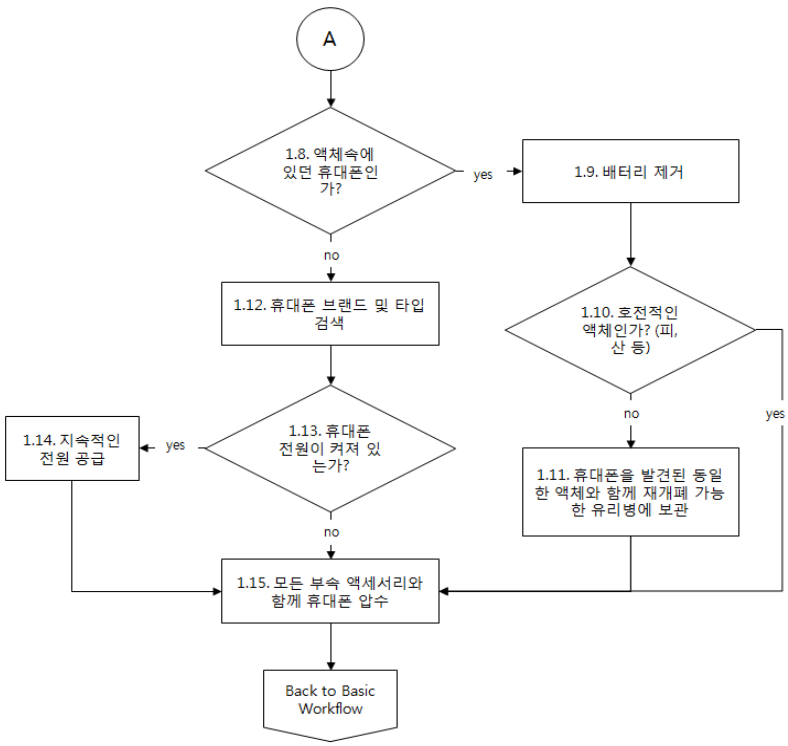
또한 현장보존의 절차는 다음과 같이 수행하면 된다. 우선 휴대폰 및 발견장소에 대한 사진촬영을 하고, 휴대폰 조사에 위험이 있는지를 판단해서 있다면 전문가에게 연락을 하고, 없다면 지문이나 DNA와 같은 다른 포렌식 분석방법이 필요한지를 판단

한다. 있다면 해당 전문가에게 연락을 하고, 없다면 전자파에 대한 휴대폰 보호가 필요한지를 판단한다. 그렇다면 해당 전문가에게 연락하고, 그렇지 않다면 A단계를 진행한다.



[그림 17] 현장 보존 프로세스의 순서도 1/2: (경찰청 국외훈련 보고서)

A절차에서는 먼저 휴대폰이 액체 속에 있었는지 여부를 판단하고, 그렇다면 배터리를 제거하고 어떤 종류의 액체인지를 살펴봐서 피나 산 등이라면 모든 부속 액세서리와 함께 휴대폰을 압수하고, 그렇지 않다면 함께 발견된 액체와 함께 재개폐가 가능한 유리병에 보관하여 압수를 한다. 액체속에 없었다면 휴대폰 브랜드 및 타입을 검색하고, 휴대폰이 켜져 있는지를 살펴봐서 전원을 공급하여 압수하고, 그렇지 않다면 그 상태로 압수를 한다.



[그림 18] 현장 보존 프로세스 순서도 2/2: (경찰청 국외훈련 보고서)

이미 우리나라의 수사기관들도 그와 같은 절차에 의해 업무를 수행할 것이라고 생각된다. 그러나 주목할 점으로 이와 같은 절차를 수사기관과 법원이 함께 제정했다는 것이다. 즉, 수사기관은 이 절차에 따라 모바일 포렌식을 수행했다는 것만 입증하게 되면 법원은 그 절차를 신뢰하게 되는 것이다. 이와 같은 협력은 디지털 포렌식에 있어서 매우 의미있는 것이라고 할 것이다.

사. 네덜란드 포렌식 연구소의 시사점

NFI는 사실상 ENFSI에서도 가장 핵심적인 역할을 수행하고 있다. 특히 우리 경찰이 가장 주목하고 모델로 삼고 있는 기관 중 하나라고 할 수 있다. NFI에서 눈에 띄는 것은 해당 기관이 디지털 포렌식과 관련된 제도가 기술에 있어서 언제나 선도적으로 대응하고, 다른 기관들과의 네트워크의 중요성을 이해하고 실제로 업무에 연결시키고

있다는 것이다. 그처럼 NFI는 지속적으로 디지털 포렌식에 대한 품질관리를 하기 때문에 NFI의 디지털 포렌식 절차는 유럽차원에서도 매우 높은 신뢰성을 받고 있다는 것이다. 특히 모바일 포렌식과 관련해서는 상당히 높은 기술을 가지고 있어서 다른 기관에서 수행할 수 없는 디지털 포렌식을 수행하기도 한다. 예를 들어, 암호로 인해 접근할 수 없는 스마트폰을 물리적으로 분리하여 그 내용을 알아내기도 한다. 매일매일 신속하게 변화하고 있는 디지털 포렌식 기술에 대해 수사기관이 뒤처지지 않기 위해서는 선재적인 기술도입과 지속적인 품질관리가 중요하다.

또한 NFI의 모바일포렌식 절차에서 볼 수 있듯이 해당 절차를 만드는데 있어 법원과의 협의가 있었다는 것은 매우 주목해 볼 필요가 있다. 디지털 포렌식 절차는 디지털 증거를 법정에 제출하기 위한 과정이다. 따라서 디지털 포렌식 절차가 불투명하거나 신뢰성이 없는 경우에는 그를 통해 산출된 디지털 증거도 법정에서 사용할 수 없게 되는 것이다. 그런데 법원은 수사기관이 수행하는 디지털 포렌식 절차에 대해서 항상 신뢰를 줄 수는 없다. 이는 디지털증거가 쉽게 변경될 수 있기 때문이다. 하지만 언제나 디지털 포렌식 절차를 의심하여 절차에 대한 검증을 거치게 된다면 재판의 중심이 정작 디지털증거에 대한 검증이 아니라 디지털 포렌식 절차에 대한 검증에 중점을 둘 수밖에 없다. 이는 현행 우리의 상황을 보면 쉽게 알 수 있다. 그러므로 법원이 디지털 포렌식 절차모델에 참여하여 절차의 신뢰성을 담보한다면 재판에서는 디지털 증거의 검증에 보다 집중할 수 있게 된다. 그러므로 NFI에서 법원과 함께 만든 모바일 포렌식 절차가 우리에게 주는 시사점은 매우 클 수 있다.

또한 NFI의 경우 네덜란드의 포렌식과 관련된 모든 기능을 수행하고 있다. 따라서 디지털 포렌식과 관련된 경험과 기술은 대부분 NFI가 가지고 있다고 하겠다. 그러므로 디지털 포렌식과 관련해서 이론뿐 아니라 실무에 관한 부분에 대한 교육자료도 해당 기관이 가장 풍부하다고 할 것이다. NFI의 조직도를 보면 'NFI 학교'가 있다. 이 기관에서는 디지털 포렌식과 관련된 경험을 전파하는 기능을 한다고 하겠다. 현재 우리나라의 경우 디지털 포렌식과 관련된 교육을 몇몇 대학에서 주로 담당하고 있다.[592] 그러나 살아있는 디지털 포렌식 교육을 위해서는 디지털 포렌식 기관이 교육의

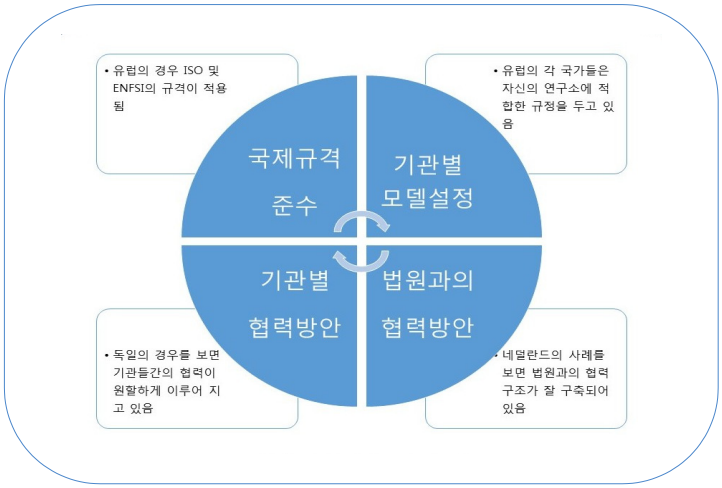
592) http://www.yonhapnews.co.kr/bulletin/2016/09/27/0200000000AKR20160927190400004.HTML?input=1195m〈2016.9.30 최종방문〉.

일부도 담당하는 것이 매우 효과적이라고 사료된다.

제6절 주요 외국의 디지털 포렌식 시스템에 있어서의 시사점

유럽 주요국의 디지털 포렌식 모델 구축현황을 살펴보면서 우리나라에는 크게 네 가지 부분에서 주목해야할 점들이 있다. 다만, 그 보다 앞서 유럽의 경우 우리나라와는 다소 다른 정치적·사회적·문화적·지리적·사이버 환경에 처해 있다는 것을 이해할 필요가 있다. 유럽의 경우 많은 국가들이 국경을 맞대고 있으며, EU라는 큰 테두리 속에서 국가간 인구의 이동이 매우 많은 편이다. 그러므로 대부분의 정책이나 모델이 단순히 한 국가 차원에 머무르기 보다는 EU차원에서 논의되고, EU차원에서 논의되는 내용들이 각 회원국들의 상황에 맞게 적용되는 과정을 거치게 된다. 그에 반해 우리나라는 삼면이 바다이며, 위로는 북한이 중국과의 직접적인 접촉을 막고 있기 때문에 사실상 고립된 섬나라와 같은 지위에 있다. 그러므로 대부분의 정책이나 모델들이 우리나라 영역내로 국한된다. 비록 지방자치제가 시행되고 있어서 각 지방이 자치권을 가지고 있다고 하더라도 그 범위는 상당히 제한적이며, 미국이나 독일과 같이 연방제의 형식을 취하고 있는 것도 아니다.

그에 반해 정치적 또는 정책적 차원에서는 미국 뿐 아니라 일본, 중국, 러시아 등과도 밀접한 관계를 맺을 수밖에 없는 상황이다. 더욱이 사이버공간에서는 북한은 우리나라에 대한 주요 공격자이고, 상당수의 사이버범죄가 중국을 그 발원지로 삼고 있으며, 또한 상당수 해킹범죄들은 우리나라를 경우해서 발생하기도 하는 특수성을 가지고 있다. 따라서 유럽 주요국의 디지털 포렌식 모델 구축현황을 살펴보고 우리나라에 적용가능성 여부를 판단함에 있어서는 그와 같은 다양한 환경적 요소들을 입체적으로 고려할 필요가 있다.



[그림 19] 우리에게 주는 시사점

첫째로, 디지털 포렌식에 있어서는 반드시 국제규격을 준수할 필요가 있다. 앞서 살펴본 바와 같이 유럽의 경우 크게 국제규격인 ISO의 규격과 유럽의 규격인 ENFSI의 규격을 만족시키는 범위 내에서 각 연구소 등이 디지털 포렌식을 수행하고 있다. 이는 기본적으로 디지털 포렌식에 의한 디지털증거의 사용이 단순히 한 기관이나 한 국가에 국한되지 않는 것에서 기인한다. 따라서 가능한한 국제적 또는 지역적인 표준을 준수할 필요가 있다. 이는 디지털 포렌식이 과학기술을 사용하고 있기 때문에 해당 기술에 대한 객관적인 품질이 보증될 필요가 있기 때문이다. 그 이유에 대해서는 ISO 9001의 사례를 통해서 알 수 있다. ISO 9001은 "제품 및 서비스에 이르는 전 생산 과정에 걸친 품질보증 체계"를 의미한다.[593] 여기서 주목할 것이 ISO 9001이 단순히 제품 자체의 품질만을 보증해 주는 것에 그치는 것이 아니라 제품 및 서비스 뿐 아니라 생산과 공급하는 전 과정에 대한 품질경영시스템을 평가하고 인증해 주는 것이다. 따라서 ISO 9001 인증을 받은 생산자가 생산하는 물건은 구매자에게 신뢰감을 줄 수 있으며, 그로인해 생산과 구매 절차가 쉽게 이루어 질 수 있게 된다. 물론 ISO 9001 인증을 받았다고 해서 모든 제품이나 서비스가 최고임을 보증해 주는 것은 아니다. 그러나 적어도 해당 인증을 통해 생산된 제품이나 서비스는 국제적으로 인정

593) 네이버 시사상식사전 참조(http://terms.naver.com/entry.nhn?docId=1987148&cid=43667&categoryId=43667).

하는 일정수준 이상의 품질을 보증해 줄 수 있다. 그런 맥락에서 디지털 포렌식에 있어서도 국제적인 표준을 준수할 필요가 있다고 하는 것이다.

이는 앞서 살펴본 유럽의 사례에서도 쉽게 발견할 수 있다. 유럽지역 내의 디지털 포렌식에 대한 표준을 제공해 주고 있는 ENFSI의 가이드라인을 살펴보면 여러 부분에서 ISO가 규정해 놓고 있는 표준들을 적용하고 있는 것을 보게 된다. 그러므로 ENFSI가 규정한 표준을 적용하는 유럽연합의 각 국가의 여러 연구소들은 ENFSI의 표준에 따라 자신들의 가이드라인을 만들게 되면 당연히 ISO 규격도 준수하게 되는 것이다. 그러므로 유럽연합내 국가의 어느 한 기관에서 디지털 포렌식을 수행하게 된 경우에는 해당 결과에 대한 품질을 보증 받을 수 있게 될 것이고, 법원의 입장에서도 그 결과를 증거로 채택하지 않을 이유가 없게 될 것이다. 이는 우리 법원 뿐 아니라 해당 결과가 다른 국가의 법원에서 사용되는 경우에도 매우 유용하게 된다. 그러므로 디지털 포렌식에 있어서는 해당 국제규격을 준수할 필요가 있다.

둘째로, 자신의 기관에 적합한 모델을 설정할 필요가 있다. 다만, 해당 모델은 단순히 자신의 기관에서 자생적으로 만드는 것이라기 보다는 국제기준 및 지역기준을 수용하여 자신의 기관에 맞도록 커스터마이징 한 것이어야 할 것이다. 물론 우리나라의 경우에는 지역기준이라는 것이 없기 때문에 ENFSI의 규격을 참조하면 유용할 것이다. 또한 이미 우리나라의 디지털 포렌식 관련 지침들이 해외의 지침들을 참조하였기 때문에 어느 정도 반영되어 있을 것이다. 그러나 디지털 포렌식은 기술적인 요소가 있고, 기술은 계속해서 발전하고 있기 때문에 일회적인 참조만으로는 충분하지 않고, 지속적인 검토와 반영이 필요할 것이다.

앞서 살펴본 바와 같이 유럽의 각 국가의 디지털 포렌식 관련 연구소들은 '디지털 포렌식을 위한 모범 실무 매뉴얼'을 기반으로 삼고 있다. 이처럼 해당 모범 매뉴얼이 기반이 될 수 있는 이유는 EC에서 ENFSI에 대해 신뢰를 주고 있기 때문이기도 하다. EC가 ENFSI를 신뢰하고, 그 매뉴얼도 인정해 주고 있기 때문에 각 연구소들은 당연히 ENFSI의 모범 매뉴얼을 중심으로 자신들의 매뉴얼을 만들어야 공신력을 갖게 되는 것이다. 해당 매뉴얼의 구성에 따르면 해당 매뉴얼의 앞부분에서는 해당 매뉴얼의 취지나 목적, 배경 등을 개관하고 있는 목적(Aims), 매뉴얼의 업무범위 등을 정하고 있는 범위(Scope), 매뉴얼에서 사용되는 용어 및 정의(Definitions and Terms) 등을

규정하고 있다. 그리고나서 인적자원(Personnel), 사용장비(Equipment), 표준물질(Reference Materials), 시설과 환경조건(Accommodation and Environmental Conditions), 파일보관(Archive) 등에 관한 내용과 상호검토(Peer Review), 프로토콜 검사(Examination Protocols), 연구(Research) 등과 관련된 규정을 두고 있다. 또한 검정방법과 측정도구의 불확실성에 대한 평가방법과 숙달정도 테스트 방법(Proficiency Testing), 도구사용방법 등과 같이 디지털 포렌식의 절차와 관련된 규정들을 두고 있으며, 사건 평가(Case Assessment), 조사의 우선순위와 순서, 사건의 재구성 방법, 평가방법과 해석방법 등과 같이 사건의 분석과 관련된 내용, 그리고 분석된 내용을 증거로 제출하는 방법에 대해서 규정하고 있다. 그 뿐 아니라 디지털 포렌식 수행자의 건강과 안전과 관련된 내용과 함께 해당 업무를 수행하는데 도움이 되는 관련 문헌들도 소개해 주고 있다. 그러므로 각 국가들의 연구소들은 해당 모범 매뉴얼을 자신의 연구소에 커스터마이징 하여 자신의 연구소에 맞는 모델을 구축하게 되는 것이다.

여기서 중요한 것은 '커스터마이징'이라고 할 것이다. 우리나라의 경우 디지털 포렌식과 관련된 기관으로는 대검찰청 디지털 포렌식센터(DFC),[594] 경찰청 사이버안전국 디지털 포렌식센터,[595] 국립과학수사연구원(NFS)[596] 등이 있다. NFS는 국립과학수사연구원 본원의 법공학부 내에 디지털분석과를 두고 있으며, 디지털분석과 내에 '디지털 포렌식실'과 'U-포렌식 랩'을 두고 있다. 그런데 각 기관들은 모두 같은 업무를 처리하고 있지만 구조적인 측면이나 운영적인 측면에서는 다소 차이점이 있다고 하겠다. DFC는 대검찰청에서 컴퓨터 포렌식, 데이터베이스 포렌식, 모바일 포렌식, 디지털 포렌식연구, 분석회피대응 등의 주요 업무를 수행하는 것과 동시에 전국디지털수사망을 운영하여 전국에 있는 검찰청의 디지털 포렌식 업무를 지원해주고 있다. 특히 DFC의 경우 디지털 포렌식연구 뿐 아니라 분석회피대응에도 주력하고 있기 때문에 그와 같은 특성이 매뉴얼에 반영될 필요성이 있다. 그리고 경찰청 사이버안전국 디지털 포렌식센터는 디지털 포렌식 정책기획을 담당하고 있는 '포렌식기획팀', 새로운

---

594) 대검찰청 홈페이지 참조(http://www.spo.go.kr/spo/major/forensics/forensics01.jsp).
595) 경찰청 사이버안전국 홈페이지 참조(http://cyberbureau.police.go.kr/bureau/sub4.jsp?mid=040401).
596) 국립과학수사연구원 홈페이지 참조(http://www.nfs.go.kr/main.action).

환경에 적합한 기법 및 도구를 개발하는 '첨단기법개발팀', 모바일기기 포렌식에 중점을 둔 '모바일포렌식팀', 그리고 악성코드 등 증거분석을 하는 '컴퓨터포렌식팀' 등으로 구성되어 있다. 다른 조직에 비해 모바일포렌식에 많은 중점을 두고 있기 때문에 매뉴얼에 있어서는 그와 같은 부분이 반영될 필요가 있다. 또한 NFS의 특징은 디지털 포렌식실과 함께 U-포렌식 랩을 두고 있어 원격 과학수사서비스를 제공해 주고 있다. 그러므로 NFS의 경우에는 그 특수성이 매뉴얼에 반영될 필요가 있다. 이처럼 디지털 포렌식을 수행하는 각 기관들이 가지고 있는 특성은 모두 다르기 때문에 반드시 커스터마이징을 통해서 자신의 조직에 적합한 디지털 포렌식 모델을 구축할 필요성이 있다.

셋째로, 디지털 포렌식 관련 조직들은 다른 조직과 협력할 수 있는 통로를 구축해 놓아야 한다. 이는 독일의 경우에서도 살펴볼 수 있다. 독일의 경우 비록 BKA에서 디지털 포렌식과 관련된 주요 업무들을 수행하고 있지만, 다른 기관들과도 그와 관련된 업무에 대해서 협력을 하고 있다. 사실 유럽의 주요국에 대한 분석이기 때문에 미국에 대한 분석은 없었지만, 미국의 경우에도 디지털 포렌식과 관련해서 기관들간의 긴밀한 협력이 있다. 다만, 그와 같은 협력이 단지 국가기관에 국한되어서는 안된다. 그 이유는 디지털 포렌식의 경우 다양한 기술과 결합되어 있고, 그에 맞는 툴(tools), 전문인력, 프로세스 등이 요구되는데 기술에 있어서는 국가기관에 비해 민간기관이 항상 앞서가기 때문이다. 하지만 그에 반해 우리나라 디지털 포렌식의 수요는 민간분야에서는 거의 없는 상황이므로 실제적인 사용의 경험은 국가기관이 압도적으로 많다고 할 것이다. 그러므로 민간분야의 기술은 지속적으로 기관으로 유입되어야 하며, 기관의 경험은 민간분야로 유입되어 기술개발에 도움을 줄 수 있어야 한다.

또한 국가기관들 사이의 협력은 더욱 중요하다고 할 것이다. 현재 우리나라의 경우 디지털 포렌식과 관련된 민간시장은 거의 없다고 할 것이다. 이는 미국의 경우 민사소송에서도 디지털증거가 많이 사용되고 있기 때문에 민간분야에서도 디지털 포렌식의 수요가 있는 것에 반해 우리는 민간분야에서는 디지털증거의 활용이 거의 없기 때문이다. 따라서 디지털 포렌식은 주로 형사사건과 관련해서 사용되며, 그로인해 주로 검찰이나 경찰, 국과수 정도가 주요 수요자라고 할 것이다. 그런데 사실 디지털 포렌식과 관련해서는 검찰과 경찰 및 국과수의 협력관계가 다소 구분되어 있다. 예를 들어,

학회의 경우에도 검찰주도 디지털 포렌식학회와[597] 경찰주도 디지털 포렌식학회가[598] 구분되어 있다. 또한 유럽의 ENFSI에서 볼 수 있었던 것과 같이 모든 디지털 포렌식 전문가들이 참여할 수 있는 논의의 장도 찾아보기 쉽지 않다. 즉, 우리나라의 경우 국가의 많지 않은 디지털 포렌식 관련 기관들이 한 곳에 모여 디지털 포렌식과 관련된 기술이나 절차, 협력 등을 논의할 수 있는 창구가 실질적으로 없다고 할 수 있다. 그러므로 우선 디지털 포렌식 관련 민·관의 기관들이 함께 논의할 수 있는 논의의 장이 만들어질 수 있도록 노력할 필요가 있다.

넷째로, 디지털 포렌식 절차에 있어 법원의 참여도 매우 필요하다. 이는 네덜란드의 NFI의 사례를 통해서 살펴볼 수 있다. 디지털 포렌식이 중요한 이유는 디지털 포렌식을 통해 산출되는 증거가 범죄를 입증하기 때문일 것이다. 그런데 수사기관의 디지털 포렌식 절차를 거친 디지털증거가 법정에서 증거로 사용되기 위해서는 증거능력을 인정받고, 증명력을 인정받아야 한다. 문제는 디지털 포렌식을 거치는 디지털증거는 쉽게 변경될 수 있다는 특성으로 인해 매우 엄격한 절차가 요구된다. 그런 가운데 현재 우리 법원은 디지털 포렌식과 관련된 절차에 대해서는 전혀 관여하지 않고, 단지 그 절차만을 판단하는 역할만을 하고 있다. 그러므로 법원의 디지털 포렌식에 대한 관점이 다소 불명확하게 나타나기도 한다. 예를 들어, 소위 종근당 사건에서 법원은 압수한 디지털 증거 가운데 해당 사건과 관련이 없는 증거는 삭제할 것을 요구하고 있다. 하지만 법원이 요구하는 삭제가 어떻게 이루어져야 할지, 압수한 뒤 검찰청의 디지털 포렌식센터 서버에 저장된 증거를 삭제하라는 것인지, 아니면 해당 서버에서 다운로드 받은 수사관의 컴퓨터에 저장된 증거를 삭제하라는 것인지가 명확하지 않다. 즉, 법원은 삭제를 요구하고 있지만, 디지털 포렌식의 어느 절차에서 어떻게 해야 할지를 구체적으로 밝히고 있지 않으므로 그에 대해 다양한 견해들이 제시되고 있다.[599] 만일 법원이 디지털 포렌식 절차의 과정을 좀 더 상세히 알고 있었다면 좀 더 명확한 판결문이 나왔을 것이라고 생각된다.

그러므로 법원이 디지털 포렌식의 모델과정에 대해 참여하여 디지털 포렌식의 절차

597) 한국포렌식학회(http://www.forensickorea.org/).
598) 한국디지털 포렌식학회(http://www.kdfs.or.kr/).
599) 이완규, "디지털 증거 압수수색과 관련성 개념의 해석", 법조 제686권, 2013, 152면; 이상미, "관련성 없는 디지털증거 삭제 시 이중해쉬를 이용한 무결성 입증방안", 제12회 광주전남 법학교수검찰 실무연구회 자료집, 2016, 46~50면.

가 법원에 의해 인정된다면 소송절차가 좀 더 원활하게 진행될 수 있을 것으로 여겨진다. 현행 시스템에 따르면 똑같은 내용의 증거가 수사기관에 의해 아날로그 형태로 압수되었다면 큰 문제없이 법원에 증거로 제출되어 검토될 수 있지만, 디지털증거의 형태라면 법원에 대해 디지털 포렌식 절차의 적절성과 신뢰성에 대해 인정을 받은 후에야 비로소 디지털증거를 법원이 검토할 수 있게 된다. 그렇기 때문에 피고인측은 디지털 증거의 내용보다는 디지털 포렌식 절차의 부당성을 주장하는 것에 중점을 두게 된다. 이는 실체적 진실발견 이라는 소송법의 이념을 실현하는 데에도 문제가 될 수 있을 것이다. 따라서 법원이 디지털 포렌식의 모델에 관여하여 법정에서는 디지털증거의 내용에 중점을 두고 다투어질 수 있도록 하는 것이 보다 적절할 것이다.

제4장

KOREAN INSTITUTE OF CRIMINOLOGY

디지털 포렌식 프로세스 통합을 위한 사전적·예비적 고려사항

탁 희 성

제4장

디지털 포렌식 프로세스 통합을 위한 사전적·예비적 고려사항

제1절 디지털 포렌식 프로세스 통합의 필요성

디지털 포렌식 프로세스는 단순히 디지털 포렌식 업무내용을 순서에 따라 배치하는 데서 그치는 것이 아니라, 전체 프로세스에 적용되는 관리 및 운용정책과 시스템 내에서 각 단계별로 디지털 증거가 이동하는 과정이 정확하게 기록되고, 각 단계별 구성요소에 대한 표준화 요구사항이 적용되어야 한다. 이렇게 함으로써만 디지털 포렌식 업무에 사용되는 프로세스와 절차가 적합한 품질을 유지할 수 있고, 법정에 신뢰성 있는 결과를 제공할 수 있다고 할 것이기 때문이다. 따라서 이와 같이 포렌식 업무 절차를 전체적으로 관리·통제할 수 있다는 점에서 통합적인 포렌식 프로세스로 규정될 수 있을 것이다.

이와 같이 디지털 포렌식에 있어서 프로세스 구축을 통한 각 절차의 통합적인 관리 및 통제의 필요성이 요구되는 이유는 다음 몇 가지로 정리해 볼 수 있다.

1. 법률적 프로세스와 기술적 프로세스의 유기적 연계

일반적인 범죄수사 절차에 있어서는 담당 수사관의 경험과 지식만으로도 압수·수색의 계획부터 증거물 압수, 피의자 신문, 압수 증거물의 보관 및 법정 제출에 이르기까지 전반적인 수사절차를 진행할 수 있다. 하지만 이와는 달리 디지털 증거를 수반하는 수사에 있어서는 디지털 포렌식 전문가의 경험과 지식 그리고 디지털 포렌식 도구의 도움이 없이는, 압수할 디지털 증거의 범위를 확정할 수 없는 것은 물론이고, 디지털 증거 자체를 압수하지 못하거나, 압수한 디지털 증거의 훼손 및 오염 발생으로

인하여 법정 증거로서 사용하지 못하는 문제가 발생할 수 있다.

대부분의 디지털 증거를 수반하는 사건에 있어서는 디지털 증거 외에 달리 범죄 혐의를 입증할 수 있는 자료가 없는 경우가 일반적인 바, 디지털 증거를 확보하지 못함으로 인해 또는 확보한 디지털 증거의 신뢰성을 유지하지 못하여 실체적 진실을 밝히지 못함으로 인해 형사사법적 정의에 반하는 결과를 초래할 수 있는 것이다. 즉, 다음과 같은 우려가 제기될 수 있다고 할 것이다.

첫째, 기관의 실정에 따라 디지털 증거에 대한 압수·수색을 준비하는 단계에서 디지털 포렌식 전문가의 협조와 지원을 받지 못함으로써 현장에 적합한 증거의 선별 및 수집방법을 제대로 구현하지 못하여 비례성의 원칙에 반하는 결과를 초래할 수 있다.

둘째, 디지털 증거의 압수·수색 현장에서 증거의 선별 및 수집 작업에 디지털 포렌식 전문가가 아닌 비전문가인 일선 수사관이 투입됨으로 인해 증거의 무결성 확보에 문제가 발생할 가능성이 있다.

셋째, 수사를 담당하는 수사관과 분석관의 업무 연계성이 분명하지 않게 되면 양자의 공동작업을 통해 증거를 찾아내는 것이 아니기 때문에, 수사관이 찾고자 하는 증거에 대한 명확한 계획을 갖고 있지 않으면 분석관이 정확하게 증거를 찾아낼 수가 없고, 경우에 따라서는 잦은 재분석 요청으로 인해 증거의 연계성에 단절이 발생할 가능성에 대한 우려도 배제하기 어렵다.

이와 같이 디지털 증거를 수반하는 사건에 있어서는 법률적 지식과 수사실무상의 경험을 지닌 수사관과 과학적 지식과 기술적 경험을 지닌 디지털 포렌식 조사관(분석관)의 유기적인 협조와 연계가 전제되지 않으면, 증거의 신뢰성을 물론이고 수사절차 자체에 대한 신뢰성 까지 이의가 제기될 수 있는 것이다. 따라서 법률적 프로세스와 기술적 프로세스의 유기적인 연계 및 상호 협력지원을 가능하게 하기 위해서는, 수사기관내의 디지털 포렌식 업무에 대한 거버넌스 프레임워크를 확대하여 기존의 수사업무를 디지털 포렌식 프로세스내로 통합함으로써 일관된 정책적·기술적 프레임안에서 각 단계별 프로세스간 피드백과 인터페이스를 구축할 필요가 있다.

2. 디지털 포렌식 업무에 대한 일관성 있는 신뢰기준 확보

디지털 포렌식은 기본적으로 법원에 대한 증거제출을 염두에 두고 행해지기 때문에 증거법적 판단의 근거로서 디지털 포렌식에 대한 신뢰성을 확보해야만 한다. 이러한 디지털 포렌식에 대한 신뢰는 기관의 업무에서 요구되는 정책적·절차적 표준에 따른 연계성 확보를 통해서 디지털 증거의 입증가치가 엄격한 통제하에서 보존·유지되었다는 것을 증명할 수 있는 절차적 염결성을 통해서 확보될 수 있다.

하지만 이와 같이 디지털 포렌식 절차의 염결성이 확보된다고 해도 그 과정에서 업무에 활용되는 포렌식 도구와 그 도구를 운영하는 포렌식 분석관의 업무 품질이 확보되지 못하면 디지털 포렌식의 신뢰는 깨질 수 밖에 없다. 즉, 디지털 증거를 수반하는 수사절차 전반에 걸쳐 엄격한 관리·통제시스템이 적용되어 절차의 진행과정중에 디지털 증거의 입증가치를 훼손할 여지가 전혀 개입되지 않았다고 할지라도, 디지털 증거를 수집하고 분석하여 결과를 산출하는 도구가 신뢰할 수 없는 것이고, 그 도구를 운용하여 최종적으로 법원에 디지털 증거를 통한 혐의사실에 대한 증명내용을 제출하는 포렌식 전문가의 지식과 기술이 관련 업무수행에 부적합하다면, 그에 의해 산출된 디지털 포렌식 결과는 법적 절차에서 허용될 수 없는 것이 된다.

따라서 디지털 포렌식 프로세스를 통해 신뢰할 수 있는 결과를 산출하고, 확보한 정보의 품질이 강력한 입증가치를 유지하기 위해서는 디지털 포렌식 프로세스내에서 요구되는 인적·기술적 품질수준을 증명할 수 있는 표준적인 기준이 포렌식 프로세스 안에 적용되어 있어야 할 것이다.

가. 디지털 포렌식 도구에 대한 신뢰 기준으로서의 검증

디지털 기술이 발전함에 따라 이에 대응하기 위한 디지털 포렌식 기술 역시 빠르게 발전하고 있다. 따라서 디지털 포렌식 업무에 활용되는 도구의 변화가 다른 어떤 포렌식 분야보다도 빠르다고 할 수 있다. 일반적으로 디지털 포렌식 업무에 있어서는 상용화된 도구와 자체 개발한 도구가 혼용되고 있다.

상용화된 도구 가운데 일부는 이미 전세계적으로 널리 활용되고 있어서 여러 측면에서 여러 전문가에 의해 기능적 요구사항에 대한 검증이 어느 정도 이루어졌거나

또는 공신력 있는 CFTT에 의한 테스트를 거침으로써 도구의 적절성에 대한 검증이 이루어졌다고 할 수 있다. 하지만 디지털 기술이 세분화되어감에 따라 그에 적용되는 도구의 요구사항도 매우 구체적이고 세밀한 부분으로 제한되기 때문에, 상용화된 도구라 할지라도 CFTT에 의한 테스트를 거친 경우가 아니고서는 그에 대한 검증이 제대로 이루어지고 있다고 보기는 어렵다고 할 것이다.

더욱이 기관내 포렌식 업무의 필요성에 따라 자체 개발된 도구인 경우에는 자체적으로 사용하는 과정을 통해 그 기능의 적합성 여부를 확인하는 것 외에는 달리 그 도구의 적합성에 대한 검증이 행해질 수 있는 프로세스가 존재하지 않는다. 특히 기관내 정책적 방침에 따라 개발된 도구의 소스코드가 비공개되는 경우에는 외부 전문가에 의한 검증이 불가능한 것은 물론이고, 형사절차의 당사자인 피고인측이 기관에서 산출한 분석결과를 재분석하고자 해도 그 도구가 어떤 방법과 기술을 활용한 것인지 확인할 수 없기 때문에 그 신뢰성 여부를 검증할 방법이 없다고 할 수 있다.

디지털 포렌식 도구는 그것을 누가 사용하느냐에 관계없이 과학적 타당성이 고려된 최소한의 기준을 충족해야 하며, 그러기 위해서는 도구가 결과를 산출해내는 프로세스를 설명할 수 있는 알고리즘이 정의되어야 하고, 그 기능이 예측가능해야 하며, 허용가능한 오류의 범위내에서 재현가능해야 하고, 프로세스를 검증할 수 있는 측정 시스템을 갖추어야 하는 것이다.[600] 이와 같이 디지털 포렌식 도구에 대한 검증시스템이 디지털 포렌식 프로세스내에 적용됨으로써 프로세스 업무품질에 대한 신뢰가 확보될 수 있다고 할 것이다.

나. 디지털 포렌식 분석관에 대한 신뢰 기준으로서 자격인증

디지털 기술의 빠른 변화는 이를 분석하여 결과를 추출해내야 하는 디지털 포렌식 분석관의 지식과 기술수준을 한계에 부딪치게 하는 결과를 낳는다. 디지털 포렌식 분야도 디지털 기술과 환경이 변화감에 따라 전통적인 컴퓨터 포렌식에서 모바일 환경에서 요구되는 포렌식 분야 - 모바일, 암호, 클라우드, 사물인터넷, 안티포렌식 등 -로 점차 세분화되고 다양화 되어가고 있는 추세에 있기 때문에, 이러한 기술분야

600) 래리 다니엘/라즈 다니엘, 포렌식 전문가와 법률가를 위한 디지털 포렌식, 2012, 44면.

의 발전에 대응할 수 있는 지식과 실력을 갖추지 않고서는 디지털 포렌식 업무를 제대로 하기 어렵다고 할 수 있다.

따라서 디지털 포렌식 분석관의 전문성과 기술수준을 유지하기 위해서는 지속적인 교육과 훈련 그리고 실력에 대한 검증이 필요한데, 현재 각 기관들은 체계화된 교육훈련 시스템을 갖추고 있지 못한 것이 현실이다. 더욱이 디지털 포렌식 업무량에 비하여 분석업무를 담당하는 인원이 적은 관계로 교육기회도 제대로 갖기 어려울 뿐만 아니라, 교육훈련에 따른 테스트를 통해 실력을 검증할 수 있는 기회도 갖지 못하고 있다.

이와 같이 디지털 포렌식 분석관의 지식 및 기술적 능력에 대한 일정한 수준이 유지되지 못하는 경우 법정에서 전문가로서 증언을 할 수 없는 문제가 제기될 수 있다. 즉 결과를 산출한 분석관이 해당 포렌식 업무에 적합한 지식과 기술적 능력을 갖추었는가에 대한 검증자료를 법원 또는 반대 당사자가 요구하는 경우, 이를 제출하지 못함으로 인해 전문가 증인의 적격을 인정받지 못하게 되면 그가 분석한 결과도 증거로서 활용하지 못하는 문제가 발생할 수 있다고 할 것이다. 특히 형사소송법이 개정되어 디지털 포렌식 자료에 의해 디지털 증거의 진정성립을 인정할 수 있게 됨으로 인해 디지털 포렌식 분석관의 전문가 증언이 필수적으로 요구되는 상황에서 전문가 증인으로서 자격증명방법이 요구된다고 할 것이다.

현재로서 디지털 포렌식 실무 분야에서 필요한 최소한의 자격을 갖춘 포렌식 전문가의 전문성을 검증할 수 있는 시스템이 있어야 하며, 전문가 자격은 디지털 포렌식에 관한 전문적인 기술교육을 이수하고 디지털 증거 분석에 대한 경력이 있어야 하는 것 뿐만 아니라 구체적으로 산출된 결과와 관련된 분야에 대한 전문성도 증명할 수 있어야 할 것이다.[601]

---

601) 래리 다니엘/라즈 다니엘, 앞의 책, 90-93면. ; 디지털 포렌식 전문가들이 참여하는 워크숍에서 분석관들은 디지털 포렌식 분석관이 전문가 증언을 함에 있어서 전문가로서의 지위를 유지하기 위해서는 지속적인 훈련과 검증이 중요하다고 지적하고 있다; Sean E.Goodison/Robert C. Davis/Brain A. Jackson, “Digital Evidence and the U.S. Criminal Justice System:Identifying Technology and other needs to more effectively acquire and utilize digital evidence”,; https://www.ncjrs.gov/pdffiles1/nij/grants/248770.pdf

다. 디지털 포렌식 프로세스의 통합적 요구사항으로서 디지털 포렌식 분석실에 대한 인증의 확보

마지막으로 디지털 포렌식 프로세스의 통합에 있어서 궁극적으로 확보되어야 하는 것은 디지털 포렌식 분석실 자체에 대한 인증 확보의 문제라고 할 수 있다. 이는 앞에서 기술한 디지털 포렌식 절차별 요구사항 - 절차적 연계성, 도구, 분석관 -을 모두 포괄하는 문제라고도 할 수 있다. 즉, 디지털 포렌식 분석실 자체에 대한 국제적 표준에 따른 인증을 확보하게 되면 절차적·도구적·인적 신뢰성도 함께 인증되는 것이고, 디지털 포렌식 업무품질 자체에 대한 신뢰성을 인정받는 것이기 때문에 가장 기본적이고 중요하지만 가장 어려운 문제라고도 할 수 있다.

현재 디지털 포렌식 분석실에 대한 국제적인 표준적 요구사항에 따른 인증과 관련된 기준으로는 ISO/IEC 17025가 있는데, 이는 안전하고 신뢰성 있는 측정 장비를 갖추고 있다는 전제하에서 조직 및 관리시스템에 관련한 경영적 요구사항과 직원·시설·품질보증·결과보고 등에 관한 기술적 요구사항 등으로 구성되어 있다. 앞의 제3장에서 기술한 바와 같이 미국과 영국, 그리고 EU 산하의 디지털 포렌식 업무를 수행하는 기관들은 디지털 포렌식 업무의 신뢰성 확보에 있어서 가장 중요한 것이 이와 같은 국제적인 인증을 확보하는 것이라는 인식을 갖고 있고, 따라서 ISO/IEC 17025에 의한 인증을 확보하였거나 확보하기 위한 노력을 기울이고 있는 것을 볼 수 있다.

이와 같은 디지털 포렌식 분석실에 대한 ISO/IEC 17025의 인증이 요구되는 것은 포렌식 서비스 제공자로서 포렌식 분석실에 의해 유지되는 가능한 한 최고의 표준들을 통해 포렌식 과학에 있어서의 품질표준을 보장하고자 하는데 있다고 할 수 있다. 즉 포렌식 과학에 있어서 품질표준은 국제적 표준인 ISO/IEC 17025에 의한 인증을 통해 가장 잘 확보될 수 있다고 보고 있는 것이다.[602]

우리나라의 경우 KOLAS(Korea Laboratory Accreditation Scheme)에서 ISO/IEC 17025에 의거하여 인증을 하고 있지만 현재까지는 전통적인 법과학 분야로 한정되어 있으며, 국내 환경에 적합한 디지털 포렌식에 관한 검증제도나 수준 평가방법 및 기준에 대한 연구도 현저히 부족한 상황이라 할 수 있다.[603] 따라서 현재 국내에서

602) David Watson/Andre Johes, Digital Forensics Processing and Procedures - Meeting the Requirements of ISO 17020, ISO 17025, ISO 27001 and Best Practice Requirements, 2013, p.29.

운용되는 디지털 포렌식 분석실 가운데 ISO/IEC 17025에 의한 인증을 받은 곳은 없는 상태이지만 기관별로 인증을 위한 노력은 기울이고 있다.

제2절 디지털 포렌식 프로세스 구축을 위한 국제적 표준 요건의 충족

1. 디지털 포렌식 프로세스에 대한 인증의 필요성

디지털 포렌식 프로세스에 대한 신뢰성을 확보하기 위해서는 포렌식 분석관의 전문성, 분석도구의 정확성, 분석실의 신뢰성, 통합 관리 및 통제를 위한 표준절차 준수 등 4가지 요구사항에 대한 인증제도의 필요성이 고려될 수 있다.[604]

디지털 포렌식 분야에 있어서 전문가 자격 공인과 관련해서는 미국 국립법과학센터의 디지털 포렌식 자격 위원회(Digital Forensic Certification Board)에 의한 인증이 있다. DFCB는 디지털 포렌식 전문직에 있어서의 공적인 신뢰와 신용을 촉진하기 위하여 존재하는 기관이며, 그에 의한 인증은 승인된 표준에 따라 직무를 수행함에 있어서 그 분야의 전문가들에 의해 확립된 명시적인 기준을 충족할 수 있는 능력의 레벨을 나타내는 것이라고 설명하고 있다.[605] DFCB는 미국내 전문가에 대한 표준을 설정하는 주요기관인 NCCA(National Commission of Certifying Agencies)에 의해 인증된 국가표준을 준수[606]하는 포렌식 전문가 인증위원회(Forensic Specialties Accreditation Board)[607]의 인증획득을 검토중에 있다고 한다.[608]

---

603) 박희일/윤종성/이상진, "디지털 포렌식 수준 평가지표 개발에 관한 연구", 정보보호학회논문지, 2015, 1154면.

604) 김기범/장기식/장윤식/이상진/임종인, "디지털 포렌식 전문가 자격모델 개발", 디지털 포렌식 연구 제3호, 2008, 32면.

605) http://www.dfcb.org/about.html; 2016.10.5.

606) http://thefsab.org/; 2016.10.5.

607) 포렌식전문가 인증위원회의 인증프로그램은포렌식 공동체에 의해 포렌식 과학자 또는 포렌식 전문가를 인증하는 기관이나 전문가 위원회를 평가, 승인, 관리할 수 있는 메카니즘을 확립하고자 하는 것으로, AAFS(American Academy of Forensic Science)·NFSTC(National Forensic Science Technology Center), NIJ(National Institute of Justice)의 지원으로 만들어졌으며, 인증 표준(Standards for Accrediting Forensic Specialty Certification Boards)을 제시하고 있다.; http://thefsab.org/files/standards_20110220.pdf; 2016.10.5.

분석도구에 대한 검증과 관련하여서 가장 공신력있는 것은 미국 국가표준기술연구소(National Institute of Standards and Technology)의 컴퓨터 포렌식 도구 평가프로젝트(Computer Forensics Tool Testing)이다. CFTT에서는 디지털 포렌식 도구가 정확한 결과를 도출하는지 여부를 확인하는 기술적 평가를 수행하고 있으며, CFTT 평가 방법 자체가 디지털 포렌식 도구가 갖추어야 할 기본적인 준수사항으로 받아들여짐으로써 국제표준과 다름없이 받아들여지고 있다.[609] 한편, 소프트웨어 품질 평가를 위한 국제표준모델인 ISO/IEC 9126이 디지털 포렌식 도구 품질평가 기준으로 제시되고 있기도 하다.[610]

디지털 포렌식 분석실에 대한 인증과 관련하여서는 국제표준인 ISO/IEC 17025과 ASCLD/LAB의 인증프로그램이 있다. 미국, 영국, EU 산하의 디지털 포렌식 분석실의 경우 ISO/IEC 17025에 따른 인증 뿐만 아니라 ISO/IEC 27001, 27020에 따른 인증을 확보하였거나 확보하고자 노력하고 있는 것으로 나타나고 있다. 여기에서 인증이란 인정 내지 승인을 받은 기관이 개인 또는 조직, 제품 또는 서비스, 절차 또는 공정, 사건 또는 상황 등의 속성, 특징, 품질, 자격 또는 상태 등이 기준에 부합하는지 여부를 평가하고 검증하는 공식절차를 말한다.[611]

마지막으로 통합관리 및 통제를 위한 표준절차 준수에 있어서는 미국, 영국, EU에서 이미 구체적인 표준실무지침 또는 모범실무지침 등이 마련되어 시행되고 있다. 특히 영국의 경우 법과학 서비스 제공이 과학적 품질 표준체계하에서 이루어질 수 있도록 법과학 규제기관을 두고 있을 뿐만 아니라, 디지털 포렌식 프로세스 및 그 프로세스내에서 행해지는 모든 활동들에 품질관리시스템(Qualtiy Management System)과 통합관리시스템(Integrated Management System)을 적용하고 있다.[612]

이하에서는 이와 같이 디지털 포렌식 프로세스에 적용되고 있는 공신력 있는 기관

608) 임종인, 경찰의 차세대 디지털 포렌식 기반구축방안, 2008, 71면.
609) 탁희성/이상진, 디지털 증거분석도구에 의한 증거수집 절차 및 증거능력 확보방안, 2006, 131-132면.
610) 이동윤, 디지털 포렌식 도구를 위한 ISO/IEC 9126 기반의 품질평가모델, 숭실대 석사논문, 2014. 참고.
611) David Watson/Andre Johes, p.796.
612) David Watson/Andrew Jones, Digital Forensics Processing and Procedures; Meetings the Requirements of ISO 17020, ISO17025, ISO27001 and Best Practice Requirment, 2013, 181면.

에 의한 표준 또는 국제 표준의 내용을 간략히 검토하고자 한다.

2. 디지털 포렌식 전문가 자격 인증을 위한 표준

가. 포렌식 전문가 인증위원회 표준(Standards for Accrediting Forensic Specialty Certification Boards)[613]

1) 개요

이 표준은 법과학 전문가 인증위원회가 포렌식 과학 또는 기타 포렌식 전문분야에서 활동하고 있는 사람들을 인증하기 위한 프로그램을 승인함에 있어서 적용하는 것이다. 여기에 포함된 표준들은 지식, 기술, 능력을 평가, 기록, 유지하는 절차만을 다루고 있다.[614]

2) 인증 기구

인증 기구는 합법적으로 인정될 수 있는 단체 또는 그 단체의 일부이어야 하고, 인증과 관련한 모든 문제에 대해 독립적이고 공정해야만 한다. 인증 기구는 이해관계 당사자들에게 그 능력과 공정성, 무결성에 있어서 신뢰를 제공할 수 있도록 조직되어야 하며, 모든 훈련이나 관련 활동들이 인증 프로그램의 신뢰성, 객관성 및 공정성을 훼손하지 않도록 해야만 한다.[615]

인증 기구가 그 프로그램 시행을 위해 마련한 정책과 절차 매뉴얼은 공정하고, 객관적이며 비차별적이어야 하며, 연방과 주법을 준수해야 한다. 그리고 인증 프로그램의 범위를 명확히 정의해야 하며 웹사이트를 통해 일반이 활용할 수 있도록 해야 한다.[616]

3) 인증 표준

인증 표준과 관련해서는 자격 인정, 전문가 개발 또는 훈련 요건, 자격과 시험,

---

613) Forensic Specialties Accreditation Board, Inc., Forensic Specialties Accreditation Board, Inc., 2011.
614) Forensic Specialties Accreditation Board, Inc., op.cit., p.3.
615) Forensic Specialties Accreditation Board, Inc., .op.cit., p.4.
616) Forensic Specialties Accreditation Board, Inc., .op.cit., p.5.

윤리표준과 전문가 표준이 기술되어 있다. 먼저 자격 인정과 관련해서는 신청자의 "학교 교육 또는 그에 상당하는 훈련, 관련 전문가로서의 경험 또는 채용, 특정한 분야에 요구되는 능력에 이르는 충분한 훈련, 관련 전문 라이센스, 증명서 또는 등록"에 대한 평가와 검증을 요구하고 있다.[617]

다음으로 포렌식 전문분야에 있어서 최초의 전문성 개발 또는 훈련을 위한 일반요건으로는 우선 훈련의 내용과 범위, 훈련받은 사람에 대한 평가와 결과물에 대한 기록을 작성해야만 하며, 포렌식 전문분야에서 요구되는 지식과 자격은 수업과정, 워크숍, 훈련과정 등의 복합적 방법을 통해 확보되어질 것을 요구하고 있다. 또한 인증을 신청한 사람에 대한 교육은 광범위한 동료심사를 요하는 공식적인 훈련 프로그램을 포함해야 한다.[618]

자격과 관련해서는 최소한 관련 분야의 구체적인 지식, 기술, 그리고 능력에 대한 신뢰할 수 있고 유효한 시험을 통해 그 자격이 평가되어야 하며, 모든 테스팅 절차는 인증프로그램의 범위에 의해 포함되는 포렌식 전문분야 내에서의 최근의 표준을 반영한 것이어야 하고 공정하고 정확해야 한다고 기술하고 있다.[619] 자격에 대한 평가는 능력시험, 사례검사, 법정증언에 대한 검사, 사건 프리젠테이션, 평가 또는 이러한 방법들을 적절히 조합한 방식으로 할 수 있다.

마지막으로 인증절차는 인증을 신청한 사람은 인증 기구에 의해 인정된 윤리표준과 전문가 표준을 준수한다는 것을 서면으로 동의하도록 요구해야 한다.

4) 재인증

재인증은 지속적인 전문성 개발, 업무 경험 그리고 윤리표준과 전문가 표준에의 재확인에 대한 성공적인 입증을 요한다. 지속적인 전문성 개발에 대한 측정은 훈련과정 또는 워크숍, 컨퍼런스 참석, 관련 출간물의 작성 또는 리뷰, 훈련 진행, 사건 준비와 관련 업무경험 등에 의해 행해질 수 있다. 또한 재인증을 위해서는 지속적인 관련 업무경험에 대한 기록이 요구되며, 윤리표준과 전문가 표준을 계속 준수할 것이라는 것을 서면으로 재확인해야 한다.[620]

---

617) Forensic Specialties Accreditation Board, Inc., .op.cit., pp.7-8.
618) Forensic Specialties Accreditation Board, Inc., .op.cit., p.8.
619) Forensic Specialties Accreditation Board, Inc., .op.cit., p.9.

5) 최초의 인증을 위한 심사

심사는 유효하고 신뢰할 수 있는 방식으로 인증 신청자의 지식·기술·능력을 평가하도록 설계되어야 하고, 목표한 포렌식 전문분야 내에서의 능숙한 업무를 위해 요구되는 지식과 기술·능력을 포함해야 한다. 심사에 떨어진 경우에는 즉시 재심사 받을 수 없으며, 재심사할 수 있는 최소한도의 의무적 대기 기간이 60일 미만이 되어서는 안도록 해야 한다고 기술하고 있다.[621]

나. 디지털 포렌식 자격 위원회(DFCB)의 인증 자격[622]

DFCB는 2006년에 민간기업, 정부, NCFC와 합의한 전문가 자격 모델을 개발했는데, 여기에서 DFCB는 디지털 포렌식에 있어서의 자격을 판단함에 있어서 4가지 핵심적인 역량을 제시하고 있다. 기반기술, 증거획득, 검사, 분석이 그것이다.

기반기술(Foundation Skills)에 있어서는 품질보증, 법과 윤리, 법률상 권한, 기술, 프로세스, 개념 등의 항목으로 구성되어 있으며, 증거획득(Acquisition)에 있어서는 프로세스, 증거식별, 획득 계획, 법률상 권한, 획득 기술 등의 항목으로 구성되어 있다. 조사(Examination)에 있어서는 네트워킹과 통신·특별한 형태의 데이터·조사 기법·컴퓨터와 데이터 개념·하드웨어·조사 프로세스 등의 항목이 기술되어 있으며, 마지막 분석(analysis)에 있어서는 법률과 절차·기록·분석 기법·기술 등의 항목으로 기술되어 있다.[623]

3. 디지털 포렌식 도구에 대한 검증 기준

디지털 포렌식 분야에 있어서 활용되고 있는 도구는 이미 상당부분 상용화되어 있지만, 이 분야의 기술변화가 워낙 빠르기 때문에 새로운 도구 개발의 필요성이 지속적으로 요구되고 있다. 따라서 현장조사에 신속하게 대응하기 위해서 수사기관 자체내에 개발 부서를 두거나 외부업체에 개발을 맡기기도 하기 때문에 기관 자체

620) Forensic Specialties Accreditation Board, Inc., .op.cit.,p.10.
621) Forensic Specialties Accreditation Board, Inc., .op.cit.,p.11.
622) http://www.dfcb.org/New_DFCB_Site/certification.html; 2016.10.5.
623) http://www.dfcb.org/New_DFCB_Site/certification.html; 2016.10.5.

개발한 도구를 사용하는 비율도 점차 늘어나고 있다.

이와 같이 디지털 포렌식 도구의 발전과 변화가 빠르기 때문에 사용하고 있는 도구가 신뢰할 수 있는 것인지에 대한 검증을 하는 것이 용이하지는 않다. 그럼에도 불구하고 신뢰성 있는 도구에 기반하지 않은 채 산출된 결과는 법적 판단의 근거로서 허용될 수 없기 때문에 도구 자체의 신뢰성에 대한 검증은 필수적이라 할 것이다. 현재 몇몇을 제외한 대부분의 디지털 포렌식 도구들은 신뢰성을 명확하게 검증받지 못한 상황하에서 활용되고 있기 때문에, 분석관들이 도구에 대한 신뢰성을 가지고 사용할 수 있도록 객관적인 검증방법이 필요하다[624]고 할 것이다.

일반적으로 디지털 포렌식 도구의 신뢰성은 시험을 거쳐 그 적격성이 확인되고, 검증과 확인이 이루어져야만 하지만,[625] 현재로서는 포렌식 도구의 적격성을 심사할 수 있는 인증시스템이 갖추어져 있지는 않다. 다만 앞서 기술한 바와 같이 미국 국립표준기술연구소가 CFTT 프로젝트에 의해 디지털 포렌식 도구 개발단계 또는 개발된 도구에 대한 검증시에 활용할 수 있는 기능별 요구사항이 담긴 정의서와 기술적 사양에 대한 명세서를 문서로 제시함으로써, 원본 증거의 훼손방지, 정확한 디지털 증거 수집, 무결성 확보 및 검증기능 보장에 기여하고 있다[626]

미국 국립표준기술연구소가 디지털 포렌식 도구에 대한 검증과 관련하여 진행하는 또 하나의 프로젝트는 Computer Forensic Reference Data set(CFReDS) 프로젝트이다. 이 프로젝트는 컴퓨터 포렌식용 이미지 파일과 모바일 이미지 파일 등을 제공하여 교육과 도구성능 및 검증평가를 위해 사용하고 있다.[627]

가. CFTT 프로젝트

CFTT는 디지털 포렌식 도구의 신뢰성 확보를 위한 원본 디지털 증거의 훼손 방지· 정확한 디지털 증거 수집· 무결성 확보 및 검증 기능을 보장하기 위해 디지털 포렌식에 사용되는 도구의 요구사항을 정의하고, 각 도구들을 검증하는 방법 및 절차를

624) 최재민/오정훈/이상진, “국내환경에 적합한 컴퓨터 포렌식 도구 검증용 이미지 구성방안 연구”, 디지털 포렌식 연구 제7호, 2010, 68면.
625) 임종인, 경찰의 차세대 디지털 포렌식 기반 구축방안, 2008, p.73.
626) 최재민/오정훈/이상진, 앞의 논문, 69면. 70면.
627) 최재민/오정훈/이상진, 앞의 논문, 69면.

확립하여 디지털 포렌식 도구의 테스트 베드를 구축하는 것을 주목적으로 하고 있다.[628]

CFTT 테스트 대상이 되는 디지털 포렌식 도구의 유형은 Disk Imaging, Forensic Media Preparation, Write block(hardware), Write block(software), Deleted File Recovery, Mobile Devices, Forensic File Carving, String Search 이며, 이러한 유형의 디지털 포렌식 도구를 대상으로 한 평가명세서는 2016년 현재 155개가 공개되어 있다.[629]

CFTT가 디지털 포렌식 도구를 테스팅하는 접근방법은 적합성 시험과 품질시험을 위하여 널리 승인된 국제적인 방법론에 기반을 두고 있으며,[630] 특히 다양한 기능과 특징을 가지고 있는 디지털 포렌식 도구에 대한 테스트 기능 기반의 접근을 통해 증거수집, 검색, 복구 등의 각 기능별로 일련의 테스트를 수행하고 있는 것이 특징이다.[631] CFTT 디지털 포렌식 도구 검증 제도는 특정한 빌드 환경과 버전에서만 그 신뢰성을 인정하기 때문에, 이미 검증된 도구라 해도 새로운 버전이 만들어지거나 업그레이드가 이루어진 경우에는 다시 도구 검증 프로세스를 거쳐야 한다.[632]

나. CFReDS 프로젝트

CFReDS는 수사를 지원하기 위해 가상의 디지털 증거 데이터 셋을 조사관들에게 제공하는 것을 목적으로 한다.[633] 이 프로젝트를 통해 배포되는 이미지들을 이용하여 컴퓨터 포렌식 도구의 검증, 장비 점검, 조사관 훈련, 조사관 숙련도 테스트 등을 할 수 있다.[634]

CFReDS 사이트를 통해 15가지의 데이터 셋을 제공하고 있는데 이는 지속적으로 업데이트 되고 있음을 볼 수 있다. 15가지 데이터 셋은 다음과 같다. Hacking Case, Data Leakage Case, Russian Tea Room, asb image, dd, E01, Create a reference

628) 최재민/오정훈/이상진, 앞의 논문, 70면.
629) http://www.cftt.nist.gov/index.html; 2016.10.10.
630) http://www.cftt.nist.gov/Methodology_Overview.htm; 2016.10.10.
631) 최재민/오정훈/이상진, 앞의 논문, 72면.
632) 최재민/오정훈/이상진, 앞의 논문, 72면.
633) http://www.cfreds.nist.gov/; 2016.10.10.
634) http://www.cfreds.nist.gov/; 2016.10.10.최재민/오정훈/이상진, 앞의 논문, 72면.

drive, Basic Mac image, Rhino Hunt, Memory Images, DCFL, Mobile Device Image, Container Files, Deleted File Recovery, File Carving, File Carving CFTT Images, String Search (CFTT) 등이 제공되고 있고, 각각의 데이터 셋에 대한 설명이 간략하게 기술되어 있다.[635]

4. 디지털 포렌식 분석실 인증 표준

거의 모든 포렌식 기관들은 적절한 업무 방식을 확립하고, 높은 품질의 서비스를 제공하고자 노력하는데, 이를 위해 포렌식 기관에 적용가능한 인증 요구사항을 해당 기관의 통합관리시스템에 적용하고 있다.[636] 따라서 디지털 포렌식 분석실들도 국제표준인 ISO 인증을 획득함으로 디지털 포렌식 프로세스의 신뢰성을 확보하고자 하는 것이 일반적인 경향이라 할 수 있다.

디지털 포렌식 분석실 인증과 관련하여 일반적으로 적용되는 대표적인 국제표준은 ISO 17025와 ISO 9001, ISO 27001 등이 있는데, 이 가운데 ISO 17025는 ISO 9001준수를 전제로 하고 있다. 하지만 ISO 17025 인증을 바탕으로 ISO 9001에 의한 인증을 주장할 수 없고, ISO 9001 인증 획득으로 ISO 17025 인증이 자동 부여되는 것은 아니다.[637]

ISO 17025는 ISO 9001에서 다루지 않는 기술적 자격 요건을 다루고 있으며, ISO 9001에 대한 인증 그 자체로 법과학 기관이 유효한 데이터 및 결과를 생산할 자격이 있음을 입증해주는 것은 아니라는 점에서 양자는 차이가 있다. 따라서 법과학 기관은 ISO 17025와 ISO 9001에 대한 인증 둘다를 획득해야 한다.[638]

이러한 국제표준에 따라 포렌식 기관이 인증을 받게 되면 다음과 같은 장점이 있다.[639]

"ⅰ) 법과학 기관내 직원에 대한 자격이 인정된다

635) http://www.cfreds.nist.gov/; 2016.10.10.
636) David Watson/Andrew Jones, op.cit., p.78.
637) David Watson/Andrew Jones, Digital Forensics Processing and Procedure, 2013, p.798.
638) ibid.
639) David Watson/Andrew Jones, op.cit., pp.798-799.

ii) 절차 및 결과물의 정확성 및 무결성이 보장된다.
iii) 제3자에 대하여 관련규정 준수를 입증할 수 있다.
vi) 기관이 발행한 보고서에 대한 신뢰가 높아진다.
v) 법과학 기관이 국제적으로 인정을 받는다
iv) 법과학기관의 운영에 관한 프로세스와 절차가 문서화되고 검증된다.
vii) 엄격한 품질관리절차에 의하여 오류 및 결함이 감소된다.
viii) 업무 재수행이 감소하거나 없어짐으로써 시간과 비용이 절약된다.
ix) 시험장비의 적합성, 교정 및 유지관리가 가능해진다.
x) 법과학 기관이 유효한 품질보증시스템을 가지고 있으며, 기술적으로 자격이 있는 것으로 평가되는가의 여부를 확인할 수 있는 피드백과 운영능력을 갖게 된다."[640]

즉 이와 같이 디지털 포렌식 기관의 절차, 직원, 도구, 보고서 등 전체 프로세스에 대한 신뢰를 확보할 수 있다는 점에서 ISO 인증의 필요성과 중요성은 강조될 수 밖에 없다.

가. ISO/IEC 17025

ISO/IEC 17025은 국제표준화 기구에 의해 제정된 시험/교정기관의 자격에 관한 일반적 요구사항의 국제표준이자 인증기준이다.[641] 따라서 이 국제표준은 각 시험/교정기관이 관리시스템의 운영, 기술적 자격, 기술적으로 유효한 결과를 산출할 능력을 입증하기 위해 충족해야 할 요구사항을 포함하고 있다. 본 국제표준을 준수하는 시험/교정기관은 ISO 9001을 준수해야 하며, 따라서 본 국제표준의 요구사항을 준수하는 경우에는 해당 기관의 시험/교정활동 품질관리시스템의 운영이 ISO 9001상의 원칙 또한 충족하는 것이 된다.[642]

ISO/IEC 17025의 적용범위는 관리요건과 기술요건으로 구분되어 있다.

---

640) ibid.
641) 박희일/윤종성/이상진, 디지털 포렌식 수준평가지표 개발에 관한 연구, 정보보호학회논문지, 2015, 1154면.
642) ISO/IEC, International Standard ISO/IEC 17025; General requirements for the competence of testing and calibration laboratories, 2005, p.1.

1) 관리요건

가) 실험실의 준수 의무사항

"a) 관리체계의 시행, 유지관리 및 개선 등의 업무를 수행하고, 관리체계 또는 시험/교정 수행절차 위반사례를 파악하고, 위반방지 및 최소화를 위한 조치를 개시하는데 필요한 권한 및 자원을 지닌 관리직원과 기술직원을 마련해야 한다.

b) 경영진 및 기타 직원이 업무의 품질에 부정적 영향을 미칠 수 있는 내외부의 상업적 재정적 압력 및 기타 압력으로부터 자유로울 수 있도록 하는 제도를 시행해야 한다.

c) 결과의 전자적 저장 및 전송에 대한 보호절차를 포함하여 고객의 비밀정보 및 보유권리를 보호하기 위한 방침 및 절차를 마련해야 한다

d) 기관의 자격, 공정성, 판단 또는 업무의 순수성에 대한 신뢰를 저해할 수 있는 활동에 관여하지 않도록 하는 방침 및 절차를 마련해야 한다

e) 해당 기관의 조직 및 관리구조, 특허 관련 기구내에서의 위치, 품질관리, 기술업무 및 지원 서비스 사이의 관계를 정의해야 한다

f) 시험/교정의 품질에 영향을 미치는 업무를 관리·수행 또는 검증하는 모든 인원의 책임, 권한 및 상호관계를 정해야 한다.

g) 시험/교정의 방법·절차·목적을 잘 알고 있고, 시험/교정의 결과에 대한 평가에 숙련된 직원이 시험/교정 직원, 피훈련자를 적절히 감독하도록 해야 한다.

h) 실험실 운영에 있어서 요구되는 품질을 확보하는데 필요한 자원의 제공과 기술적 운영에 전반적 책임을 지는 기술 관리가 있어야 한다.

I) 직원 중 1인을 품질관리자로 임명하고, 해당 품질관리자는 기타 의무 및 책임과 별도로 품질 관련 관리시스템을 항상 시행하고 준수하도록 할 책임과 권한을 보유하도록 해야 한다.

j) 핵심관리직 인원 아래 부관리자를 임명해야 한다

k) 기관의 각 직원은 자신의 활동이 지니는 의미와 중요성을 인식하고, 해당 기관의 관리체계의 목적 달성에 기여하는 바를 인식해야 한다."[643]

643) ISO/IEC, International Standard ISO/IEC 17025, op.cit., pp.2-3.

나) 관리 시스템

시험/교정기관은 해당 기관의 활동범위에 적합한 관리시스템을 시행, 유지해야 하며, 결과의 품질을 확보하는데 필요한 수준의 정책, 시스템, 프로그램, 절차, 지시사항을 문서화해야 한다. 품질정책 기술서에는 모범적 직무수행 및 고객을 위한 시험/교정 품질 확보의무 준수, 실험실의 서비스 표준 명시, 품질관련 관리시스템의 목적, 기관내 직원들의 품질문서의 숙지 및 해당 업무 방침 및 절차 시행 요건, 본 국제표준 준수와 기관의 관리시스템 효과성 지속 및 제고의무 준수 등이 포함되어야 한다.[644]

다) 문서 통제

시험/교정 기관은 관리체계에 속하는 모든 문서에 대한 관리절차를 수립하고 유지해야 하며, 각 문서를 정기적으로 검토하고, 필요에 따라 개정하여 해당 요구사항에 대한 적합성을 유지하고 준수할 수 있도록 해야 한다.[645]

라) 부적합 시험/교정 업무 관리

시험/교정기관은 시험/교정 업무 또는 해당 업무의 결과가 기관 자체의 절차 또는 고객과 합의한 요구사항에 적합하지 않을 경우, a) 부적합 업무에 대한 관리책임 및 권한을 부여하고 부적합 업무 파악시 조치를 정하고 수행한다, b) 부적합 업무의 중대성에 대한 평가를 실시한다, c) 문제를 즉시 시정하고 동시에 부적합 업무에 대한 용인가능성을 결정한다, d) 필요시 고객에게 해당 사항을 통보하고 해당 업무에 대한 리콜을 실시한다.[646]

마) 재발방지 및 예방 조치

시험/교정기관은 부적합 업무 또는 관리시스템의 방침/절차 위반 또는 기술 업무 방침/절차 위반이 확인되었을 경우 취할 재발방지조치에 관하여 절차 및 방침을 수립해야 한다. 재발방지조치는 해당 문제의 규모 및 위험성에 비례하는 조치여야 한다. 예방을 위해서는 기술적 사항 또는 관리체계 관련사항을 불문하고 개선이 필요한 사항 및 부적합의 잠재적 원인을 파악해야 한다.[647]

---

644) ISO/IEC, International Standard ISO/IEC 17025, op.cit., pp.3-4.
645) ISO/IEC, International Standard ISO/IEC 17025, op.cit., p.4
646) ISO/IEC, International Standard ISO/IEC 17025, op.cit., p.7.
647) ISO/IEC, International Standard ISO/IEC 17025, op.cit., p.8.

바) 기록 관리

교정/시험 기관은 품질기록 및 기술 기록의 확인·수집·색인·접근·제출·보관·유지 및 처분에 대한 절차를 수립하고 유지해야 하며, 모든 기록은 파손·품질저하 및 손실을 방지할 수 있는 적합한 환경이 있는 시설에 보관해야 한다. 기록 보관시 보안 및 기밀을 유지해야 하고, 전자적으로 저장된 기록에 대한 보호 및 백업절차 마련, 기록에 대한 무단접근 또는 수정방지 절차를 마련해야 한다.[648]

기록에 오류가 있을 경우, 오류 부분을 판독 불가능하게 만들거나 완전 삭제하는 대신 삭선을 그어 표시하고 정확한 내용을 같이 기입해야 하며, 오류내용 정정시 정정한 사람의 서명을 기입해야 한다.

2) 기술요건

가) 일반 사항

실험실에 의해 수행되는 시험/교정의 정확성과 신뢰성을 판단하는 요소로는 인적 요소, 시설 및 환경 조건, 시험/교정 방법 및 방법 검증, 장비, 측정 추적관리, 샘플, 시험/교정 항목의 취급 등이 있다.

나) 인사

시험/교정기관의 경영진은 각 장비운용 직원, 시험/교정 수행 직원, 결과 평가 직원, 시험보고서/교정인증서에 대한 서명권자 등이 충분한 자격을 갖추도록 해야 한다. 각 업무를 수행하는 직원에 대해서는 해당 업무에 필요한 교육, 훈련, 경험 또는 능력에 기초하여 그 자격을 부여해야 한다.[649]

기관은 직원에게 필요한 훈련을 제공하기 위한 방침과 절차를 마련해야 하며, 훈련 프로그램은 업무와 관련성이 있어야 하고 그 효과성을 평가해야 한다. 또한 직원의 권한, 자격, 교육 및 전문 자격, 훈련, 능력 및 경험과 관련된 기록을 유지해야 한다.[650]

일부 기술적 영역의 업무를 수행해야 하는 직원은 개인 인증이 요구되는데, 이 경우 개인인증 요구사항은 관련 규정이나 해당 기술분야의 표준 또는 고객의 요구사

---

648) ISO/IEC, International Standard ISO/IEC 17025, op.cit., p.9.
649) ISO/IEC, International Standard ISO/IEC 17025, op.cit., p.11.
650) ISO/IEC, International Standard ISO/IEC 17025, op.cit., p.12.

항에 근거한다. 그리고 시험보고서에 기재하는 의견 및 해석을 작성하는 직원은 해당 시험수행에 필요한 자격·훈련·경험 및 지식 뿐만 아니라, 시험대상 품목이나 제조기술 관련 지식, 관련 입법 및 표준에 명시된 일반적 요구사항, 시험대상 품목이나 제품 등의 정상적 사용과 관련하여 발견된 편차의 중요성에 대한 이해를 갖추어야 한다.[651]

다) 시설 및 환경 조건

실험실은 환경조건에 의하여 시험/교정 결과가 무효로 되거나 측정 품질에 부정적 영향을 미치는 일이 없도록 해야 하며, 시험/교정 결과에 영향을 미칠 수 있는 시설 및 환경조건 관련 요구사항에 대한 기록을 작성해야 한다.[652] 또한 실험실은 시험/교정 방법 및 절차에서 요구하는 환경 조건 또는 결과의 품질에 영향을 미치는 환경조건에 대한 모니터링, 관리 및 기록을 실시해야 하며, 환경조건으로 인하여 시험/교정 결과에 위험이 발생할 경우에는 시험/교정을 중단해야 한다.[653]

라) 시험/교정 방법과 방법 검증

(1) 시험/교정 방법

실험실은 업무 범위에 포함되는 모든 시험/교정에 관하여 적절한 방법과 절차를 사용해야 하며, 방법과 절차에는 대상 품목의 시료 선정·취급·운송·보관 및 준비 그리고 시험/교정 데이터의 통계분석 및 측정의 부정확성에 대한 추정이 포함되어야 한다.[654]

기관의 업무 관련 지침·표준·매뉴얼 및 참고자료는 최신 버전으로 유지해야 하고, 각 직원이 용이하게 확인할 수 있도록 제공해야 한다. 정해진 시험/교정 방법에서 벗어난 방법을 사용하기 위해서는 그에 대한 기록과 기술적 근거 그리고 승인이 있어야 한다.[655]

실험실은 고객의 요구와 해당 시험/교정에 적합한 방법을 활용해야 하며, 이 경우 국제, 지역, 국가 표준에서 정한 방법을 사용하는 것이 바람직하다. 고객이 시험/교정 방법을 지정하지 않은 경우, 기관은 국제·지역·국가 표준에서 정한 적절한 방법 또는

651) ISO/IEC, International Standard ISO/IEC 17025, op.cit., p.11.
652) ISO/IEC, International Standard ISO/IEC 17025, op.cit., p.12.
653) ibid.
654) ibid.
655) ibid.

저명한 기술기구가 정한 방법, 관련 과학논문 또는 학술지에 수록된 방법, 장비 제조사가 정한 적절한 방법을 선택해야 한다. 만약 기관에서 자체 개발하거나 도입한 방법은 그것이 사용목적에 적합한 것이고, 검증을 거친 것이라면 사용할 수 있다.[656]

표준방법에 해당하지 않는 방법을 사용할 필요가 있는 경우에는 고객과 합의하에 해당 방법을 사용해야 하며, 이러한 비표준 방법을 사용하기 전에 적절한 검증을 거쳐야 한다. 그리고 신규 시험/교정 방법은 시험/교정 실시 전에 해당 절차를 개발해야 하고, 그 절차 안에는 적절한 식별정보, 범위, 대상품목 설명, 측정 대상의 한도·수량·범위, 기술성능 요구사항을 포함한 기구 및 장비내역, 합격/불합격 기준 및 요건, 기록대상 데이터 및 분석/결과 제시방법, 부정확성 또는 부정확성 추정 절차 등이 포함되어야 한다.[657]

(2) 방법 검증과 측정의 부정확성 추정

실험실은 비표준 방법, 기관이 설계 및 개발한 방법, 의도된 사용 범위 밖에서 사용하는 표준방법, 표준 방법에 대한 확대 및 수정 사항 등을 검증하여 해당 방법이 의도된 목적에 적합함을 확인해야 한다. 검증은 해당 방법이 적용된 목적 또는 분야의 요구사항을 충족하는데 필요한 범위에서 실시한다.[658]

검증된 방법으로부터 획득할 수 있는 수치의 범위 및 정확성(예: 결과의 부정확성, 검출 한계, 방법의 선정, 선형성, 반복가능성/재현가능성의 한계, 샘플/시험 대상의 매트릭스로부터의 간섭에 대한 교차민감성 및 외부 영향에 대한 견고성)은 고객의 요구사항과 관련성을 갖추어야 한다.[659]

실험실은 측정의 부정확성 추정 절차를 보유하고 적용해야 하며, 합리적 추정은 시험방법의 성능 및 측정 범위에 대한 지식을 기초로 도출해야 한다.[660]

(3) 데이터 관리

시험/교정 데이터의 획득·처리·기록·보고·저장 또는 검색에 컴퓨터 또는 자동화된 장비를 사용하는 경우, 실험실은 다음 사항을 준수해야 한다.[661]

---

656) ISO/IEC, International Standard ISO/IEC 17025, op.cit., p.13.
657) ibid.
658) ISO/IEC, International Standard ISO/IEC 17025, op.cit., p.14.
659) ibid.
660) ibid.

"a) 사용자가 개발한 컴퓨터 소프트웨어를 충분한 수준으로 자세히 기록하고, 사용 목적에 대한 적합성을 충분히 검증해야 한다
b) 데이터 보호절차를 수립 및 시행해야 하며, 그 절차에는 데이터 입력 또는 수집·저장·전송 및 처리의 무결성 및 기밀성 등이 포함되어야 한다.
c) 컴퓨터 및 자동 장비가 본래 기능을 유지하도록 관리하고, 시험/교정 데이터 유지관리에 필요한 환경 및 운용조건을 마련한다."[662]

(4) 장비

시험·교정 및 시료 선정에 쓰이는 장비 및 소프트웨어는 필요한 수준의 정확도를 달성할 수 있어야 하며, 해당 시험/교정에 적용되는 규격을 준수해야 한다. 장비를 실제 업무에 투입하기 전에 교정 및 점검하여 해당 장비가 기관의 요구사항을 충족하며 관련 표준규격을 준수함을 확인해야 한다.[663]

시험/교정에 있어서 중요한 장비 및 소프트웨어 각각에 대한 기록을 유지해야 하며, 측정장비의 안전한 취급·운송·보관·사용 및 유지관리절차를 마련하여 본래기능을 유지하고 오염 및 노후화를 방지해야 한다.[664] 따라서 업무량이 과도했거나 잘못 취급한 장비, 오류 의심이 있는 결과를 제시하는 장비, 결함이 있는 것으로 파악되거나 정해진 한계 밖의 결과를 나타내는 장비는 사용을 중단해야 한다.[665]

(5) 시험/교정 결과의 품질 확보

실험실은 시험/교정의 유효성을 모니터링 하기 위한 품질관리절차를 마련해야 하며, 시험/교정 결과 데이터는 결과의 추이를 파악할 수 있는 방식으로 기록해야 한다. 그리고 품질관리 데이터를 분석하고, 사전 정의한 기준을 벗어나는 데이터의 경우 해당 문제를 시정하고 부정확한 결과 보고를 방지하기 위한 조치를 계획 및 실시해야 한다.[666]

---

661) ISO/IEC, International Standard ISO/IEC 17025, op.cit., p.15.
662) ibid.
663) ibid.
664) ISO/IEC, International Standard ISO/IEC 17025, op.cit., p.16.
665) ibid.
666) ISO/IEC, International Standard ISO/IEC 17025, op.cit., p.20.

(6) 결과 보고

시험실에 수행하는 시험/교정 결과는 시험/교정 방법에서 정한 지침에 따라 정확하고 명확하게 그리고 모호함이 없이 객관적으로 보고해야 한다. 시험보고서 또는 교정 인증서는 최소한 다음의 정보를 포함해야 한다.[667]

"a) 제목

b) 실험실의 명칭 및 주소, 시험/교정 수행장소가 기관의 주소와 다른 경우 해당 장소의 위치

c) 시험 보고서 또는 교정 인증서의 고유 식별 정보

d) 고객의 성명 및 주소

e) 사용한 방법의 명시

f) 시험/교정 대상 품목의 설명, 상태 및 명확한 식별 정보

g) 시험/교정 품목의 수령 일자가 결과의 유효성 및 적용에서 중요한 경우에는 해당 수령 일자 및 수행 일자

h) 해당 기관 기관 또는 타 기관이 사용한 시료 선정계획 및 절차가 결과의 유효성 또는 적용과 관련이 있는 경우에는 해당 계획 및 절차

i) 시험/교정 결과 및 해당 사항이 있는 경우 측정단위

j) 시험보고서/교정인증서에 대한 승인권자의 성명, 직책 및 서명 또는 그에 상응하는 식별정보

k) 해당사항이 있는 경우, 시험/교정 결과가 그 대상 품목에 국한하여 관련됨을 표시하는 정보"[668]

(7) 시험 보고서와 교정 인증서

시험보고서는 시험결과 해석에 필요한 다음의 내용을 포함해야 한다

"a) 기존 시험방법과 다른 방법의 사용, 방법 추가, 또는 기존 방법의 제외, 환경조건 등 구체적 시험조건에 관한 정보

b) 해당 사항이 있는 경우, 요구사항/규격에 대한 준수 또는 비준수 여부에 관한 사항

667) ibid.
668) ISO/IEC, International Standard ISO/IEC 17025, op.cit., pp.20-21.

c) 해당 사항이 있는 경우, 추정된 측정의 부정확성에 관한 설명
d) 해당 사항이 있고 필요한 경우, 의견 및 해석
e) 특정 방법, 고객 또는 고객군이 요구하는 추가 정보"[669]

교정인증서는 시험 결과 해석에 필요한 다음 내용을 포함해야 한다.

"a) 측정 결과에 영향을 미치는 교정 수행 조건
b) 측정 부정확성/명시된 측정 규격 또는 해당 규격의 일부 항목에 대한 준수 관련 내용
c) 측정 소급성에 관한 근거"[670]

(8) 의견 및 해석

보고서/인증서에 의견 및 해석을 포함할 경우, 실험실은 해당 의견 및 해석에 대한 근거를 기록해야 한다. 의견 및 해석을 시험보고서에 포함할 경우, 해당 내용이 의견 및 해석에 해당함을 명확히 표시해야 한다.

나. ISO 9001[671]

ISO 9001은 품질관리시스템에 관한 요건을 확립하는 표준으로, 7가지 품질관리원칙을 기반으로 한다. 고객중심, 리더십, 적극 참여, 프로세스 접근법, 개선, 증거기반 의사결정, 관계관리가 그것이다. 이 표준은 계획-실행-검토-조치 사이클 및 리스크 기반 사고가 포함된 프로세스 접근법을 활용한다. 프로세스 접근법은 상호 관련된 프로세스를 하나의 시스템으로 이해하고 관리하는 것으로, 조직이 의도한 결과를 달성하는 과정에서 조직의 효과성과 효율성에 기여한다.

1) 품질관리시스템(Quality Management System)

이 표준은 기관이 고객 요구사항 및 적용되는 법적·규제적 요구사항을 충족하는 제품 및 서비스를 일관성있게 제공하는 능력을 실증할 필요성이 있는 경우, 그리고

669) ISO/IEC, International Standard ISO/IEC 17025, op.cit., p.21.
670) ISO/IEC, International Standard ISO/IEC 17025, op.cit., p.22.
671) http://www.dmsc.moph.go.th/iso/upload/iso9001_2015.pdf; 2016.10.5. ISO 9001 원문을 볼 수 있다. 본 보고서에서는 한국경영시스템(주)에서 한글로 번역한 ISO 9001:2015 규격요구사항을 원용하고자 한다.

조직이 시스템의 개선을 위한 프로세스와 고객 요구사항 및 법적·규제적 요구사항에 적합함을 보증하기 위한 프로세스를 포함하는 시스템의 효과적인 적용을 통해 고객만족을 증진시키고자 하는 경우에 있어서 기관의 품질관리시스템에 대한 요구사항을 규정한다.[672]

기관은 품질관리시스템에 필요한 프로세스를 정하고, 기관 전반에 프로세스의 적용을 정해야 하며, 다음의 사항을 실행해야 한다.

"a) 요구되는 inputs 및 이들 프로세스로부터 기대되는 outputs의 결정
b) 프로세스의 순서 및 상호작용의 결정
c) 효과적 운영 및 프로세스 관리를 보장하기 위해 필요한 기준 및 방법의 결정과 적용
d) 프로세스에 필요한 자원의 결정 및 자원의 가용성 보장
e) 프로세스에 대한 책임과 권한의 부여
f) 6.1의 요구사항에 따라 결정된 위험 및 기회의 조치
g) 프로세스의 평가 그리고 프로세스가 의도한 결과 달성을 보장하기 위해 필요한 모든 변경사항의 실행
h) 프로세스 및 품질관리시스템 개선"[673]

2) 리더십(Leadership)

최고경영진은 다음의 사항에 의해 품질관리시스템에 관한 리더십과 책임을 입증해야 한다.

"a) 품질관리시스템의 효과성에 대한 책임
b) 품질 정책 및 품질 목표가 품질관리시스템을 위해 확립되고 조직의 전략적 방향과 맥락에 부합한다는 것에 대한 보증
c) 품질관리시스템 요구사항이 기관의 업무 프로세스와 통합됨을 보장

---

672) ISO, International Standard ISO 9001 Quality Management System-Requirements, 2015, p.1.; 한국경영시스템(주), ISO 9001:2015 규격요구사항, 2015, 6면에서 재인용.
673) ISO, International Standard ISO 9001, op.cit., pp.2-3; 한국경영시스템(주), 앞의 자료, 7면에서 재인용.

d) 프로세스 접근법 및 리스크 기반 사고의 활용 촉진
e) 품질관시스템에 필요한 자원의 가용성 보장
f) 효과적인 품질관리의 중요성 그리고 품질관리시스템의 요구사항과의 적합성에 대한 중요성의 소통
g) 품질관리시스템이 의도한 결과 달성 보장
h) 품질관리시스템의 효과성에 기여하기 위한 인원의 고용, 지휘 및 지원
i) 개선촉진"[674]

최고 경영진은 품질정책을 확립·실행 및 유지해야 하며, 확립된 품질정책은 문서화된 정보로 이용가능 하도록 유지해야 한다. 최고경영진은 품질관리시스템이 이 표준의 요구사항에 적합하며, 프로세스가 의도된 결과를 도출하고 있다는 것을 보장하기 위해, 품질관리시스템의 변경이 계획되고 실행될 때 품질관리시스템의 완전성이 유지된다는 것을 보장하기 위해 책임과 권한을 부여해야 한다.[675]

3) 계획(Planning)

기관은 품질관리시스템에 필요한 관련 기능·수준 및 프로세스에서 품질목표를 수립해야 하고, 품질목표는 품질정책과 일관성이 있고, 측정가능 해야 하며, 적용되는 요구사항이 고려되어야 하고, 제품 및 서비스의 적합성과 고객만족의 증진과 관련되어야 하며, 모니터링 및 의사소통이 되어야 하고, 적절한 경우에 갱신되어야 한다.[676] 그리고 품질목표에 대해서는 문서화된 정보를 유지해야 한다.

4) 지원(Support)

기관은 품질관리시스템의 수립, 실행, 유지, 지속적 개선을 위해 필요한 자원을 결정하고 제공해야 한다. 즉 품질관리시스템의 효과적 실행 및 프로세스 운영과 관리에 필요한 인원을 결정하고 제공해야 하며, 제품 및 서비스의 적합성을 달성하기

674) ISO, International Standard ISO 9001, op.cit., p.3.; 한국경영시스템(주), 앞의 자료, 8면에서 재인용.
675) ISO, International Standard ISO 9001, op.cit., p.4..; 한국경영시스템(주), 앞의 자료, 9면에서 재인용.
676) ISO, International Standard ISO 9001, op.cit., p. 5.; 한국경영시스템(주), 앞의 자료, 9면에서 재인용.

위해 프로세스 운영에 필요한 기반구조를 결정, 제공 및 유지해야 한다.[677]

제품 및 서비스가 요구사항에 대한 적합성을 검증하기 위하여 모니터링 또는 측정이 사용될 경우, 기관은 유효하고 신뢰할 수 있는 결과를 보장하기 위하여 필요한 자원을 결정하고 제공해야 한다.[678]

기관의 품질관리시스템에는 이 표준에서 요구하는 문서화된 정보와 품질관리시스템의 효과성을 위해 필요한 것으로 결정한 문서화된 정보가 포함되어야 하며, 적합성의 증거로 보유 중인 문서화된 정보는 의도하지 않은 수정으로부터 보호되어야 한다.[679]

5) 운영(Operation)

기관은 다음 사항을 통해, 제품 및 서비스의 제공을 위한 요구사항의 충족 그리고 제6절에서 정한 조치를 실행하기 위해 필요한 프로세스를 계획, 실행 관리해야 한다

"a) 제품 및 서비스에 대한 요구사항 결정
b) 프로세스와 제품 및 서비스 수락에 대한 기준 수립
c) 제품 및 서비스 요구사항에 대한 적합성 달성을 위해 필요한 자원의 결정
d) 기준에 따른 프로세스의 관리 실행
e) 프로세스가 계획된 대로 수행되었다는 것에 대한 신뢰성 확보 및 제품과 서비스 요구사항에 대한 적합성 실증을 위해 필요한 정도의 문서화된 정보결정 및 보유"[680]

기관은 고객에게 제공될 제품 및 서비스에 대한 요구사항을 결정할 경우, 적용되는 모든 법적 및 규제적 요구사항과 조직에 의해 필요한 것으로 고려된 요구사항을 보장해야 한다.[681]

---

677) ISO, International Standard ISO 9001, op.cit., p. 6.; 한국경영시스템(주), 앞의 자료, 10면에서 재인용
678) ISO, International Standard ISO 9001, op.cit., p. 7.; 한국경영시스템(주), 앞의 자료, 11면에서 재인용
679) ISO, International Standard ISO 9001, op.cit., p. 9.; 한국경영시스템(주), 앞의 자료, 13면에서 재인용
680) ISO, International Standard ISO 9001, op.cit., p. 9.; 한국경영시스템(주), 앞의 자료, 13면에서 재인용
681) ISO, International Standard ISO 9001, op.cit., p. 10.; 한국경영시스템(주), 앞의 자료,

가) 제품 및 서비스의 설계 및 개발

기관은 설계 및 개발할 제품 및 서비스의 특정 형태에 필수적인 요구사항을 결정하는 경우, 기능 및 성능/성과 요구사항, 이전의 유사한 설계 및 개발활동으로부터 도출된 정보, 법적·규제적 요구사항, 기관이 실행을 약속한 표준 또는 실행지침, 제품 및 서비스 성격에 기인한 실패의 잠재적 결과 등을 고려해야 한다.[682]

기관은 달성될 결과의 규정, 설계 및 개발 결과가 요구사항을 충족하는지 능력을 평가하기 위한 검토 시행, 설계 및 개발의 결과가 input 요구사항에 충족함을 보장하기 위한 검증활동 시행, 결과로 나타난 제품 및 서비스가 규정된 적용에 대한 또는 사용 의도에 대한 요구사항을 보장하기 위한 실현성 확인 활동의 시행, 검토 또는 검증 및 실현성 확인 활동 중 식별된 문제점에 대한 필요한 모든 조치의 시행, 이들 활동에 대한 문서화된 정보의 보유 등을 보장하기 위해 설계 및 개발 프로세스에 대한 관리를 적용해야 한다.[683]

나) 생산 및 서비스 제공

기관은 다음의 관리조건하에서 제품 및 서비스 제공을 실행해야 한다.

"a) 생산되어야 하는 제품 및 제공되어야 하는 서비스, 또는 수행되어야 하는 활동의 특성과 달성되어야 하는 결과를 규정한 문서화된 정보의 가용성

b) 적절한 모니터링 자원 및 측정 자원의 가용성 및 활용

c) 프로세스 또는 결과의 관리에 대한 기준 그리고 제품 및 서비스에 대한 합격 판정기준이 충족되었음을 검증하기 위해 적절한 단계에서 모니터링 및 측정 활동의 실행

d) 프로세스 운영을 위한 적절한 기반 구조 및 환경의 활용

e) 요구되는 모든 자격을 포함하여 역량 있는 인원의 선정

f) 결과로 나타난 결과가 후속되는 모니터링 또는 측정에 의해 검증될 수 없는 경우, 생산 및 서비스 제공을 위한 프로세스의 계획된 결과를 달성하기 위한

14면에서 재인용

682) ISO, International Standard ISO 9001, op.cit., pp.11-12..; 한국경영시스템(주), 앞의 자료, 15면에서 재인용

683) ISO, International Standard ISO 9001, op.cit., p. 12.; 한국경영시스템(주), 앞의 자료, 15면에서 재인용

능력의 실현성 확인 및 주기적 실현성 재확인

g) 인적 오류를 예방하기 위한 조치의 실행

h) 공개, 인도 및 인도 후 활동의 실행"[684]

6) 성과 평가(Performance Evaluation)

기관은 품질관리시스템의 성과 및 효과성을 평가하고 결과의 증거로 적절한 문서화된 정보를 보유해야 한다. 그리고 품질관리시스템에 대한 기관 자체의 요구사항과 본 표준에 의한 요구사항에 대한 적합성, 품질관리시스템이 효과적으로 실행 및 유지되는지 여부에 관한 정보제공을 위해 계획된 주기로 내부심사를 해야 한다.[685]

최고 경영진은 지속적인 적절성, 충분성, 효과성 그리고 조직의 전략적 방향과의 지속적인 정렬성을 보장하기 위해 계획된 주기로 품질관리시스템을 검토해야한다.[686]

7) 개선(Improvement)

부적합 사항이 발생한 경우 그 사항을 관리 및 시정하기 위한 조치를 취하고 결과를 처리해야 하며, 부적합 사항의 재발방지를 위해 원인을 제거하기 위한 조치 필요성을 평가해야 한다. 부적합 사항의 성격 및 취해진 모든 후속조치와 시정조치 결과는 모두 증거로서 문서화된 정보를 보유해야 한다.[687]

다. ISO/IEC 27001[688]

본 표준은 정보보안 관리체계의 수립, 시행, 유지관리 및 지속개선에 관한 요구사항 제공을 목적으로 하는 것이다[689]

---

684) ISO, International Standard ISO 9001, op.cit., p. 14.; 한국경영시스템(주), 앞의 자료, 17면에서 재인용

685) ISO, International Standard ISO 9001, op.cit., p. 17.; 한국경영시스템(주), 앞의 자료, 19면에서 재인용

686) ISO, International Standard ISO 9001, op.cit., p. 18.; 한국경영시스템(주), 앞의 자료, 20면에서 재인용

687) ISO, International Standard ISO 9001, op.cit., p. 19.; 한국경영시스템(주), 앞의 자료, 21면에서 재인용

688) https://trofisecurity.com/assets/img/iso27001-2013.pdf; 2016.10.5.

689) ISO/IEC, International Standard ISO/IEC 27001 Information technology-Security

정보보안 관리체계는 기관의 절차 및 전체 관리체계의 일부로서 통합되어 있어야 하며, 절차·정보체계·관리방안 설계시 정보보안을 고려해야 한다. 기관 내외부 당사자들은 본 표준을 활용하여 해당 기관이 자신의 정보보안 요구사항을 충족할 수 있는 능력이 있는지 여부를 평가한다.[690]

1) 리더십

가) 리더십과 책임(Leadership and commitment)

최고 경영진은 다음사항을 준수함으로써 정보보안 관리체계와 관련한 리더십 및 책임성을 입증해야 한다.

"a) 기관의 전략 방향에 부합하는 정보보안 방침 및 정보보안 목표를 수립하도록 한다.

b) 기관 절차에 정보보안 관리 체계 요구사항을 통합한다.

c) 정보보안 관리 체계에 필요한 자원을 확보한다.

d) 효과적인 정보보안 관리의 중요성 및 정보보안 관리 체계 요구사항 준수의 중요성을 전파한다.

e) 정보보안 관리 체계가 그 목적을 달성할 수 있도록 한다.

f) 기관 내 인원이 정보보안 관리 체계의 효과성 확보에 기여하도록 지시하고 지원한다.

g) 지속적인 개선을 추진한다.

h) 관련 관리직 인원이 각자의 책임 분야에 해당하는 리더십을 보일 수 있도록 지원한다."[691]

나) 정책(Policy)

최고 경영진은 다음사항을 충족하는 정보보안 정책을 수립한다

"a) 기관의 목적에 부합하여야 한다.

b) 정보보안 목표를 규정하거나 정보 보안 목표 설정을 위한 기본틀을 규정하여야

---

techniques- Information Security management systems-Requirememts, 2013, p. v.

690) ibid.

691) ISO/IEC, International Standard ISO/IEC 27001, op.cit., p.2.

한다.

c) 정보보안 관련 요구사항을 충족할 책무를 규정하여야 한다.

d) 정보보안 관리 체계의 지속 개선에 대한 책무를 규정하여야 한다.

정보보안 방침은 다음 사항을 충족하여야 한다.

e) 방침을 문서화하여 제공하여야 한다.

f) 기관 내부에서 공유하여야 한다.

g) 해당 사항 있는 경우, 관계 당사자에게 제공하여야 한다."[692]

2) 계획(Planning)

가) 정보보안 위험 평가

시험/교정기관은 다음을 충족하는 정보보안 위험평가 절차를 정하고 적용해야 한다. 그리고 시험/교정 기관은 정보보안 위험평가 절차에 관한 정보를 문서화하여 보유하여야 한다.

"a) 다음 사항을 포함하는 정보보안 위험 기준 수립 및 유지

1) 위험 수용 기준

2) 정보보안 위험 평가 수행 기준

b) 각 정보보안 위험 평가 결과의 일관성, 유효성 및 비교가능성 확보

c) 정보보안 위험 파악

1) 정보보안 위험 평가 절차를 적용하여, 정보보안 관리 체계 내 정보의 기밀, 무결성 및 가용성의 손실과 관련된 위험을 평가.

2) 위험 책임자 파악

d) 정보보안 위험 파악

1) 6.1.2 c) 1)항에서 파악한 위험이 실현될 경우 나타날 잠재적 결과에 대한 평가

2) 6.1.2 c) 1)항에서 파악한 위험의 현실적 발생 가능성 평가

3) 위험 수준 파악

---

692) ISO/IEC, International Standard ISO/IEC 27001, op.cit., pp.2-3.

e) 다음 방법에 의한 정보 보안 위험 평가

1) 위험 분석 결과를 6.1.2 a)항에 따라 수립한 위험 기준과 비교

2) 분석한 위험에 대한 대응 우선순위 설정"[693]

다음으로 정보보안 대응절차에 있어서는 다음의 사항을 고려해야 한다.

"a) 위험평가 결과를 고려하여 적절한 정보보안 위험대응 방안 선정

b) 정보보안 위험 대응방안 시행을 위한 필요한 관리조치 결정

c) 필수적인 관리조치가 누락되지 않도록 확인

d) 기관에 필요한 관리조치의 목록 및 목록에 포함된 관리 조치 각각에 대한 포함근거, 조치의 시행여부, 포함시키지 않은 관리 조치에 대한 제외 근거를 내용으로 하는 적용 범위를 포함하는 확인서 작성

e) 정보보안 위험대응 계획 작성

f) 정보보안 위험대응 계획과 잔존정보 보안위험의 수용에 대한 위험책임자의 승인 확보"[694]

나) 정보보안 목표 및 달성 계획

시험/교정기관은 관련 기능과 수준에 있어서 정보보안 목표를 확립해야 한다.

정보보안 목표는 다음사항을 충족해야 한다.

"a) 정보보안 정책에 부합해야 한다

b) 측정가능해야 한다

c) 해당 정보보안 요구사항 및 위험 평가와 위험대응의 결과를 고려해야 한다

d) 목표를 공유해야 한다

e) 적절히 업데이트 되어야 한다"[695]

3) 자격(Competence)

시험/교정기관은 기관의 감독하에 업무를 수행하는 직원 가운데 정보보안 실적에 영향을 미치는 인원의 필수자격을 결정하고, 교육·훈련·경험을 통해 적절한 자격을

693) ISO/IEC, International Standard ISO/IEC 27001, op.cit., pp.3-4.
694) ISO/IEC, International Standard ISO/IEC 27001, op.cit., p.4.
695) ISO/IEC, International Standard ISO/IEC 27001, op.cit., p.5.

갖추도록 해야 한다. 필요한 경우 필수자격 확보를 위한 조치를 취하고 해당 조치의 효과성을 평가하며, 자격에 대한 적절한 증거자료를 문서화하여 보유해야 한다.[696]

4) 정보의 문서화(Documented Information)

문서화된 정보를 작성하고 개시할 경우, 기관은 식별정보 및 기술정보·형식 및 매체 그리고 문서의 적절성 및 충분성 검토 및 승인의 적절성 여부를 확인해야 한다.[697]

문서화된 정보의 관리를 위하여 문서의 배포·접근·검색·사용, 문서의 보관 및 보존, 변경사항 관리, 보유 및 처분 등의 활동을 실시해야 한다.[698]

5) 운영(Operation)

기관은 정보보안 요구사항 충족에 필요한 절차를 계획·시행 및 관리해야 하며, 6.1항에 따른 조치와 정보보안 목표달성을 위한 계획을 시행해야 한다. 그리고 기관은 계획된 주기에 따라 정보보안 위험평가를 정기적으로 실시하고, 평가결과에 관한 정보를 문서화하여 보유해야 한다.

6) 실적 평가(Performance evaluation)

기관은 정보보안 실적 및 정보보안 관리체계의 효과성 평가를 위해 모니터링, 측정, 분석, 평가를 실시해야 한다. 그리고 모니터링 및 측정결과에 대한 증거자료를 적절히 문서화하여 보유해야 한다.[699]

기관은 정해진 주기에 따라 내부감사를 정기적으로 실시하여 관리체계가 기관 자체 요구사항 및 국제 표준상 요구사항에 부합하는지 여부, 관리체계의 효과적 시행 및 유지 여부 등에 관한 정보를 제공해야 한다.[700]

7) 개선(Improvement)

부적합 사항이 발생하는 경우 관리 및 시정조치를 실시하고, 부적합 사항으로 인한

696) ibid.
697) ISO/IEC, International Standard ISO/IEC 27001, op.cit., p.6.
698) ISO/IEC, International Standard ISO/IEC 27001, op.cit., p.7.
699) ISO/IEC, International Standard ISO/IEC 27001, op.cit.,pp.7-8.
700) ISO/IEC, International Standard ISO/IEC 27001, op.cit., p.8.

결과에 대응해야 한다. 그리고 부적합 사항의 원인제거 및 재발방지를 위한 조치의 필요성에 관해서는 원인 및 발생가능성 판단, 필요한 조치 시행, 기관의 재발방지조치의 효과성 검토, 정보보안 관리체계 변경 등의 방법을 통해 평가한다.[701]

기관은 부적합 사항의 성격 및 기관이 취한 후속 조치와 재발방지 조치결과를 문서화하여 보관해야 한다.

제3절 디지털 포렌식 프로세스에 대한 법적 심사기준

1. 디지털 증거에 대한 법적 심사기준의 한계

법원은 디지털 증거의 증거능력을 판단함에 있어서 동일성·무결성·신뢰성에 대한 입증을 중심으로, 절차적 연계성의 유지, 원본과 복제본의 해시값 비교검증, 출력에 이용한 컴퓨터의 기계적 정확성, 프로그램의 신뢰성, 입력·처리·출력 각 단계에서의 조작자의 전문적인 기술능력과 정확성 담보 등을 그 논거로서 제시하고 있다. 하지만 이러한 요건들이 담보되어야 한다는 당위적 논거만 제시할 뿐 도구로서 하드웨어와 소프트웨어의 신뢰성 그리고 조작자의 기술적 능력과 정확성에 대한 구체적인 법적 판단기준은 제시된 바가 없다. 즉 과학적 증거방법으로서 디지털 포렌식 도구와 포렌식 분석관에 대한 법적 판단기준은 신뢰성과 정확성이라고 하는 추상적 용어로 정의되고 있을 뿐, 어떤 기준에서 신뢰할 수 있는 것인지에 대한 법적 판단의 근거는 결여되어 있다고 할 것이다.

디지털 데이터를 수집 및 선별하여 분석하는 과정 - 탐색, 복구, 추출 등 -을 거쳐, 결과를 제출하는 절차, 그 과정에서 사용되는 디지털 포렌식 도구, 그리고 그 도구를 사용하여 포렌식 절차를 진행하는 디지털 포렌식 분석관, 그리고 그에 의해 산출된 결과를 기술한 포렌식 보고서에 이르는 모든 것이 과학적 지식을 기반으로 한 전문성 그리고 기술적 지식과 경험이 요구되는 영역이라 할 수 있다. 이와 같이 과학과 기술이 지배하는 영역을 법적 판단안으로 가져와서 법적인 관점에서의 신뢰성을 판단하기 위해서는, 최소한 그 적용된 과학과 기술이 유효하다는 검증을 전제로 독자적인 사법

701) ISO/IEC, International Standard ISO/IEC 27001, op.cit., p.9.

적 평가가 이루어져야 할 것이다. 즉 디지털 증거는 디지털 기술에 적합한 도구에 기반하여 산출되는 것이기 때문에, 물리적으로는 내용 확인이 어려운 형태의 디지털 증거를 인식가능한 상태의 자료로 전환하여 혐의사실을 입증할 수 있는 형태로 법정에 제출하기까지의 과정에 적용된 과학적 방법과 기술적 원리에 대한 이해가 전제되어야 그 신뢰성을 판단할 수 있다고 할 것이다. 다만 과학적 이론과 기술적 운용방식을 제대로 이해하기 어려운 판사에게 과학적 이론이나 기술의 운용이 정확한 것인가의 여부를 결정하도록 요구할 수는 없지만, 최소한 과학으로서의 건전성 또는 응용 기술로서의 유효성을 적합하게 하는 기준을 충족하는가의 여부를 확인하여 판단하도록 요구할 필요는 있다고 할 것이다.

아직까지는 디지털 증거를 수반하는 사건들에 있어서 디지털 포렌식 도구의 신뢰성, 포렌식 분석관의 자격 내지 전문성, 디지털 포렌식 프로세스의 유효성 등이 전면적인 법적 쟁점으로 다투어진 경우가 없었기 때문에, 법원의 입장에서도 이에 대하여 특별한 판단을 할 필요가 없어서 디지털 증거를 둘러싼 포렌식 영역에서의 과학적·기술적 요소에 대한 법적 평가기준이 정립되지 못하였다고 할 수 있다. 하지만, 디지털 기술의 발전과 함께 디지털 포렌식 기술의 개발속도도 점차 빨라지고 있고, 요구되는 기술영역도 점차 다양화되어 가고 있는 상황에서, 도구나 전문가 또는 프로세스에 대한 공식적인 검증도 없이 그에 대한 법적 신뢰를 어떻게 판단할 것인가에 대한 문제는 언제든지 제기될 수 있다고 할 것이다. 그리고 형사소송법 개정으로 “과학적 분석결과에 기초한 디지털 포렌식 자료에 의한 증명”으로 증거능력을 인정할 수 있게 되었으므로, 디지털 포렌식 자료의 신뢰성 뿐만 아니라 그 기초가 된 과학적 분석의 신뢰성에 대한 입증이 요구될 수 밖에 없다. 따라서 이에 대한 법적 판단기준을 어떻게 정립할 것인가에 대한 논의가 필요하다고 할 것이다.

2. 디지털 포렌식과 Daubert Test 기준의 부적합성

법적 공동체안에서는 디지털 포렌식에서 활용된 소프트웨어와 도구의 신뢰성을 이끌어낼 때, 그리고 디지털 포렌식 분석관이 제출한 포렌식 보고서에 적용된 과학적 방법과 그에 의해 도출된 결과의 신뢰성을 판단할 때, 일반적으로 Daubert test의 적용이 가장 우선하여 고려될 수 있다

Daubert v. Merrell Dow 판결은 판사가 과학적 증거가 연방법정에서 허용될 수 있는가의 여부를 판단할 수 있는 5가지의 기준을 확립했는데, 이를 Daubert test 또는 Daubert standards라 한다. Daubert 기준은 증거를 준비하거나 밝혀내는데 활용되는 모든 과학적 절차에 적용되며, 과학적 증거를 승인하기 위한 객관적 가이드라인을 판사에게 제공한다.

가. Daubert standards

Daubert 판결[702]에서 미 연방대법원은 아래의 기준을 사용하여 과학적 증거의 허용성을 판단하였다.

(1) 검증가능성 : 과학적 이론과 절차가 독자적으로 검증한 것인가
(2) 동료심사 : 과학적 절차가 출간되었으며 동료심사의 대상이 되었는가
(3) 오류율 : 과학적 절차의 활용과 관련하여 오류율을 알게 될 가능성이 있는가 또는 알려진 오류율이 존재하는가
(4) 표준 : 과학적 절차의 방법을 통제하기 위한 표준과 프로토콜이 존재하는가
(5) 승인 : 과학적 절차가 일반적으로 관련 과학 공동체에 의해 승인되었는가

이 판결에서 Blackmun 판사는 과학적 결론 보다는 그것이 도출된 원리나 방법의 중요성에 입각하여 법관이 과학적 증거에 대하여 어떠한 태도를 취하여야 하는가를 지적하고 있다.

"첫째, 과학적 증거의 유효성에 대한 판단은 판사의 책임과 권한에 속하므로 판사들은 과학적 증거가 법의 영역으로 들어오는데 있어서 문지기 역할을 해야 한다.

둘째, 판사가 독자적으로 과학적 증거의 유효성을 판단할 때는 과학이 과학적 연구의 타당성을 판단할 때 사용하는 기준을 사용하여 특정한 과학적 지식이 타당한 것일 가능성이 클 때만 그 지식을 증거로서 고려해야 한다.

셋째, 사실규명과 사실에 대한 이해에 도움이 되는 과학적 지식만 법정에서 수용할 수 있다.

넷째, 전통적인 교차신문과 반대증거의 제출, 입증책임이 불확실하지만 증거를 허

---

702) Daubert v. Merrell Dow Pharmaceuticals, 509 U.S.579(1993)

용할 수 있는 적절한 수단이 된다"[703]

나. 디지털 포렌식과 Daubert 기준의 부적합성에 대한 논의

Daubert test는 현재 과학적 증거의 허용성 여부와 관련하여 보편적인 신뢰성 판단 기준으로 인식되고 있지만, 디지털 포렌식에 의해 산출된 디지털 증거에 Daubert 기준을 적용하여 법적 허용가능성 여부를 판단할 수 있는가에 대해서는 비판적 시각이 존재한다.

디지털 포렌식 도구에 활용되는 소프트웨어는 그 성질에 있어서 과학적인 것이 아니며 따라서 과학과 동일한 원칙을 이용해 신뢰해서는 안된다는 견해가 있다.[704] 즉 건전한 과학적 프로세스는 반복가능하고 검증이 가능하지만, 디지털 데이터를 분석하는 도구와 방법은 특허 등으로 인해 소스가 폐쇄되어 있기 때문에 재현하는 것이 가능하지 않다는 것이다. 그리고 이러한 도구를 활용하는 디지털 포렌식 조사관도 도구의 사용방법은 알지만 도구운용의 기술적 방식에 대한 설명을 제대로 하지 못하기 때문에 신뢰할 수 없다는 것이다. 따라서 이 견해를 주장하는 사람은 판사는 자동적으로 포렌식 도구를 과학적 프로세스의 일부로서 신뢰해서도 안되고, 그것을 활용하는 포렌식 조사관도 신뢰해서는 안된다고 하는 약간은 극단적인 주장을 하고 있다.[705]

이와는 좀더 다른 차원에서 디지털 포렌식이 Daubert test에서 제시된 기준을 충족하기 어려운 측면이 있음을 제시하는 견해가 있다. 즉 디지털 포렌식 분야의 역사가 너무 짧은 반면에 변화속도는 너무나 빠르기 때문에 동료심사의 대상이 되기에 부적합할 뿐만 아니라 관련 공동체에 의한 승인이 큰 중요성을 갖지 못한다는 것이다.[706] 또한 Daubert 기준은 이론이나 기술이 동료심사의 대상이 되지 않고 있거나 또는 출간되지 않고 있다는 사실이 자동적으로 그 도구나 소프트웨어를 허용할 수 없는

---

703) Thomas G. Field, Jr & Colleen M. Keegan, "Daubert's Significance", http://www.fplc.edu/RISK/vol4/fall/daubert.htm; 탁희성/이상진, 디지털 증거분석도구에 의한 증거수집절차 및 증거능력 확보방안, 2006, 165면에서 재인용.

704) Zdziarsko's blog of things, "The Importance of Forensic Tools Validation"; https://www.zdziarski.com/blog/?p=3112; 2016.8.10.

705) ibid.

706) David Watson/Andrew Jones, Digital Forensics Process and Procedures, 2013, p.5.

것으로 만들지도 않기 때문에[707] 디지털 포렌식에 있어서 Daubert 기준에 따른 판단에는 한계가 있다는 것이다.

다. Daubert 기준의 확장으로서 금호타이어 판결

이와 같이 디지털 포렌식은 과학이 아니기 때문에 Daubert 기준이 적용되어서는 안된다는 비판에도 불구하고, 디지털 증거의 허용성에 대한 판단기준으로 Daubert 기준이 적용되고 있는 것은 금호타이어 판결[708] 때문이라고 할 수 있다.

즉 금호타이어 판결에서 미 연방대법원은 Daubert test는 과학자가 아닌 엔지니어 및 그 외 분야의 전문가 증언에 적용할 수 있다고 판단하였다. 즉 법관이 과학적 지식과 기술적 지식을 구분하여 증거규칙을 달리 적용하는 것은 불가능하거나 매우 어렵기 때문에, 과학적·기술적 또는 전문적 지식이 사실심 법관을 보조할 수 있는 경우에는 전문가로 인증된 증인은 의견의 형태로 이를 진술할 수 있으며, 그러한 전문가 증언의 증거능력을 판단함에 있어서는 Daubert 기준이 적용이 된다고 본 것이다.[709]

이 판결에 의하게 되면 디지털 포렌식을 과학이 아니라고 해도, 전문적 지식과 기술 그리고 경험에 기반한 디지털 포렌식 분석관의 분석결과물, 그리고 그 산출방법에 대한 증언에 대해서도 Daubert 기준을 적용하여 그 신뢰성을 판단할 수 있다고 볼 것이다.

3. 디지털 포렌식에 적합한 법적 평가기준의 재정립

가. Daubert test에 대한 환상

일반적으로 과학적 증거에 대해서는 Daubert test가 엄격히 적용되고 있다고 생각한다. 하지만 미 연방법원의 경우 Daubert 분석이 거의 행해지지 않거나 행해지더라도 엄격하게 그 기준을 적용하지 않은 채 포렌식 증거들이 허용되고 있다고 보고되고

---

707) http://www.forensicmag.com/article/2011/03/validation-forensic-tools-and-software-quick-guide-digital-forensic-examiner; 2016.8.10.
708) Kumho Tire Co. v. Carmichael, 526 U.S.137(1999)
709) 노명선, "해외 판례 동향", Forensics 2011, 19면.

있다.[710] 더욱이 2009년 포렌식 기술의 활용에 있어서 품질과 일관성 확보를 위한 개선방안과 가이드라인을 제시한 National Research Council 보고서에 따르면, 포렌식 운용에 있어서 불일치, 일관성 없는 관행, 표준화 결여, 증명과 승인의 결여, 해석적 문제들이 존재하는 것이 확인되었다고 보고하고 있다.[711] 그럼에도 불구하고 법원은 여전히 Daubert test를 통하여 포렌식 증거에 대한 사법시스템의 신뢰를 견고히 유지하고 있고, 비과학적 법과학의 유효성에 대한 신뢰를 보인다고 하는 비판이 가해지고 있다.[712] 즉, 연방법원들이 비과학적 포렌식 증거들에 대해서 Daubert 분석도 하지 않은 채 받아들이거나 심지어는 그러한 증거가 그동안 허용되어 왔다는 내력을 이유로 부적절하게 증거로 허용하고 있다는 것이다.

이와 같이 사법영역에 있어서는 포렌식 증거의 신뢰성과 관련하여 Daubert test 기능이 지나치게 과대평가된 측면이 존재하는 것이 사실이며, 이는 어느 정도 과학에 대한 무의식적 신뢰의 환상에서 비롯된 것일 수 있다. Daubert test는 과학적 증거가 제시하는 과학적 토대와 방법이 과학공동체와 법정에서 지지를 받을 수 있는 것인가를 사실인정자들로 하여금 검토하고 고민하게 하는 출발점으로서 생각해야지, 그 기준만 충족하면 신뢰할 수 있는 과학적 증거라고 단정지을 수 있는 결정자로서 생각해서는 안된다고 할 것이다.

Daubert test가 과학적 증거의 신뢰성을 확보할 수 있는 유일한 기준은 아니므로, 그 분야에서 활용되는 과학과 기술에 대한 신뢰를 법적으로 입증해줄 수 있는 하나의 척도로서 유효하게 적용될 수 있는 방식으로 재정립할 필요가 있다고 할 것이다.

---

710) Adam Teicher, “Weaving functional brain imaging into the tapestry of evidence: A case for functional neuroimaging in federal criminal courts”, Fordham Law Review, Vol.80, 2011, p.395; 탁희성/이인영/권준수/강도형/장준환, 뇌과학의 발전과 형법적 패러다임 전환에 관한 연구 II, 2014, 275면에서 재인용.

711) Adam Teicher, op.cit., 382; 탁희성/이인영/권준수/강도형/장준환, 앞의 보고서, 276면에서 재인용.

712) Michael J.Saks, “Explaining the Tension Between the Supreme Court’s Embrace of Validity as the Touchstone of Admissibility of Expert Testimony and Lower Court’s(Seeming) Rejection of Same”, Episteme, Vol.5, 2008, p.336; 탁희성/이인영/권준수/강도형/장준환, 앞의 보고서, 276면에서 재인용.

나. 디지털 포렌식에 적합한 법적 평가기준 재검토

디지털 포렌식 프로세스를 거쳐 산출된 결과로서 디지털 증거의 증거능력에 대한 Daubert 기준은 과학적 절차의 건전성과 신뢰성에 대한 심사에 중점을 두고 있지만, 그러한 절차의 건전성 등이 증거의 신뢰성을 보장하는 것은 아니라는 점을 염두에 둘 필요가 있다. 특히 디지털 포렌식 분야에 있어서 도구나 장비에 해당하는 하드웨어와 소프트웨어는 거의 전체적으로 즉석 매뉴얼 분석 프로세스가 구조화되어 있어서 굳이 수년간의 경험이나 훈련이 없이도 분석업무와 보고서 작성이 가능하다고 할 수 있다.[713] 이와 같이 디지털 포렌식 도구와 장비의 운용이 매뉴얼화 됨으로 인해 포렌식 조사관의 전문적 지식 수준이 낮아지는 문제가 발생하고 있다.

Daubert 기준에 있어서 디지털 포렌식 조사관의 자격을 측정할 수 있는 기준은 없기 때문에, 포렌식 조사관에 의해 작성된 보고서를 심사함에 있어서는 포렌식 조사관의 자격을 우선하여 엄격히 심사해야 한다. 그리고 그 심사에 있어서는 인증, 교육 또는 실무 경험의 수준 등을 적절히 조합하여 고려할 필요가 있다고 할 것이다. 또한 앞서 기술한 바와 같이 디지털 포렌식 기술의 발전속도와 변화를 고려할 때 저널 등의 출간에 의한 동료심사는 거의 적용하기 어려운 기준이라 할 수 있다.

이와 같이 디지털 포렌식의 신뢰성에 대한 법적 평가기준으로서 Daubert 기준을 그대로 적용하는 데는 한계가 있을 수 밖에 없다. 따라서 Daubert test의 취지를 유지하면서도 디지털 포렌식의 신뢰성을 법적 기준에서 평가할 수 있는 수정된 형태의 기준이 검토될 필요가 있다고 할 것이다.

---

713) Daniel B.Garrie&David Morrissy, "Digital Forensic Evidence in the Courtroom: Understanding Content and Quality", Northwestern Journal of Technology and Intellectual Property, Vol.12, 2014, p.124.

제5장

KOREAN INSTITUTE OF CRIMINOLOGY

디지털 포렌식 프로세스 통합 프레임 구축을 위한 정책적 제언

탁 희 성

제5장

디지털 포렌식 프로세스 통합 프레임 구축을 위한 정책적 제언

제1절 디지털 포렌식 프로세스 통합 모델 프레임

1. 디지털 포렌식 프로세스 통합관리시스템 구축

가. 통합관리시스템의 기본 개요

디지털 포렌식 프로세스에 있어서 가장 기본적으로 인식해야 할 사항은 모든 기관의 디지털 포렌식 업무에 있어서 동일하게 적용할 수 있는 표준적인 디지털 포렌식 프로세스는 불가능하다는 것이다. 이는 각 기관별로 디지털 포렌식 업무를 수행하는 목적과 기능이 다르고, 디지털 포렌식 부서의 규모와 업무범위가 다양하기 때문이다. 다만 이와 같은 차이에도 불구하고 디지털 포렌식 프로세스를 통해 디지털 포렌식 업무가 일정한 수준의 품질을 유지할 수 있고, 이에 의해 디지털 증거분야에 있어서 신뢰할 수 있는 결과를 산출할 수 있는 업무관행을 확립하고 유지할 수 있는 체계적인 접근방법을 제시할 수 있다는 점에서 디지털 포렌식 프로세스의 중요성을 인식할 필요가 있다고 할 것이다.

이러한 디지털 포렌식 프로세스가 일관성과 신뢰성을 갖출 수 있도록 함에 있어서는 그 전체적인 프로세스 운용에 공통적으로 적용할 수 있는 통합관리시스템을 갖추는 것이 전제되어야 한다. 즉, 기관이 수행한 디지털 포렌식 프로세스에 의해 산출된 결과의 정확성 및 신뢰성에 영향을 미칠 수 있는 주요 요인 - 문서화된 절차의 정확성, 직원에 대한 교육·훈련, 프로세스의 지속적인 개선 및 유지, 포렌식 업무수행을 위한 환경적 조건, 기관이 포렌식 업무에 사용하는 하드웨어, 소프트웨어, 장비 등 -이

적절히 관리 및 통제할 수 있는 관리시스템이 필요하다고 할 것이다.

따라서 통합관리시스템은 디지털 포렌식 업무를 수행하는 기관의 모든 영역 - 즉, 시설, 직원, 도구 및 장비, 절차, 교육 훈련 등 -, 그리고 수행되는 모든 활동 - 수집, 분석, 기록, 보존, 증언 등 - 에 적용되어야 한다. 즉 통합관리시스템은 디지털 포렌식 업무를 수행하는 기관에 있어서의 모든 지침·절차·규정·표준·인증 등을 포괄하는 표준운영절차이자, 기관의 디지털 포렌식 업무목표 즉 디지털 증거의 신뢰성 확보를 위한 일관된 정책적 뒷받침이라고 할 수 있다. 이러한 접근방법은 하나의 일관된 시스템에서 디지털 포렌식 업무 프로세스와 절차들을 총괄적으로 관리할 수 있게 할 뿐만 아니라, 업무간 효율적 연계를 가능하게 함으로써 포렌식 프로세스가 관련 업무에 적합한 방식으로 운용·심사·유지·통제된다는 것을 보장할 수 있게 한다.

나. 통합관리시스템의 기본원칙 확립

디지털 포렌식 기관은 신뢰할 수 있는 디지털 증거를 확보하기 위한 디지털 포렌식 프로세스 통합관리시스템을 구축함에 있어서 기본적으로 준수되어야 할 업무원칙을 가지고 있어야 한다.

포렌식 업무를 처리함에 있어서 일반적으로 승인된 몇가지 원칙들이 있는데, G8 원칙, ACPO 원칙, IACIS 행위수칙, IOCE 원칙 등이 그것이다.[714] 먼저 G8에서 제시하고 있는 디지털 증거처리 원칙은 다음과 같으며, IOCE 원칙도 ⅰ)을 제외하고는 이와 동일하다.

"ⅰ) 일반 법과학 및 절차 원칙을 모두 적용한다.
ⅱ) 디지털 증거 확보 후 해당 증거를 변경하는 행위를 하지 않는다.
ⅲ) 원본 디지털 증거에 접근할 필요가 있는 경우, 해당 직원은 적절한 훈련을 이수해야 한다.
ⅵ) 디지털 증거의 확보·접근·저장·이송에 관한 모든 활동은 철저히 기록하여 유지하고, 검토를 위해 제공되어야 한다.

---

714) David Watson/Andre Jones, Digital Forensics Processing and Procedures:Meeting the Requirements of ISO 17020, ISO 17025, ISO 27001 and Best Practice Requirements, 2013, p.371.

v) 각 개인은 디지털 증거가 자신의 점유에 있을 때 그와 관련하여 취해진 모든 조치에 대해 책임을 진다.

iv) 디지털 증거의 확보·접근·저장 또는 이송을 담당하는 기관은 위 원칙을 준수할 책임이 있다."[715]

IACIS(International Association of Computer Investigative Specialists)에 의해 제시된 디지털 포렌식 관련 행위수칙은 다음과 같이 정리될 수 있다.

"i) 증거에 대한 영향을 최소화한다

ii) 원본 매체에 대한 변경사항을 모두 파악한다

iii) 해당 지역의 증거규칙을 준수한다

vi) 포렌식 분석은 기관의 능력범위를 벗어나서는 안된다."[716]

영국의 ACPO(Association of Chief Police Officer)가 제시한 디지털 증거 처리 원칙은 앞의 제3장에서도 기술한 바 있지만 다시 정리하면 다음과 같다.

"i) 법집행기관 또는 그 직원은 이후 법원에서 활용할 컴퓨터 또는 저장매체상 데이터를 변경해서는 안된다.

ii) 컴퓨터 또는 저장매체상 원본 데이터에 접근할 필요가 있는 경우, 그 직원은 관련 자격을 갖추어야 하며, 그 행위의 관련성 및 의미를 설명하는 증거를 제출할 수 있어야 한다.

iii) 디지털 증거에 적용된 모든 프로세스에 대한 감사 추적 또는 기록을 작성하여 유지해야 한다. 독자적인 제3자가 그러한 프로세스를 검사할 수 있어야 하고 동일한 결과를 도출할 수 있어야 한다.

vi) 수사를 담당한 사람은 법률과 원칙의 준수를 확보할 전반적인 책임을 진다"[717]

이와 같이 기존에 주요 기관들에 의해 승인된 디지털 증거 처리업무의 기본원칙의 내용에 비추어 볼 때, 디지털 포렌식 프로세스 전체에 가장 기본이 되어야 할 업무처리 원칙은 다음과 같이 정리해 볼 수 있다.

---

715) ibid.
716) ibid.
717) Association of Chief Police Officers, ACPO Good Practice Guide for Digital Evidence, 2012, p.6.

첫째, 디지털 포렌식 프로세스 전체에 걸쳐 디지털 증거는 변경되어서는 안된다.

둘째, 디지털 포렌식 업무를 수행하는 직원은 관련 자격과 교육·훈련 기록을 유지해야 한다.

셋째, 디지털 증거에 취해진 모든 조치들은 엄격히 기록되어야 한다.

넷재, 디지털 증거와 관련한 모든 법규와 관련 원칙들을 준수해야 한다.

다. 통합관리시스템의 구성

통합관리시스템은 기관이 디지털 포렌식 업무를 수행함에 있어서 관련 직원들이 따라야 하는 기관의 프로세스와 방침을 만들고, 검증하고, 유지하는 일련의 정책과 절차라고 할 수 있다. 디지털 포렌식 업무와 관련하여서는 기존의 판례들을 통해서 제시된 증거법적 요구사항·법령상의 규정들·기관내 업무지침·분야별 모범 실무매뉴얼 뿐만 아니라 포렌식 프로세스에 필수적인 정책 등에서 비롯된 다양한 대내외적 요구사항들이 존재하기 때문에, 이를 일관성 있게 프로세스 운용에 반영할 수 있는 통합적인 관리체계가 필요한 것이다. 또한 디지털 포렌식의 신뢰성 확보와 관련하여 요구되는 국제적인 표준으로서 ISO 인증이 요구되는 상황하에서 ISO 표준에 따른 구체적인 기준들을 준수해야 하기 때문에, 이러한 표준들이 통합관리시스템을 통해서 유지 및 관리될 수 있도록 해야 할 필요성이 있다고 할 것이다.

1) 절차적 지침의 수립 및 유지

디지털 포렌식 기관들은 디지털 포렌식 프로세스 단계별로 또는 업무 분야별로 기관내부 실무지침이나 가이드라인을 두고 있는 것이 일반적이다. 이러한 가이드라인이나 지침을 개발하는 이유는 그것이 증거가 처리되는 방식에 있어서 일관성이 존재한다는 것을 보장하기 때문이며, 이와 같이 일관성이 확보된 가이드라인이나 지침들을 활용함으로 인해 디지털 증거의 무결성 또는 산출된 결과의 신뢰성을 입증할 수 있는 것이다.

이러한 지침이나 가이드라인 등은 통상 해당 절차나 업무의 필요성에 기하여 구체적이고 세부적인 내용으로 구성되어 있는 것이 일반적이다. 즉 전체적인 프로세스 관점에서 만들어진 것이 아니기 때문에 지침간에 충돌이 발생하거나 반대로 일정한

사항에 있어서는 절차적 흠결이 발생할 수도 있다. 특히 디지털 포렌식을 요구하는 영역이 다양해지면서 하나의 사건에 있어서 여러 분야의 디지털 포렌식 업무가 동시에 이루어지는 경우에 그러한 문제가 발생할 수 있다.

또한 디지털 기술이 급속하게 발전하는데 대응하여 디지털 포렌식 업무에 적용되는 지침이나 가이드라인도 적시에 수정·개선될 필요가 있는데, 그러한 변화를 지속적으로 관찰하고 검토하여 반영할 수 있는 관리주체가 명확하지 않는 한 관련 업무수행만으로도 벅찬 실무진 차원에서 신속히 수정하거나 개선할 것을 기대하기는 쉽지 않다. 이와 같이 디지털 포렌식 업무수행에 적용되어야 할 지침이나 가이드라인이 현실적인 상황을 제대로 반영하지 못하게 되면, 이를 따를 수 없게 되고 결국 그에 의해 산출된 결과가 어떠한 절차에 따라 산출된 것인지를 확인하고 검증할 수 있는 방법이 없다고 할 것이다. 이는 디지털 포렌식 프로세스에 대한 신뢰를 훼손할 우려가 있기 때문에, 관리적인 차원에서 포렌식 프로세스에서 절차별로 또는 분야별로 운용되는 절차적 지침이나 가이드라인을 일관성 있게 개발하고, 이를 유지·보완·수정·대체할 수 있도록 하는 것이 디지털 포렌식 프로세스의 유효성과 신뢰를 유지하는 방법이라 할 것이다.

2) 품질 관리시스템 구축

디지털 포렌식 프로세스에 있어서 통합관리시스템이 요구되는데는 절차적인 일관성이나 신뢰성을 확보하고자 하는 목적도 있지만, 궁극적으로는 그와 같이 신뢰할 수 있는 일관된 프로세스를 통해서 일정한 수준 이상의 품질을 갖춘 결과를 산출함으로써 디지털 증거를 법정에서 신뢰할 수 있도록 하기 위한 것이라 할 것이다. 따라서 디지털 포렌식 프로세스 관리시스템의 중심은 업무 품질을 관리할 수 있는 시스템을 갖추는 것이라 할 수 있다. 이를 위해서 디지털 포렌식 업무를 수행하는 기관은 ISO 9001 인증을 갖출 필요가 있는데, 이는 통합관리시스템 및 품질관리시스템에 의한 새로운 관리체계의 필수적인 토대를 제공하기 때문이다.

가) 업무품질 관리

디지털 포렌식 업무품질을 유지하기 위해서 기관은 모든 업무에 대하여 적절한 품질의 업무방식을 수립하고 시행해야 하며, 디지털 포렌식 업무를 수행하는 직원은

통합관리시스템의 방침·절차·표준에 따라 업무를 수행해야 한다. 또한 포렌식 업무를 수행하는 직원은 적절한 교육과 훈련을 이수하여 해당 업무에 대한 자격을 갖추어야 하며,[718] 해당 자격에 대한 증빙기록을 보유할 것이 요구된다. 그리고 포렌식 조사관이 검증되지 않은 도구를 사용하는 경우 의도하지 않은 데이터의 변경이 발생할 우려가 있기 때문에, 의도한대로 정확하게 업무를 수행하기 위해서는 검증된 도구를 사용해야 한다.[719]

기관이 수행하는 모든 디지털 포렌식 업무처리는 통합관리시스템의 요구사항을 충족해야 하고, 과학적 건전성과 반복성을 갖추어야 하고, 신뢰성 있는 결과를 제공해야 한다. 그리고 기관내에서 적용되고 있는 인증·표준 등과 관련하여 요구되는 사항들을 준수함으로써 통합관리시스템내에서 품질관리시스템을 수립·시행·유지할 필요가 있다.[720]

업무품질 관리를 위해서는 모든 디지털 포렌식 조사 보고서의 일부는 제출되기 전에 다른 자격있는 디지털 포렌식 조사관에 의해 기술적인 검토를 받아야 하는데, 이러한 기술적 검토의 목적은 다음과 같다.

"ⅰ) 보고서가 명확하고 이해하기 쉽게 되어 있다
ⅱ) 수행된 절차가 적절히 문서화되었으며 포렌식적으로 건전했다.
ⅲ) 조사기록이 그 결과를 재현하기에 충분할만큼 상세하게 되어 있다.
ⅵ) 포렌식 조사관의 해석과 결론이 합리적이고, 조사기록에 의해 뒷받침되며, 과학적으로 유효하다"[721]

이러한 품질관리업무가 기관의 품질수요를 충족하도록 하기 위해서는 정기적으로 품질관리시스템에 대한 심사가 행해져야만 한다.

나) 환경품질 관리

디지털 포렌식 업무를 수행하는 기관은 사건처리에 영향을 미칠 수 있는 환경조건

718) David Watson/Andre Jones, op.cit., p. 182.
719) Council of the Inspectors General on Integrity and Efficiency, Quality Standards for Digital Forensics, 2012, p.3.
720) ibid.
721) Council of the Inspectors General on Integrity and Efficiency, Quality Standards for Digital Forensics, 2012, p.3.

에 대한 보호조치를 취해야 한다. 특히 디지털 증거의 취약성을 고려하여 전원 관리, 정전기 방전과 정전기 간섭표준운용절차, 온습도 제어 등이 갖추어져 있어야 한다.[722]

3) 표준의 적용 및 유지관리

앞서 기술한 바와 같이 디지털 포렌식 프로세스의 신뢰성을 확보하기 위해 적용이 요구되는 국제적 표준은 다수가 존재한다. 그 가운데 디지털 포렌식 분석실(연구소)와 관련하여 가장 기본적으로 요구되는 국제적 표준이 ISO 17025인데, 이 표준에 의한 인증을 받기 위해서는 해당 기관이 품질관리시스템을 운영하는 것 뿐만 아니라, 기술적 자격을 갖추고 기술적으로 타당한 결과를 생산할 수 있어야 하며, 표본 추출을 포함한 시험/교정을 시행할 수 있는 관련 자격 요구사항을 명시해야 한다.

이와 같이 ISO 인증을 적용·유지하게 되면, 디지털 포렌식 업무를 수행하는 기관은 특정 사건에서 증거의 최초 접촉시부터 최종 증거제출에 이르기까지 다음의 사항을 입증할 수 있게 되고, 따라서 기관에서 수행되는 디지털 포렌식 프로세스 전체에 대한 신뢰성을 담보받을 수 있다고 할 수 있다.

"ⅰ) 최초 접촉부터 증거제출시까지 사건처리 과정이 자격과 능력을 갖춘 포렌식 분석관에 의해 수행되었으며, 해당 분석관은 사건처리 과정에서 사용한 도구 및 방법론에 대한 훈련을 받았으며, 사건처리에 필요한 모든 정보에 접근할 수 있었다.

ⅱ) 사건처리에 사용한 방법 및 도구는 기술적으로 건전성을 갖추었고, 의뢰인(수사관)의 요구사항에 적합하였다

ⅲ) 사건처리에서 사용한 모든 도구, 하드웨어, 소프트웨어는 사건처리과정에서 적절하게 유지관리 되었으며, 적법한 사용권한을 유지하였다.

ⅳ) 결과물을 제출하기 전에 철저히 검토하였으며 의뢰인(수사관)의 요구사항을 충족했다.

ⅴ) 사건처리과정에서 파악한 부적합 사례는 적시에 효과적으로 처리하였다

ⅵ) 사건처리의 모든 과정에 대해서는 문서화된 절차가 존재한다

---

722) ENFSI, Best Practice Manual for the Forensic Examination of Digital Technology, 2015, p.15.

vii) 위 사항에 대한 모든 근거는 전자기록관리시스템(Electronic Records Management System)안에 수록되어 있다"[723]

이와 같이 ISO 인증을 통해 디지털 포렌식 업무품질과 결과에 대한 공신력을 확보할 수 있다는 점에서 볼 때, 디지털 포렌식 업무를 수행하는 기관들은 ISO 인증을 받는데 노력을 기울일 수 밖에 없다고 할 것이다.

그런데 ISO 인증은 한번 획득하는 것으로 계속 그 유효성을 유지하는 것이 아니며, ISO 표준별로 갱신주기가 있는데, 3년, 5년, 10년 등으로 되어 있다. 즉 최초 인증일로부터 정해진 갱신기간내에 갱신심사가 실시되어야 하며, 유효기간 이내에 심사가 종료되어야 하며, 심사시 부적합 사항에 대해서는 시정조치가 완료되어야 한다. 만약 유효기간내에 갱신심사가 진행되지 않으면 인증의 유효성은 종료된다.

디지털 포렌식 프로세스에는 하나의 표준이나 인증만이 있는 것이 아니라 여러 분야에 적용되는 다수의 국제적인 표준이나 인증이 있을 수 있는데, 이를 체계적으로 관리하지 못하게 되면 표준에의 부적합 내지 인증 만료 등으로 인해 표준이 적용된 프로세스에 대해 신뢰가 확보되지 못할 우려가 있을 수 있다. 따라서 디지털 포렌식 프로세스에 적용되는 국제표준에 대해서는 정기적으로 그 준수여부를 리뷰해야 하고, 부적합 상황이 발생한 경우에는 즉시 시정조치를 하고 그 기록을 남겨야 한다. 또한 관리적인 측면에서 획득된 인증이 유효기간내에 심사가 이루어질 수 있는 시스템을 갖추어야만 디지털 포렌식 업무의 공신력이 대내외적으로 유지될 수 있다고 할 것이

2. 디지털 포렌식 프로세스간 연계시스템 구축

디지털 포렌식 프로세스에는 법률적 부분, 기술적 부분, 정책적(관리) 부분이 포함되어 있는데, 현재 대부분의 기관들은 기관의 규모에 따라 이러한 부분들을 업무상 분리하고 있거나 혼재시키고 있다. 디지털 포렌식 업무를 수행함에 있어서 이러한 분야간 관리책임이 구분되어 있게 되면, 서로 다른 분야의 업무특성에 대한 이해와 인식의 한계로 업무의 연계성을 확보하기 어려울 뿐만 아니라, 각각의 업무프로세스

723) David Watson/Andrew Jones, Digital Forensics Processing and Procedure; Meeting the Requirements of ISO 17020, ISO 17025, ISO 17001 and Best Practice Requirements, 2013, p.195.

에 대한 지침이나 매뉴얼이 있기 때문에 서로의 업무영역에서 준수해야 하는 사항에 있어서 충돌이 있을 수 있다. 마찬가지로 소수의 기술인력만으로 디지털 포렌식 업무를 수행하는 기관의 경우에는 법률적인 부분과 정책적인 부분에 대해서는 제대로 된 프로세스를 갖추어 대응하는데 한계가 있을 수 밖에 없다.

앞서 기술한 통합관리시스템이 전체적인 디지털 포렌식 프로세스에 대한 정책적인 측면과 절차적인 측면에서의 요구사항을 총괄적으로 관리하는 것이라고 본다면, 프로세스 연계시스템은 그러한 정책적·관리적 요구사항이 적용된 보다 세부적이고 구체적인 실무상 업무연계 프로세스라고 할 수 있을 것이다. 즉 디지털 증거를 수반하는 사건처리가 이루어지는 실무에서 이러한 법률적·기술적·정책적 분야가 체계적이고 유기적으로 연계될 수 있는 표준업무 프로세스를 개발하여, 서로의 업무에 대한 협조와 지원, 피드백이 가능한 시스템이 갖추어질 필요가 있다고 할 것이다.

가. 기술적 프로세스와 법률적 프로세스의 연계

1) 압수·수색의 적법성 확보를 위한 프로세스 연계

수사기관이 디지털 증거를 확보함에 있어서 압수·수색을 할 수 있는 법률상의 권한을 확보하는 것이 가장 우선되어야 한다는 것은 형사절차의 기본원칙이다. 하지만 디지털 증거에 있어서는 압수·수색 영장을 발부받았다는 것만으로 압수·수색의 적법성이 당연하게 확보되어지지는 않는다.

특히 우리의 형사절차에 있어서 디지털 증거의 압수·수색은 그 방법이 법률에 명문화되어 있기 때문에, 관련성 있는 것에 한한 선별압수가 원칙이고 일정한 예외적 사유에 한해 정보저장매체를 압수할 수 있고, 압수후 검색 및 분석과정에 피고인 등의 참여가 허용되어야 비로소 적법한 압수·수색이라 할 수 있다. 하지만. 디지털 증거의 대량성 및 네트워크 관련성으로 말미암아 사건과의 관련성 확인 및 선별이 용이하지 않은 상황에서 압수·수색현장에서 예외사유에 대한 판단의 적절성을 확보하기가 어렵기 때문에 영장의 범위를 초과할 개연성이 항상 존재한다고 볼 수 있다.

이와 같이 영장범위 내에서의 관련성 있는 증거에 대한 선별압수가 적법하게 이루어지기 위해서는 담당 수사관과 디지털 포렌식 조사관(분석관)간의 협의하에 압수·수

색 계획이 수립되어야 할 뿐만 아니라, 현장에 디지털 포렌식 조사관이 참석하여 직접 다양한 형태의 정보저장매체에 저장된 정보를 기술적으로 선별하여 복제할 수 있어야 한다. 또한 현장에서 선별 복제압수가 불가능하다는 판단을 함에 있어서 디지털 포렌식 조사관의 전문지식과 기술에 비추어 예외사유로서의 정당성을 확보할 필요가 있다. 디지털 기술에 문외한인 담당 수사관의 판단 만으로 예외사유로 보아 정보저장매체 자체를 압수하게 되면, 재판과정에서 예외사유로서 정당성을 확보하지 못함으로 인해 위법한 압수가 되어 증거능력 자체가 모두 배제될 우려가 있다.

이와 같이 디지털 증거에 대한 압수·수색의 적법성을 확보함에 있어서 법률상의 권한을 확보하여 형식적인 적법성을 갖추는 것은 수사실무 담당자 이지만, 압수·수색의 내용이 영장의 범위를 벗어나지 않게 함으로서 실질적인 적법성을 확보하는 것은 디지털 포렌식 조사관(분석관)이라 할 것이다. 따라서 디지털 포렌식 프로세스에 있어서 담당수사관에 의한 압수·수색 협조요청이 이루어져야 하고, 이에 따라 디지털 포렌식 조사관(분석관)이 사전 압수·수색 계획단계에서의 참여 및 현장 기술 지원을 할 수 있도록 시스템적으로 연계시키는 것이 압수·수색의 적법성을 유지하는데 필수적이라 할 것이다.

2) 디지털 증거의 증거능력 확보를 위한 프로세스 연계

디지털 포렌식 프로세스의 신뢰성은 디지털 증거의 증거능력을 뒷받침하는 가장 중요한 요소라고 할 수 있다. 즉 이미 법원의 판결을 통해 디지털 포렌식 프로세스의 절차적 측면에서의 무결성과 chain of custody는 디지털 증거의 증거능력을 판단하는 기본적인 요건이 되고 있다. 물론 구체적으로 디지털 포렌식 프로세스가 무엇이며 어느 단계에서부터 어느 단계까지를 프로세스안에 포함된다고 보는가에 대해서는 판결에 전혀 언급된 바가 없지만 대체적으로 수집, 선별, 분석, 제출까지를 포렌식 프로세스로 이해하고 있는 것으로 보여진다.

이러한 디지털 포렌식 프로세스의 절차적 요건과 달리 그 절차를 구성하는 기술적 요건과 관련한 판단기준은 법률의 개정 또는 법원의 판결변경에 의해 언제든지 변경·수정될 수 있다. 즉 법적 판단에 따라 기술적 요건이 달라질 수 있는 것이 디지털 포렌식 프로세스라고 할 수 있다. 따라서 법률이 디지털 증거능력의 인정요건으로서

무엇을 규정하고 있는가에 따라서, 그리고 그 법률을 적용하는 법원이 증거능력의 인정요건을 사건과 관련하여 구체적으로 어떻게 해석하고 있는가에 따라서 디지털 포렌식 프로세스의 구성적 측면 혹은 기술적 측면이 달라질 수 있다.

예로써 형사소송법 제313조 개정으로 "과학적 분석결과에 기초한 디지털 포렌식 자료에 의한 증명"이라는 규정이 신설됨으로서, 디지털 포렌식 자료의 공정하고 객관적인 산출 및 그 자료를 제출한 디지털 포렌식 조사관의 법정 증언이 요구될 수 밖에 없게 되었다. 이 경우 디지털 포렌식 자료가 신뢰할 수 있는 것인가 그리고 그 자료를 산출한 디지털 포렌식 조사관(분석관)이 해당 업무를 할 자격 혹은 능력이 있는가, 그리고 기술적 전문가가 어떻게 법정 증언을 효과적으로 해낼 것인가가 디지털 포렌식 프로세스안에서 증명되고 구현되어야 비로서 그 신뢰성을 확보할 수 있다고 할 것이다. 마찬가지로 판례가 디지털 포렌식에 의해 산출된 결과에 대해 사용된 디지털 포렌식 도구의 검증 여부를 문제삼거나, 분석결과를 제출한 디지털 포렌식 기관의 국제적 표준 적용 여부를 그 신뢰성의 판단요소로 제시하게 되는 경우에는, 디지털 포렌식 프로세스안에 도구 검증절차와 실험실(분석실)에 대한 국제표준의 인증을 갖추어야만 디지털 포렌식에 의해 산출된 결과의 신뢰성이 확보될 수 있다고 할 것이다.

이와 같이 디지털 포렌식 프로세스에 있어서는 법적 영역과 기술적 영역은 불가피하게 연결될 수 밖에 없지만, 이러한 법적 영역안에서 이루어진 판단기준을 기술적 영역에 적용될 수 있도록 하는 것은 디지털 포렌식 프로세스 전체에 적용되는 정책적 판단에 의해서 가능하다고 할 수 있다. 즉 법적 판단기준이 디지털 포렌식 기술에 자동적으로 적용될 수는 없는 것이고, 그러한 기술영역에 요구되는 자격·인증·표준 등이 무엇인가에 대한 판단이 필요하고, 경우에 따라서는 시스템을 새롭게 개발해야 하는 문제도 있기 때문에, 이를 디지털 포렌식 프로세스에 어떻게 적용할 것인가는 디지털 포렌식 기관의 정책적 결정을 요하는 것이라 할 것이다.

이와 같이 디지털 포렌식과 관련한 법적 근거와 판단이 적절하게 디지털 포렌식 업무에 피드백될 수 있고, 통합관리시스템을 통해 디지털 포렌식의 기술적 업무내용이 변경될 수 있는 연계시스템이 확보되는 경우, 디지털 증거에 대한 법적 신뢰가 보다 명확하게 확보될 수 있을 것이다.

나. 포렌식 업무 프로세스간 피드백 시스템

디지털 포렌식 프로세스는 기관별로 그 구성이 다를 수 있겠지만 일반적으로 준비 → 선별→수집→분석→추출→평가 및 해석→결과 보고서 제출→보존→법정 증언 순으로 생각해 볼 수 있다. 여기서 '준비·선별·수집'은 압수·수색절차로서 담당 수사관의 업무이지만 디지털 포렌식 기술의 지원을 기반으로 이루어지며, '분석·추출·평가 및 해석, 결과보고서 제출'은 디지털 포렌식 분석관의 업무이지만 수사관의 요청범위내에서 이루어지는 절차이다. 그리고 '보존과 법정증언'은 디지털 포렌식 분석관과 수사관의 협업을 통한 법적 절차라고 볼 수 있다. 즉 디지털 포렌식 프로세스에는 법적 절차와 기술적 절차가 오버랩 되어가면서 진행될 수 밖에 없고, 따라서 포렌식 분석관의 지원을 기반으로 해야 제대로 된 수사가 이루어질 수 있고, 또한 수사관의 명확한 요청과 지휘가 있어야 사건의 입증에 필요한 디지털 증거를 정확하게 산출해낼 수 있다고 할 것이다.

그런데 이러한 업무간 프로세스가 효율적으로 진행되면서도 정확한 결과를 산출해 내기 위해서는 one-way 방식이 아니라 업무간 피드백이 가능한 방식으로 구성되어야 할 것으로 생각한다. 즉 수사관은 자신이 요청한 디지털 증거에 관하여 제출된 분석결과를 검토한 후 포렌식 분석관에게 재분석을 요청할 수 있어야 하고, 포렌식 분석관이 분석업무 과정에서 수사관이 요청한 범위의 데이터는 아니지만 사건의 혐의를 입증할 수 있는 데이터를 확인한 경우에는 수사관으로 하여금 분석요청범위를 수정하거나 재분석요청을 하도록 요구할 수 있어야 하기 때문이다. 특히 사전 준비단계에서 디지털 포렌식 조사관(분석관)과의 협의 내지 지원하에 압수·수색이 진행되지 못한 경우에는 이와 같이 수사관과 분석관간의 업무간 피드백이 원활해야 보다 정확하고 신뢰할 수 있는 디지털 증거를 산출해낼 수 있다고 할 것이다.

다만 이와 같이 업무간 피드백이 이루어진 모든 절차와 과정이 업무 시스템상 기록으로 남아야 한다. 이러한 기록을 통해 디지털 포렌식 프로세스의 객관성과 염결성이 확보될 수 있으며, 또한 산출된 결과의 재현가능성도 담보할 수 있기 때문이다.

다. 포렌식 업무간 권한 통제시스템 확보

디지털 포렌식 프로세스 연계시스템을 구축함에 있어서 앞서 기술한 바와 같이 업무간 연계와 피드백이 중요한 만큼 각 업무간 통제시스템의 중요성도 인식할 필요가 있다. 즉 디지털 포렌식 프로세스에서 가장 중요한 것이 디지털 증거의 무결성 확보이기 때문이다. 업무의 연계성을 위해 각 업무에 대한 단계별 접근통제가 이루어지지 않게 되면 디지털 증거에 대한 무결성을 담보할 수 없고, 이는 디지털 증거의 증거능력의 배제로 이어질 수 밖에 없다.

디지털 포렌식 프로세스의 선순환적 연계시스템을 보장하면서도 디지털 증거의 무결성의 훼손을 방지하기 위해서는 각 업무 프로세스에 대한 접근권한을 명확히 설정하여 해당 사건의 담당 수사관과 디지털 포렌식 분석관 외에는 접근할 수 없도록 해야 한다. 그리고 사건 담당 수사관이라 해도 디지털 포렌식 분석관이 분석한 결과 또는 추출한 자료 외에 업무시스템상에 있는 분석대상 데이터 자체에 대한 접근은 차단되어야 할 것이다. 이는 고의가 아니더라도 기술에 문외한인 수사관의 과실이나 우연성으로 말미암아 분석대상 데이터의 변경이나 오염을 발생시킬 우려가 있기 때문이다.

제2절 주요 프로세스별 고려사항

1. 준비 및 수집단계

가. 적법절차 준수

디지털 포렌식 프로세스에 있어서 처음부터 마지막까지 가장 엄격하게 준수되어야 하는 원칙은 바로 적법절차이다. 즉 디지털 포렌식을 수반한 수사가 법률상 정당하게 확보된 권한에 의하지 않게 되면 수사 자체가 위법한 것이 되므로 디지털 포렌식도 신뢰할 수 없는 것이 된다. 또한 정당한 법률상 권한에 의해 확보된 디지털 증거에 대해 포렌식 프로세스가 진행되었다고 하더라도 디지털 포렌식 프로세스 자체가 증거법적 요구사항을 갖추지 못하게 되면 포렌식 프로세스 자체에 대한 신뢰성 뿐만 아니

라 디지털 증거에 대한 신뢰성까지 확보되지 못하는 결과가 초래될 수 있다.

따라서 디지털 포렌식 프로세스에 있어서 적법절차의 준수는 법적 영역을 담당하는 수사관 뿐만 아니라 기술적 영역을 담당하는 디지털 포렌식 분석관(조사관)들도 직접적인 책임을 부담할 수 밖에 없다고 할 것이다. 즉, 디지털 포렌식 업무에 관여하는 사람들은 관련 법률상 요건을 준수해야 할 뿐만 아니라 형사사법시스템상 요구사항을 이해해야 하고, 디지털 증거와 관련한 증거법적 요구사항의 변화 - 특히 판결에 의해 제시되는 -를 정확히 이해하고 업무에 적용해야 한다.

이와 같이 디지털 포렌식 업무와 관련하여 적용되는 법적 요구사항 및 기준들 즉, 법률상·절차상 요건들이 포렌식 업무에 적절히 반영되어야 포렌식 프로세스의 적법성에 문제가 발생하지 않을 수 있다고 할 것이다. 다만 이러한 법률상 요건들을 포렌식 업무를 수행하는 개개인들이 숙지하고 준수하는 것도 중요하지만, 이러한 적법성 준수요건을 개인의 책임에 맡기기 보다는 디지털 포렌식 운용 시스템안에 법률상 요건들이 적용되어 구현될 수 있도록 설계되어 시행될 필요성도 고려할 가치가 있다고 생각한다. 즉 디지털 포렌식 프로세스 통합시스템 설계 단계에서 법적 요구사항이나 기준들을 적용시킴으로써 법적 요구사항과 기술적 요구사항이 하나의 프로세스로 함께 진행될 수 있도록 하는 것도 검토해볼 가치가 있다고 할 것이다.[724] 이와 같이 시스템을 통해서 디지털 포렌식 업무의 적법성이 확보될 수 있도록 하는 것이 사람에 의한 오류의 위험을 최소화할 수 있는 방안이라 할 수 있을 것이다.

나. 포장과 이송 및 보존

디지털 증거는 최대한 오염되지 않는 방식으로, 그리고 표준화되고 승인된 디지털 포렌식 절차에 따라 증거를 수집해야 한다. 수집된 디지털 증거를 안전하게 보존한 상태에서 분석실로 이송할 때는 전자기적 차단이 가능하도록 포장된 상태로 이송되어야 한다.

디지털 포렌식 기관은 이송된 디지털 증거가 적절하게 포장되어 봉인된 상태인지,

---

724) 이는 데이터 처리시 설계단계에서부터 기술적으로 프라이버시를 보호할 수 있는 구조를 갖춤으로써 처음부터 프라이버시를 보호하고자 하는 개념인 privacy by design에 착안한 것으로서, 디지털 포렌식 프로세스시스템에 있어서도 설계단계에서 기술적으로 적법절차를 준수할 수 있도록 하는 legality by design이 충분히 가능할 것으로 생각된다.

봉인 이전단계에서의 증거물 이동 기록(장소적 이동, 인적 이동, 전자적 이동 등)이 표시된 연속성 확인 표지가 있는지 확인해야 한다. 기관에 접수된 디지털 증거가 보관의 연속성에 대한 확인이 불가능한 경우에는, 해당 증거물의 접수를 거부하거나 불가피한 경우에는 그 사유를 명확히 기록하고 접수단계에서부터 새로운 연속성 레이블을 작성하여 부착해야 한다.[725]

디지털 포렌식 기관은 봉인된 증거물을 접수한 후 증거물 로그에 기록하고 이동 로그를 갱신하여 증거물을 송달한 사람으로부터 기관에의 접수까지의 증거물 이동내역을 기록해야 한다. 그리고 접수시 증거물의 포장상태 및 연속성 레이블 또는 훼손부분 등에 대한 정확한 확인이 가능하도록 촬영하여 증거물과 함께 시스템에 등록해야 한다.[726]

2. 분석 및 추출 단계

가. 디지털 포렌식 분석관(조사관)의 자격 및 전문성 유지

1) 자격 및 능력 검증

디지털 포렌식은 업무 특성상 전문적인 지식과 기술을 요하는 분야이다. 따라서 디지털 포렌식 분석실(연구소)에 대한 국제표준인 ISO 17025는 포렌식 분석관(조사관)이 해당 업무수행에 적합한 자격을 갖추고, 해당 자격에 대한 증빙기록을 보유할 것을 요구하고 있다.[727]

포렌식 분석관(조사관)의 자격은 주기적으로 검토 및 평가되어야 하고, 만약 법원에 제출한 디지털 포렌식 분석결과가 문제가 있는 것으로 판단되는 경우에 해당 포렌식 분석관에 대한 재평가를 할 필요성이 제기될 수 있다.[728]

포렌식 분석관은 포렌식 업무 수행에 필요한 전문기술에 대한 인증을 확보하는 것이 바람직하며, 새로운 기술자격을 확보한 경우 해당 기관은 포렌식 분석관이 그 자격을 이용하여 사건을 처리할 수 있는 기술적 자격을 갖추었는지를 확인해야

725) David Watson/Andrew Jones, op,cit.,p.386.
726) ibid.
727) David Watson/Andrew Jones, op,cit.,p.195.
728) ibid.

한다.[729]

2) 교육훈련

디지털 포렌식 업무를 수행하는 기관은 포렌식 분석관(조사관)이 갖추어야 할 필수적인 자격을 결정하고, 각 분석관(조사관)들이 이러한 자격을 성취하고 유지할 수 있는 훈련을 제공해야 한다. 즉 기관은 포렌식 분석관(조사관)들이 본인의 능력과 기술을 개발하고 유지할 수 있도록 충분한 교육훈련프로그램을 개발하여 제공해야 한다. 특히 디지털 포렌식 분야는 그 기술적 변화가 빠르기 때문에, 포렌식 분석관들이 그러한 기술을 적시에 습득하여 포렌식 업무에 적절히 대응할 수 있도록 내외부적으로 충분한 교육훈련기회들이 제공되어야 한다. 이러한 교육훈련을 통해서 포렌식 분석관(조사관)들이 포렌식 업무수행에 적합한 기술과 지식, 그리고 자격과 경험을 갖추도록 해야 한다. 그리고 포렌식 분석관(조사관)은 이러한 교육훈련을 통한 자신의 지속적인 전문성 개발 및 교육훈련 기록 그리고 포렌식 업무수행 경험 기록 등을 유지함으로써 법정에서 전문가 자격에 대한 입증요구에 대비해야 한다.

3) 포렌식 분석관으로서의 의무와 책임

가) 포렌식 분석관으로서의 인식제고

모든 포렌식 분석관(조사관)은 업무프로세스와 관리시스템을 준수하는 것이 형사절차에 있어서 어떠한 의미를 갖는지를 이해하고 그 중요성을 인식해야 한다. 만약 이러한 업무 프로세스와 관리시스템을 준수하지 않았을 경우에 발생할 수 있는 잠재적인 결과가 전체 포렌식 업무 뿐만 아니라 기관 자체에 대한 신뢰도를 하락시킬 수 있다는 점을 명확히 이해하여야 할 것이다.

나) 객관성과 공정성 확보

디지털 포렌식 분석관들은 해당 업무를 수행함에 있어서 객관적이고 공정한 자세를 유지할 책임이 있다고 할 것이다. 즉 포렌식 분석관(조사관)들이 디지털 증거를 어떻게 분석하고 추출하고 해석하는가에 따라 실체적 진실이 달라질 우려가 있기 때문에, 포렌식 분석관(조사관)들은 자신의 전문적 지식과 기술에 기초한 판단이 객관성을

729) ibid.

유지하도록 노력해야 한다.

따라서 포렌식 분석관들은 편견이나 이해의 충돌 또는 다른 사람으로부터의 부당한 영향력 없이 결론을 산출해낼 수 있어야 한다. 만약 포렌식 분석관 본인이 해당 사건과 이해관계 등이 있는 경우에는, 포렌식 프로세스 전체를 관리하는 부서에 이러한 사실을 고지하고, 해당 업무에서의 배제를 요청할 의무[730]가 있다고 할 것이다. 하지만 포렌식 분석관 스스로 이러한 사실을 고지할 것을 항상 기대하기는 어려우므로, 디지털 포렌식 프로세스 관리자는 동료심사를 통해 포렌식 분석관이 산출한 업무결과를 상호검증할 수 있는 시스템을 갖추거나 별도의 감독체계를 수립해야 할 것으로 생각된다. 이러한 상황에 대비하여 디지털 포렌식 기관은 통합관리시스템안에 이해관계 충돌방지 지침[731]을 도입하는 것도 고려해 볼 수 있다고 할 것이다.

다) 윤리의무

디지털 포렌식 분석관은 자신의 경험과 지식을 바탕으로 분석결과를 진지하게 검토하고, 건전한 판단력으로 해당 사안에 대한 결론을 도출해야 한다. 그리고 결론을 도출한 후 자신의 능력범위내에서 최대한 정확하게 보고서를 작성, 제출함으로써 해당 사건의 맥락에서 관련자들에게 그 보고서내의 사실이 이해되고 적용할 수 있도록 해야 한다. 이러한 기능을 수행함에 있어서 포렌식 전문가는 해당 분야에서 널리 인정되는 고도의 전문가 윤리원칙에 부합하는 방식 및 절차를 준수해야 한다.[732]

나. 디지털 포렌식 도구 및 방법론

디지털 포렌식 업무를 수행하는 기관은 대부분 자체적으로 도구를 개발하기 보다는 이미 상용화되어 검증된 도구를 사용하기 때문에 일반적으로 표준화된 방법을 사용하고 있다고 볼 수 있다. 즉 도구의 사용설명서안에 정의된 절차, 널리 인정되는 검증절차, 그리고 관련표준을 따르는 경우, 디지털 사건처리 프로세스에 관한 표준방법으로 인정되므로, 디지털 포렌식 기관은 이러한 상용도구들을 선호하는 경향이 있다. 따라서 대부분의 경우 디지털 포렌식 도구의 사용이 법원에서 인정을 받으며, 다른

730) David Watson/Andrew Jones, op,cit., p. 29.
731) David Watson/Andrew Jones, op,cit., p.180.
732) David Watson/Andrew Jones, op,cit., p.516.

자격있는 포렌식 분석관들도 포렌식 도구를 사용한 결과를 재현할 수 있는 것으로 입증하고 있다.[733]

하지만 새로운 포렌식 도구를 사용하는 경우에는 기관의 포렌식 도구에 대한 기준을 적용하거나 이중도구 검증을 통해서 해당 도구의 유효성을 검증해야 한다. 즉 새로운 도구를 설치하거나 기존 도구의 새로운 버전을 설치하는 경우, 표준 시험용 사건을 사용하여 테스트 한 후 표준시험 실시 결과를 예상결과와 비교하여 기존 도구에 의한 결과와의 동일성 여부를 확인해야 한다.[734]

디지털 포렌식 기관은 포렌식 업무에 사용하는 하드웨어와 소프트웨어의 모든 구 버전을 복구할 수 있어야 하므로, 표준빌드를 복구할 수 있도록 소프트웨어와 하드웨어의 모든 버전을 보유해야 한다. 이는 증거의 수집 또는 처리와 관련하여 문제나 오류가 발생한 경우에 이것이 사건처리에 사용한 도구가 이미징 또는 분석에 있어서 문제를 유발한 원인이 아님을 증명하기 위한 것이다.[735]

3. 결과물 제출 단계

가. 결과물에 대한 검증

디지털 포렌식 기관은 기본적으로 포렌식 분석관(조사관)에 의해 산출된 최종 결과물이 기관내 품질관리 프로세스를 준수하였으며, 결과물이 산출되기까지 포렌식 분석관(조사관)에 의해 행해진 모든 조치들이 정확하게 기록되었지의 여부를 검토함으로써 산출된 결과에 대한 신뢰성을 담보해야 한다. 만약 이러한 검토과정에서 결과물에 대한 수정이 요구되는 경우에는 명확하게 그 이유를 기재하고 수정사항이 있었다는 것을 명기해야 할 것이다.

포렌식 분석관(조사관)에 의해 산출된 결과물에 대한 검증방식으로는 분석팀과 별도의 검증팀을 운영하는 방식과 동일 부서내 동료간 상호검증 방식, 또는 동일 분석관에 의한 결과물 재산출에 의한 검증방식 등이 있을 수 있다. 최종적으로 산출된 디지털 포렌식 자료에 대한 신뢰정도는 후자의 방식으로 갈수록 떨어질 수 밖에 없다고 할

733) David Watson/Andrew Jones, op,cit., p.197.
734) David Watson/Andrew Jones, op,cit., p.198.
735) David Watson/Andrew Jones, op,cit., p.384.

것이다.

결과물에 대한 검증에 있어서는 사용된 기술적 방법, 정확성, 근거 등에 대한 명확한 심사 뿐만 아니라 분석관이 기록한 절차에 따른 재현가능성 및 동일한 결과의 산출 여부 등이 확인되어야 할 것이다.

나. 보고서 작성

디지털 포렌식 분석관은 해당 업무를 처리하는 과정 중에 자신이 취한 모든 조치를 기록해야 하고, 이 기록을 토대로 최종적으로 산출된 결과에 관한 보고서를 작성하게 된다. 포렌식 조사관이 업무과정에서 일정한 조치를 취한 경우 그와 동시에 기록이 이루어져야 한다.

보고서 작성은 디지털 포렌식 프로세스의 결론에 해당하는 부분으로서 최종적으로 디지털 포렌식 프로세스의 신뢰성을 입증하는데 근본적으로 중요한 역할을 담당한다고 볼 수 있다. 보고서 작성 양식은 기관에 따라 차이가 있지만, ISO 17025의 요건과 관련 증거규칙의 요건에 맞추어 작성되어야 한다.[736]

디지털 포렌식 보고서가 갖추어야 할 요건은 다음과 같이 제시될 수 있다.

“ⅰ) 형식성 : 해당 기관에서 정한 형식을 준수해야 한다.

ⅱ) 간결성 : 전체적인 내용을 간결하게 기술해야 한다.

ⅲ) 정확성 : 발견 또는 관측한 사실을 명확하게 기록해야 하고, 처리과정에서 얻은 정보는 가능한 한 많은 출처에 의해 검증해야 한다. 보고서에 기술된 내용은 해당 사건의 증거로서 입증가능 해야 하기 때문에 분석관의 개인적인 의견이나 판단을 기술해서는 안된다.

ⅳ) 이해 용이성 : 사실인정자들 - 판사 또는 배심원-이 쉽게 이해할 수 있는 용어로 작성해야 한다. 포렌식 분석관이 기술적으로 상세하고 완전한 내용의 보고서를 작성해도 이를 읽는 사람이 이해가 불가능한 경우에는 무용지물이 될 수 있다.

ⅴ) 완전성 : 보고서는 최종적으로 산출한 결론을 설명하는데 필요한 모든 정보를 수록해야 한다. 다만 데이터 용량의 증가로 보고서의 양이 과하게 늘어나거나

736) David Watson/Andrew Jones, op,cit.,p.514.

무분별한 세부사항 제공으로 증거파악이 어려울 수 있으므로, 사건과 관련된 증거를 정확하게 파악하여 제시하는 것이 중요하다.

vi) 신빙성 : 보고서를 읽는 사람이 이해할 수 있는 언어로 작성되어야 하고, 충분히 세부적 설명을 통해 그 내용을 신뢰할 수 있도록 해야 한다."[737]

그리고 포렌식 분석관이 작성한 보고서는 법정에 제출하기 전에 기관내 다른 분석관이 검토함으로써 보고서의 의견 및 결론이 건전하고, 기초가 된 사실에 활용된 도구와 방법의 적합성 여부가 검증될 필요가 있다. 이와 같은 분석결과에 대한 교차검증을 통해 디지털 포렌식 자료에 대한 신뢰성이 보다 더 확고히 증명될 수 있다고 할 것이다.

또한 디지털 포렌식 업무가 일정한 품질수준을 갖추어 행해졌을지라도 그러한 업무에 의해 산출된 결과를 기록한 보고서 자체의 품질이 갖추어지지 못하면 포렌식 업무 자체에 대해서 부정적인 평가가 행해질 수 밖에 없다.[738] 즉 법정에서는 제출된 포렌식 보고서만으로 디지털 포렌식의 신뢰성 및 디지털 증거의 증거능력을 판단하기 때문에 보고서의 품질이 수준을 유지할 수 있도록 관리적인 측면에서 기준을 마련해야 할 것이다.

4. 법정 증언단계

가. 포렌식 분석관에 의한 법정 증언 준비

법정에 제출된 디지털 포렌식 자료에 대한 포렌식 분석관의 증언의 신뢰성은 바로 디지털 증거의 신뢰성으로 직결되기 때문에, 디지털 포렌식 분석관은 법정증언을 위한 역량을 갖추어야만 한다.

디지털 포렌식 분석관이 제출한 자료가 법정에서 증거로 제시되는 경우 포렌식 분석관은 반대 당사자에 의한 교차심문의 대상이 되기 때문에, 포렌식 분석관은 자신이 제출한 디지털 포렌식 보고서가 해당 기관의 통합관리시스템내에 설정된 표준운영절차에 따라 작성된 것일 뿐만 아니라, 법규정과 증거법상 원칙의 준수하에서 일관되

737) ibid.
738) ibid.

고 표준화된 프로세스를 통해서 산출된 것이며, 작성자가 충분한 경험과 전문적 지식을 가진 사람이며, 충분히 검증된 도구를 사용하여 산출된 것이라는 점을 논리적으로 설명할 수 있어야만 한다.

하지만 디지털 포렌식 분석관은 기술분야의 전문가이기 때문에 자신이 행한 기술적 조치들이 법률적으로 어떠한 의미를 갖는지에 대하여 설명하는데는 한계가 있을 수 밖에 없다. 즉, 포렌식 업무를 수행함에 있어서 취했던 기술적 조치에 대한 입증에 초점을 맞추다 보면 우연치 않게 그로 인한 법적 절차의 하자가 드러날 가능성도 배제하기는 어렵다고 할 수 있다.

따라서 디지털 포렌식 기관은 포렌식 분석관이 법정증언을 해야 하는 경우에는 기관내 법무담당자와의 협력하에 법정에서 요구하는 정확한 증언 형식에 맞추어 본인이 산출한 결과를 가장 적절하게 증언할 수 있는 방식을 교육받을 필요가 있다고 할 것이다.[739]

나. 효과적인 증언 방식

디지털 포렌식 기관은 포렌식 분석관이 증인으로서 증거의 존재 및 유효성에 대해 증언을 할 수 있고, 그 발견과정과 증거보관의 연속성이 유지되었음을 기술적으로 설명할 수 있으며, 그러한 과정 중에 증거의 훼손 및 오염이 없었음을 증명할 수 있도록 해야 한다.[740]

하지만 디지털 포렌식에 대한 기초적인 지식이 없는 판사나 배심원들은 그러한 설명을 들어도 제대로 이해하지 못하는 경우가 있을 수 있다. 이러한 경우 법원이 허용하는 한도내에서 시각적 보조도구 - 애니메이션, 도표, 사진, 그림 등 -를 활용하여 판사나 배심원이 이해하기 힘든 내용을 쉽고 명확하게 전달하는 방식을 제공할 필요가 있다.[741]

---

739) David Watson/Andrew Jones, op,cit.,p.516.
740) David Watson/Andrew Jones, op,cit.,p.511.
741) David Watson/Andrew Jones, op,cit.,p.518.

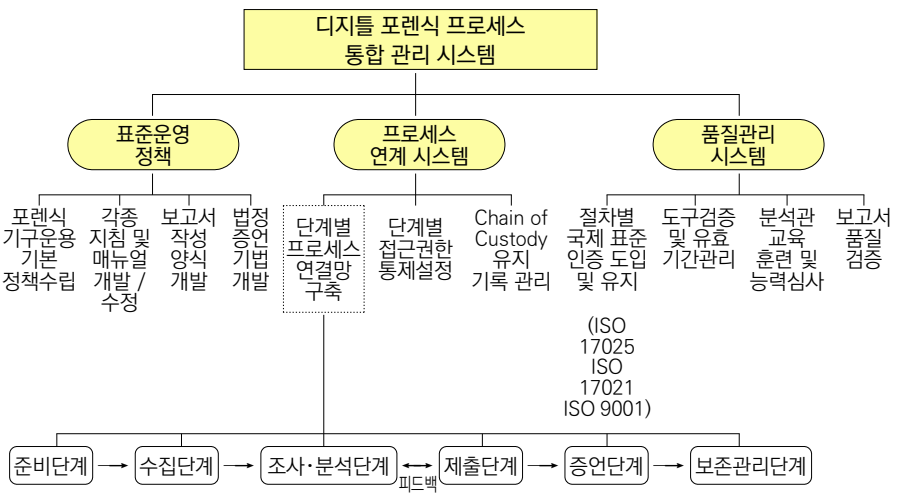
제3절 디지털 포렌식 프로세스 통합을 위한 정책적 제언

1. 디지털 포렌식 프로세스 통합을 위한 모델 프레임

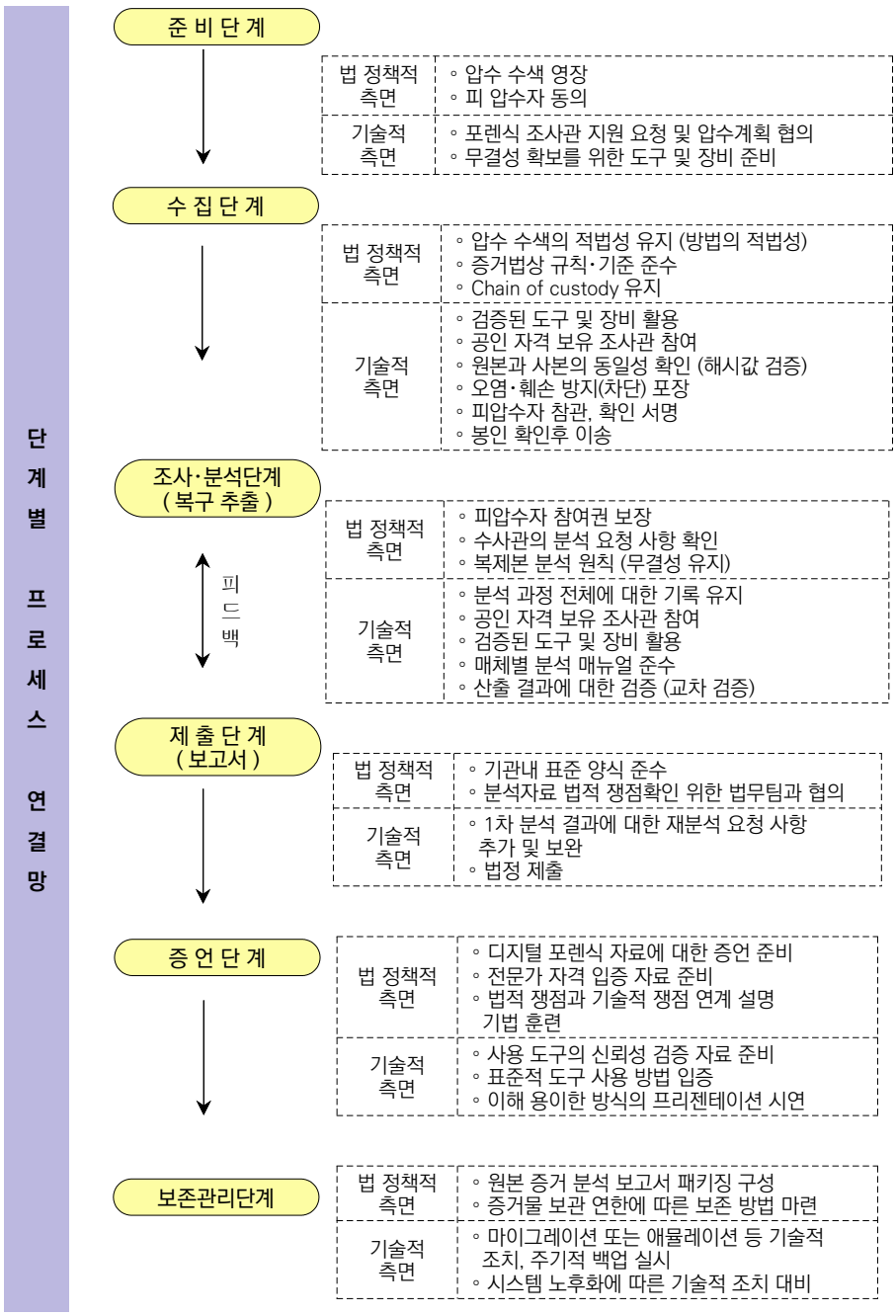
디지털 포렌식 업무를 수행하는 기관에서 디지털 포렌식과 관련한 모든 절차- 법적, 기술적 - 가 일관된 프로세스안에서 진행될 수 있도록 하기 위해서는 이를 포괄하여 관리할 수 있는 통합관리시스템이 필요하다고 할 것이다.

그리고 이러한 디지털 포렌식 프로세스 통합관리시스템을 통해서 포렌식 업무품질 유지, chain of custody를 통한 증거의 무결성 담보, 그리고 궁극적으로 디지털 포렌식 자체에 대한 신뢰성을 확보하기 위해서는 품질관리시스템, 프로세스 연계시스템, 표준운영정책시스템이 하위범주를 구성할 필요가 있다고 생각한다. 통합관리시스템이 디지털 포렌식 프로세스 통합을 위한 정책적·관리적 프레임이라고 한다면, 실무적인 포렌식 프로세스 통합은 프로세스 연계시스템을 통해서 확보될 수 있다고 할 것이다.

즉 프로세스 연계시스템하에서 단계별 프로세스 연결망을 구축하는 것이 그것인데, 준비 단계, 수집 단계, 조사 및 분석 단계, 제출 단계, 증언 단계, 보존 및 관리 단계를 선순환적 피드백이 가능하도록 구성하는 것이다. 이러한 전체적인 프레임을 좀더 구체적으로 제시하면 아래의 그림과 같다.



[그림 20] 디지털 포렌식 프로세스 통합관리시스템 모델 프레임



[그림 21] 단계별 프로세스 연결망내 단계별 표준요구사항

2. 디지털 포렌식 프로세스 통합모델 구축을 위한 제언

앞에서 그림으로 제시한 바와 같은 통합모델 프레임을 통해서 디지털 포렌식 프로세스가 기술적으로 뿐만 아니라 법적으로도 신뢰성을 갖기 위해서는 부분적으로 선결되어야 하는 몇가지 과제들이 남아 있다. 앞장에서 이미 기술하고 있는 내용들이므로 정책적 제언의 수준으로 정리해 보고자 한다.

가. 법과학적·기술적 관점에서의 제언

1) 디지털 포렌식의 표준화에 대한 요청

디지털 포렌식은 무형의 불가시적 증거를 법과학적 도구를 사용하여 유형의 가시적 증거로 전환함으로써 발생한 사실관계를 규명하고 증명하는 기술과 절차로서, 그 기술적·절차적 정확성이 담보되지 않는 한 디지털 증거에 대한 신뢰는 확보될 수 없다고 할 것이다. 그런데 전통적인 법과학 분야와는 다르게 디지털 포렌식은 디지털 기술의 빠른 변화에 대응하지 않고서는 증거탐색 및 추출 자체가 불가능할 수 있기 때문에 항상 최첨단의 기술을 습득하고 적용해야만 한다. 더욱이 디지털 증거가 존재하는 매체의 유형이 다양해짐에 따라 디지털 포렌식 도구 역시 다양해 질 수 밖에 없다. 하지만 이와 같이 빠르게 그리고 다양하게 변화하는 디지털 포렌식 기술 및 법과학적 전문지식이 법적 판단의 근거가 되기 위해서는 그것이 과학적으로 타당하고 신뢰할 수 있는것인가에 대한 증명이 전제되어야 한다.

현재 디지털 포렌식 업무를 수행하는 기관들은 대부분 기관 업무의 특성과 필요에 따라 개별적으로 상용화된 디지털 포렌식 도구를 구입하여 사용하거나 자체 개발한 도구를 사용하고 있다. 그런데 이러한 개별적인 포렌식 도구들과 그러한 도구를 활용하는 방법 등의 정확성 및 신뢰성에 대해서는 공인된 검증절차도 없고, 개별적으로 검증할 수 있는 표준적인 기준도 현재로서는 마련되어 있지 않기 때문에 디지털 포렌식에 수반되는 디지털 증거에 대한 법적 허용기준은 엄격할 수 밖에 없고, 제한적일 수 밖에 없다.

따라서 디지털 증거에 대한 신뢰를 뒷받침할 수 있는 디지털 포렌식이 법정에서 신뢰할 수 있는 기술과 절차로서 허용되기 위해서는 디지털 포렌식 분야에 적용가능

한 국제적 표준에의 인증, 포렌식 프로세스에 대한 표준적인 지침의 활용 등이 논의되는 것은 필연적이라 할 수 있다.

현재 미국, 영국, 독일, EU 등 디지털 포렌식에 있어서 앞선 시스템을 보유하고 있는 주요 국가들의 디지털 포렌식 기관들은 대부분 국제표준인 ISO/IEC 17025 인증을 확보하고 있거나, 인증확보를 위해 노력하고 있다는 것을 보여주고 있다. 즉, 범죄현장에서부터 법정에 이르기까지 전체 포렌식 프로세스에 걸쳐서 일관되고 신뢰할 수 있는 증거를 유지하기 위해서는 포렌식 업무에 있어서 ISO/IEC 17025를 확보해야 할 뿐만 아니라 관련한 다른 표준도 확보하는 것이 포렌식의 기본정책임을 강조하고 있다. 따라서 각 국가의 주요 기관에서 제시하고 있는 디지털 포렌식 모범실무지침 또는 가이드라인에 있어서도 ISO 인증의 필요성과 중요성이 기술되어 있는 것을 볼 수 있다.

국내 디지털 포렌식의 현실적 여건에 비추어 볼 때 디지털 포렌식을 담당하는 핵심기관들 조차 ISO 인증이 용이하지는 않은 것으로 보인다. 하지만 디지털 포렌식에 있어서 기술적·절차적 표준을 마련하고자 하는 노력은 앞으로 더욱 증가할 수 밖에 없는 디지털 증거의 현실적 필요성에 비추어 볼 때, 그리고 형사소송법 개정으로 디지털 포렌식 자료에 대한 정확성 및 신뢰성에 대한 입증을 요하는 법적 기준에 부합하기 위해서는 절대적으로 필요한 작업이라 할 것이다.

나. 디지털 포렌식 도구 검증절차 마련

디지털 기술이 발전함에 따라 디지털 포렌식 도구의 개발속도가 빨라지고, 도구의 유형도 다양화되어 가고 있는 것이 현실이다. 즉 디지털 포렌식 분야에 있어서 최첨단 기술을 확보하지 않고서는 급속히 발전하는 디지털 기술에 대응하여 정확한 결과를 산출해내기 어렵기 때문이다. 그런데 다양하게 개발되어 사용되고 있는 디지털 포렌식 도구가 그 기능적 요구사항에 부합하게 작동하고, 정확한 결과를 산출한다는 것을 테스트하고 공식적으로 확인해 줄 수 있는 절차가 없기 때문에, 국제적으로 검증된 몇몇 도구를 제외하고는 언제든지 법정에서 그 도구의 정확성 및 신뢰성을 문제삼을 수 있고, 그에 의해 산출된 디지털 증거의 신뢰성에 대해서도 이의가 제기될 수 있다. 즉, 새로운 기술이 비기술적 과학분야에서 인정되고 있는 포괄적인 리뷰와 심사없이

포렌식 분야에 적용되고 있기 때문에 지속적으로 신뢰성의 문제가 제기될 수 밖에 없다고 할 것이다.

디지털 포렌식 도구가 법과학적으로 타당한 도구가 되기 위해서 갖추어야 할 요건으로는, "첫째, 문제해결방법과 예상결과를 명확하게 설명할 수 있는 알고리즘을 갖추어야 한다는 것이고, 둘째, 해당 도구에서 실행될 모든 기능이 예측가능해야 하는 것이고, 셋째, 기능이 안정적으로 반복될 수 있으며 허용가능한 오류수준이 정의되어야 하며, 넷째, 분석도구의 가장 중요한 기능으로서 특정 테스트 환경 뿐만 아니라 같은 유형의 다른 도구로 해당 분석도구의 결과를 검증할 수 있는 기능을 갖추어야 한다는 것이다."[742]

그런데 상용도구의 개발이 증가함에 따라 저작권과 특허 문제로 소스코드가 비공개됨으로써 도구검증에 사실상 한계가 있다는 비판이 제기되고 있다. 이는 해당 도구를 사용하고자 하는 국가기관이 공개적으로 검증하는 것이 어렵거나 불가능하다는 것을 의미하는 것이라 할 수 있다. 따라서 국가기관에서 사용하고자 구입하는 상용도구에 한해서는 최소한 국내 또는 국외의 공신력 있는 기관으로부터 검증을 받았다는 인증을 보유하고 있을 것을 요하는 것이 바람직하며, 그것이 검증되지 않은 도구의 사용으로 인해 발생할 수 있는 실체적 진실의 왜곡과 그로 인한 형사절차의 염결성 훼손의 위험을 방지하는 방안이 될 것이다. 그리고 상용도구와 마찬가지로 기관의 업무특성에 적합한 고유한 요구사항을 반영하기 위해 자체 개발한 포렌식 도구도 반드시 국내 공신력 있는 검증 기관으로부터 그 정확성 및 신뢰성에 대한 검증을 받을 것이 요구된다고 할 것이다.

이와 같이 디지털 포렌식 도구를 검증함에 있어서는 그 기술적 요구사항의 정확한 구현 및 산출결과의 정확성에 대한 확인도 중요하지만, 완벽한 도구란 불가능하기 때문에 도구에 내재된 결함 및 결과산출에 있어서의 오류율이 결과의 신뢰성을 담보하는데 있어서 용인가능한 수준인지에 대한 확인도 필요하다고 할 것이다.

현재 우리의 경우에는 디지털 포렌식 도구를 검증할 수 있는 공신력 있는 기관은 없으며, 기관의 필요에 따라 개별적으로 외부 디지털 포렌식 전문가에게 의뢰하여 도구검증을 실시하거나 외부에 의뢰하여 제작한 도구를 기관이 자체적으로 검증하는

742) 래리 다니엘/라즈 다니엘, 포렌식 전문가와 법률가를 위한 디지털 포렌식, 2012, 44-46면.

수준에서 신뢰도 측정이 이루어지고 있다. 하지만 앞서 기술한 디지털 포렌식 전문가 인터뷰에서도 볼 수 있듯이 디지털 포렌식 도구를 실무에서 사용하고 있는 분석관들은 사용하고 있는 도구가 정확한 결과를 산출한다는 확신을 갖고 업무를 하기 위해서는 도구에 대한 공식적인 인증이 반드시 필요하다는 입장을 나타내고 있다. 그리고 디지털 포렌식 도구에 대한 인증을 통해 디지털 포렌식의 법적 신뢰성을 확보하기 위해서는 민간기구 보다는 정부기관의 주도하에서 포렌식 도구에 대한 인증체계를 갖추는 것이 필요하다는데 의견이 모아졌다.

이러한 상황에 비추어 볼 때 미국 국립표준기술연구소(NIST)의 CFTT 프로젝트를 모델로 삼아 디지털 포렌식 도구의 검증방법론을 개발하고, 도구에 대한 공식적인 테스트와 테스트 결과를 공개함으로써, 도구에 대한 공적인 신뢰를 제공하는 방식을 도입하는 것도 고려해보는 것도 바람직하다고 할 것이다.

다. 디지털 포렌식 전문가에 관한 기술적·법적·윤리적 기준 확립

디지털 포렌식에 대한 법적인 신뢰를 부여할 수 있는 또 다른 판단기준은 그 업무에 적합한 전문적인 지식과 기술을 가진 사람에 의해서 행해졌는가이다. 디지털 포렌식 전문가는 디지털 증거를 적절하게 수집하고 무결하게 보존하며, 정확하고 효율적으로 분석하고, 분석된 결과가 법적인 입증가치를 가질 수 있도록 해석할 수 있어야 한다. 이를 단순히 디지털 포렌식 도구의 매뉴얼을 운용할 수 있다는 것만으로는 이해하게 되면 디지털 증거를 분석하는 과정에서 증거의 훼손이 발생하거나 보관의 연속성이 단절될 수 있으며, 더 나아가 산출된 결과에 대한 잘못된 해석으로 유무죄 입증에 치명적 오류를 범하는 문제가 발생할 수도 있다.

적어도 형사절차에 수반되는 디지털 포렌식 업무를 수행하고자 하는 사람은 해당 공학분야의 학위, 디지털 기술의 조사에 적용할 수 있는 이론과 기술 및 절차를 증명할 수 있는 지식과 능력, 현장에서의 경험 또는 출판물을 통한 디지털 증거분야에서 전문가로서 동료에 의한 승인, 디지털 증거에 대한 형사사법시스템상 요구되는 사항들과 절차들에 대한 지식과 경험[743] 등이 요구된다고 할 수 있다. 즉 디지털 포렌식에

743) ENFSI, Guidelines for Best Practice in the Forensic Examination of Digital Technology, 2009, p.7.

서 요구되는 전문가의 자격은 디지털 포렌식에 관한 전문적인 기술교육을 받았다는 자격 뿐만 아니라 디지털 증거분석 경력, 포렌식 절차에 대한 특별한 전문지식을 갖고 있어야 하는 것이다.

현재 우리의 디지털 포렌식 분야에서 포렌식 전문가의 전문성을 검증할 수 있는 국가 차원의 기구는 마련되어 있지 않으며, 다만 학회가 중심이 된 국가공인 민간자격 제도로서 디지털 포렌식전문가 자격시험이 유일한 전문가 인증방법이 되고 있다. 이 시험이 시행되고 현재 실무에서 디지털 포렌식 업무를 수행하는 대다수의 분석관들이 자격증을 취득하고 있지만 그것이 법정에서 디지털 포렌식 전문가로 인정받는 유일한 수단이 아니기 때문에, 이 자격증은 디지털 포렌식 전문가로서 갖추어야 할 필요조건이지 충분조건이라고 볼 수는 없다.

비록 민간자격증이기는 하지만 디지털 포렌식 전문가 자격제도를 통해 디지털 포렌식업무를 수행하는 사람의 기본적인 자격에 대한 입증은 가능하게 되었다는 점에서 다행이라 할 것이다. 다만 국가공인이기는 하지만 전문가 자격을 부여하기 위해 요구하고 있는 자격이나 시험내용 등이 관련분야의 광범위한 승인이나 공인된 기준 없이 주관 기관 자체적으로 개발한 내용으로 구성되어 있기 때문에 그 자격증을 신뢰하지 못하는 경우도 있음을 볼 수 있다.

따라서 국가에서 포렌식 전문가 인증위원회(가칭)를 두고 디지털 포렌식을 포함한 각 포렌식 분야별 전문가로서 갖추어야 할 기술적, 법률적, 윤리적 기준을 표준화된 항목으로 구체적으로 정립하고, 각 분야별 민간자격증을 부여하는 기구들로 하여금 최소한 포렌식 전문가 인증위원회에서 제시한 표준항목들에 대한 검증시스템을 갖추도록 하는 것이 자격증에 대한 공신력을 제공함과 아울러 자격증을 소지한 사람에 대한 법과학 전문가로서의 공적인 신뢰를 확보하는데도 도움이 될 것으로 생각한다.

3. 디지털 포렌식 프로세스 통합을 위한 정책적 제언

가. 기관간 디지털 증거에 대한 chain of custody 방식의 표준화

우리 형사사법체계상 수사나 조사권한을 갖고 해당 기관의 업무와 관련한 범죄혐의를 입증하기 위하여 디지털 포렌식 업무를 수행하고 있는 기관들이 다수 있다. 그리고

각 기관들은 개별적으로 디지털 증거에 대한 현장 대응방식과 증거수집절차 및 디지털 포렌식 업무지침 등을 두고 있다. 이러한 기관들이 디지털 포렌식 프로세스를 통해 산출한 디지털 증거는 기소를 위한 증거자료로서 또는 그 증거를 토대로 추가적인 수사를 위해 검찰의 디지털 포렌식 프로세스로 이송된다.

이와 같이 각 기관마다 디지털 포렌식 업무를 수행함에 있어서 디지털 증거를 수집 및 처리하는 방식에 차이가 있게 되면 디지털 증거에 대한 chain of custody에 문제가 발생할 수 있다. 즉 디지털 증거를 수집한 기관이 chain of custody를 잘 유지했더라도 그 증거를 이송받은 기관이 증거보존절차를 제대로 갖추지 못했거나 분석 프로세스에 있어서 권한통제가 제대로 유지되지 못한다면 디지털 증거에 대한 chain of custody에 대한 신뢰에 문제가 생길 수밖에 없다. 마찬가지로 디지털 증거에 대한 보존 및 분석과 관련하여 엄격한 chain of custody가 유지된다고 하더라도 이미 수집단계에서 제대로 chain of custody가 유지되지 못한 상태의 증거가 이송되어온다면, 분석단계에서의 chain of custody가 의미를 갖지 못하게 될 것이다.

따라서 조사 및 수사권한이 있는 기관에서 포렌식 업무를 수행함에 있어서는 디지털 증거를 수집·처리하는 방식의 표준화가 필요하며, 최소한 기관간에 공유해야 하는 디지털 증거에 대해서는 chain of custody가 단절되지 않을 수 있는 표준방식을 확립해야 할 것으로 생각된다. 현재 디지털 포렌식 업무를 수행하는 국가기관들간에 협의체가 형성되어 있고, 연 1회 정도 협의체 모임을 통해 기관간 정보교류가 이루어지고 있다는 점에 비추어 볼 때, 기관간 협의를 통해 디지털 증거의 수집 및 처리방식의 표준화를 도출하기는 어렵지 않을 것으로 생각된다. 이와 관련해서는 증거수집 및 보관 기관간 연속성 표지 방식 통일화, 증거보존 및 관리 방식 표준화, 이송절차 표준화 등의 작업이 이루어져야 할 것으로 생각된다.

나. 디지털 포렌식 결과에 대한 재검증 절차 도입

디지털 포렌식 결과물은 디지털 포렌식 프로세스의 결론에 해당하는 부분이며, 법정에서 디지털 증거의 증거능력을 뒷받침하는 핵심자료로서 중요성을 갖는다. 즉, 디지털 포렌식 결과물안에는 디지털 증거의 분석결과에 따른 혐의입증자료 뿐만 아니라 포렌식 프로세스의 전과정에 대한 요구사항 - 절차적 일관성 및 정확성, 방법

및 도구의 적합성, 분석관의 전문성 등 -이 모두 포함되어 있어야 한다. 또한 디지털 포렌식 결과가 기재된 보고서는 객관적이고 정확해야 할 뿐만 아니라 제3자에 의해 그 결과가 재현가능할 수 있도록 프로세스 전과정에 대한 기록이 담겨 있어야 한다.

따라서 디지털 포렌식 분석관이 산출한 결과물이 최종적으로 법정에 제출되기 전에 그 내용이 기술적·법률적·절차적으로 정확한가에 대한 검토가 행해질 필요가 있다. 먼저 기술적 검토는 동료 분석관에 의해서, 법률적 검토는 법률팀의 자문을 거쳐서, 그리고 절차적 검토는 최종적으로 디지털 포렌식 프로세스 전체에 대해 책임을 지는 관리자에 의해서 행해지는 것이 바람직할 것이다. 다만 절차적 정확성은 디지털 포렌식 보고서의 표준 양식을 통해서 확보될 수 있기 때문에 특별히 절차적 요소가 문제되는 사안이 아닌 한에서는 별도의 검토를 생략할 수 있다고 할 수 있다.

디지털 포렌식 보고서에 대한 최종적인 검토에 있어서 가장 중요한 것은 기술적 정확성에 대한 검증이라 할 수 있다. 만약 법정에 제출된 이후 반대 당사자에 의해 기술적으로 산출된 결과가 재현될 수 없거나 결과가 잘못 산출된 것이라는 이의가 제기되는 경우에는 동 사안에 있어서 디지털 증거가 절대적인 중요성을 갖는 것이라 할지라도 법적 신뢰성이 배제될 수 있기 때문이다. 따라서 디지털 포렌식 분석관이 최종적으로 산출한 결과에 대해서는 다른 동료 분석관에 의한 재검증 작업이 이루어지는 것이 바람직하다.

그런데 현재 우리의 디지털 포렌식 실무에 있어서는 포렌식 업무에 종사하는 인력이 부족한 상태에서 계속 증가하고 있는 디지털 증거에 대한 분석을 담당해야 하기 때문에, 동료 분석관이 산출한 결과를 재검증하는데 투입할 수 있는 인적 자원의 여력이 없는 상태라고 할 수 있다. 따라서 디지털 포렌식 결과에 대한 재검증이 가능하기 위해서는 포렌식 업무를 담당하는 분석관의 수가 업무량에 비례하여 적정해야만 한다.

모든 사건에 있어서 디지털 증거의 중요성은 강조하면서도 정작 디지털 증거를 수집하고 분석해서 법정에 신뢰할 수 있는 자료로 제출하는 업무를 담당할 디지털 포렌식 분석관의 업무 부담을 무시한다면, 디지털 포렌식 결과물의 품질은 저하될 수 밖에 없고 그로 인한 디지털 증거에 대한 법적 신뢰 역시 낮아질 수 밖에 없다고 할 것이다. 2014년 미국 NIJ 후원으로 열린 디지털 포렌식 관련 포럼에 참석한 디지털

포렌식 분석관들도 이구동성으로 지적하고 있는 것이 기관의 책임자 또는 관리자가 디지털 포렌식에 대한 이해 내지 인식이 낮아서 그 필요성과 중요성을 공감하지 못하며, 그로 인하여 항상 인적·물적자원의 부족에 시달리고 있다[744]고 비판하고 있음을 볼 수 있다. 그리고 이러한 업무부담이 디지털 포렌식 프로세스내의 피드백회로에 영향을 미칠 뿐만 아니라 분석관들의 교육기회를 박탈함으로써 전문성 유지에도 악영향을 미치고 있다고 지적했다.[745]

현재 우리의 경우 디지털 포렌식 업무를 수행하고 있는 기관 가운데 단 한 개 기관만이 별도의 검증팀을 운영하고 있는 것으로 알려져 있으며, 다른 기관들은 중요 사건의 경우에 한해서 동일 분석관이 자신이 산출한 결과를 스스로 재검증하는 수준에 그치고 있다. 그리고 대부분의 경우에는 디지털 포렌식 결과가 해당 포렌식 분석관 개인의 능력에 전적으로 의존하고 있는 상황이라 할 수 있다. 하지만 형사절차에서 유무죄를 좌우할 수 있는 입증자료가 한 개인의 능력에 좌우되도록 하는 것은 바람직하지 않다고 할 것이다. 따라서 디지털 포렌식 결과가 형사절차에서 갖는 중요성과 의미를 고려해 볼 때, 디지털 포렌식 결과에 대한 재검증절차는 디지털 증거의 신뢰를 위해서 뿐만 아니라 형사절차의 기본원칙인 실체적 진실의 구현이라는 측면에서도 중요한 것이라는 인식이 필요하다고 할 것이다.

다. 형사소송법 개정에 따른 디지털 포렌식에 대한 법적 판단기준 마련

과학적 증거의 허용성에 대한 판단기준으로 가장 일반적으로 언급되는 것이 Daubert test 이지만 디지털 포렌식과 관련하여서는 논의된 경우가 많지 않았다. 즉 디지털 증거의 증거능력과 관련해서 대부분의 판결은 무결성과 동일성의 입증, 그리고 전문증거의 예외에 해당하는가에 대한 판단을 중심으로 논의되어 왔기 때문에, 전문가 그리고 전문기술에 의하지 않고서는 그 내용을 확인할 수 없는 비가시적 증거를 이해가능하고 인식가능한 형태의 증거로 전환하는데 활용된 디지털 포렌식

744) Sean E. Goodison/Robert C.Davis,/Brain A.Jackson, “Digital Evidence and the U.S. Criminal Justice System; Identifying Technology and other needs to more effectively acquire and utilize digital evidence” pp. 14-16; https://www.ncjrs.gov/pdffiles1/nij/grants/248770.pdf

745) Sean E. Goodison/Robert C.Davis,/Brain A.Jackson, op.cit., p.15.

기술과 전문가, 그리고 산출된 포렌식 자료에 대해서는 별도의 법적 판단을 할 필요성이 없었다고 할 수 있다. 법정에 제출된 디지털 포렌식으로 산출된 결과에 대해 법적 판단이 필요한 경우라고 해도 전문가 감정에 준하여 언급되어져 왔다.

하지만 형사소송법 제313조 제2항의 개정으로 '과학적 분석결과에 기초한 디지털 포렌식 자료, 감정 등 객관적 방법으로 성립의 진정함이 증명되는 때에는 증거로 할 수 있다'는 규정이 들어옴으로서, 디지털 포렌식 자료에 대한 법적 판단이 필요한 경우가 생길 수 있게 되었다고 할 수 있다. 즉 디지털 포렌식 자료가 정확하고 신뢰성 있게 산출되었다는 것이 입증되어야 그로부터 디지털 증거의 성립의 진정성을 증명할 수 있기 때문이다. 따라서 과학적 분석결과에 기초한 디지털 포렌식 자료가 정확하고 신뢰성 있게 산출되었다는 것이 포렌식 분석관의 증언에 의해 입증되어야 하는데, 이러한 과학적 증거에 대한 전문가 증언의 허용가능성에 대한 법적 판단기준이 무엇이어야 하는가에 대한 논의가 필요하다고 할 것이다.

앞서 기술한 바와 같이 일반적인 과학적 증거에 대한 전문가 증언의 법적 판단기준으로서 적용되어온 Daubert test 기준이 디지털 포렌식 도구로부터 산출된 결과에도 적용된다고 하는 것이 Daubert test를 확립하고 적용해온 미 연방대법원의 입장이다.[746] 따라서 디지털 증거를 추출·분석·복구하기 위해 사용된 기초가 된 방법론이나 기술들이 건전하고 유효한 것인가, 그 결과로서 산출된 증거가 신뢰할 수 있는가에 대하여 Daubert test 기준에 따른 법적 판단이 행해져야 하는 것이다. 그런데 Daubert test가 제시하고 있는 기준은 디지털 포렌식의 본질적 성격에 부적합한 측면이 있다. 따라서 과학적 증거에 범용적으로 적용되는 일반적 판단기준을 디지털 포렌식 영역에서 어떻게 해석하고 적용할 것인가를 고민할 필요가 있다고 생각한다.

즉, 디지털 포렌식에 적용되는 Daubert test 기준은 다음과 같이 정리 될 수 있다.

(1) 검증가능성 : 과학적 절차가 검증가능한 것인가
(2) 동료심사 : 과학적 절차가 출간되었으며 동료심사의 대상이 되었는가
(3) 오류율 : 과학적 절차의 활용과 관련하여 오류율을 알게될 가능성이 있는가 또는 알려진 오류율이 존재하는가

746) David Watson/Andre Jones, op.cit., p. 4.

(4) 표준 : 과학적 절차의 방법을 통제하기 위한 표준과 프로토콜이 존재하는가
(5) 승인 : 과학적 절차가 일반적으로 관련 과학 공동체에 의해 승인되었는가

이 5가지 기준 가운데 검증가능성과 오류율 그리고 표준 요건과 관련해서는 디지털 포렌식이 충분히 충족할 수 있다고 생각한다. 먼저 검증가능성과 관련하여 디지털 포렌식은 그 결과가 제3자에 의해 재현가능해야 비로서 신뢰할 수 있다고 보기 때문에 항상 디지털 포렌식 업무 과정중에 취해진 모든 조치와 절차를 기록으로 남겨서 검증가능하도록 하고 있다는 점에서 그 기준을 충족할 수 있다고 할 것이다. 다음으로 오류율과 관련해서는 디지털 포렌식 도구인 소프트웨어의 오류율이 존재하며, 결과의 신뢰성을 저해하지 않는 수준에서 허용가능한 범위내의 오류율인가를 확인하도록 하기 때문에 오류율에 관한 기준도 문제가 되지는 않는다고 본다. 그리고 표준과 관련하여 과학적 절차와 방법을 통제하기 위한 표준과 프로토콜의 존재는 디지털 포렌식에 적용되는 국제적 표준의 인증 그리고 디지털 포렌식의 절차와 품질을 통제할 수 있는 프로세스를 통해서 입증할 수 있다고 할 것이다.

문제는 동료심사와 과학공동체에 의한 승인 기준이다. 이 두가지는 모두 디지털 포렌식 기술의 빠른 발전과 변화로 인하여 그 기준을 충족하기 어렵다는 측면이 있다. 즉 디지털 환경이 빠르게 변화하는데 대응하기 위해서는 디지털 포렌식 기술도 지속적으로 변화 발전해야만 하기 때문에 동료심사를 거치거나 공동체에 의한 승인을 받을 만한 시간적 여유를 갖기가 어렵다고 할 수 있다. 예를 들어 동료심사를 거치지 않은 새로운 디지털 증거 추출 또는 복구기법을 개발하여 포렌식 업무에 적용한 경우 그러한 기술적 방법에 대한 신뢰성에 대해서는 언제든지 이의가 제기될 여지가 있는 것이다. 또한 최신기술이 적용된 매체들로부터 디지털 증거를 확보하기 위해서는 최대한 빠른 포렌식 기술개발이 필요하기 때문에 공동체의 승인을 받을 현실적인 여유가 없기 때문에 이로 인한 신뢰성의 문제 역시 제기될 수 있는 것이다.

따라서 동료심사와 과학공동체에 의한 승인기준을 디지털 포렌식에 적합한 방식으로 해석하는 것도 고려해볼 수 있다고 생각한다. 즉 기존의 동료심사가 출간물에 의한 관련 분야 전문가의 심사를 의미하는 것이었다고 하면, 디지털 포렌식에 있어서의 동료심사는 관련분야 전문가에 의한 교차검증을 통한 동료심사로 대체하는 것도 생각해 볼 수 있다고 할 것이다. 물론 변화가 빠르지 않은 분야의 디지털 포렌식의

경우에는 여전히 출간물에 의한 동료심사가 그 판단기준으로서 유효하게 작동할 수 있을 것이며, 다만 모바일 포렌식이나 클라우드 포렌식 등과 같이 기술적 변화가 빠른 분야의 디지털 포렌식에 있어서의 동료심사에 대한 판단기준은 동료전문가에 의한 교차검증으로 대체하는 방식을 고려해볼 수 있다고 생각한다.

마지막으로 과학공동체 승인 기준은 해당 디지털 포렌식 분야에 있어서 그 기술을 여러 전문가들이 사용하고 산출된 결과에 대하여 신뢰를 인정하는 것으로 대신하는 것도 생각해 볼 수 있다. 즉 디지털 포렌식 기술은 특정한 매체중심으로 개발되기 때문에 그 적용범위가 협소하여 관련공동체 자체가 일반 과학분야와는 비교되지 않을 정도로 작다고 할 수 있다. 따라서 그 기술을 사용하는 특정 분야의 사람들이 일관된 산출결과를 인정하는 것으로 공동체 승인 기준을 충족한다고 보는 것도 가능하지 않을까 한다.

기존의 전통적인 과학분야에 적용되어왔던 기준을 기술분야에 적용하는데서 비롯되었던 한계가 금호 타이어 판결에서 과학전문가에서 기술전문가로 그 범위를 확대함으로써 극복되었듯이, 앞으로의 판결을 통해서 최첨단 기술을 수반하는 디지털 포렌식에 적합한 법적 판단기준이 확립되어질 수 있을 것으로 생각한다.

참고문헌

1. 국내문헌

강지현/김민지/김성규/Jane Goodman-Delahunty/Paula Saunders/Mandeep Dhami/Yvette Tinsley, 법과학을 적용한 형사사법의 선진화 방안(II), 한국형사정책연구원 연구총서, 2011.

검찰, 국가 디지털 포렌식 센터 Brochure.

경찰청, 디지털증거처리 표준가이드라인, 2006.

경찰청, 스마트폰 포렌식 기술 연구, 국외훈련보고서 2012.

경찰청, 한국형 디지털증거 표준 관리모델에 관한 연구, 2015, 48면.

김기범/장기식/장윤식/이상진/임종인, "디지털 포렌식 전문가 자격모델 개발", 디지털 포렌식 연구 제3호, 2008.

김성룡, "이메일 압수·수색에 관한 독일 연방헌법재판소 결정의 주요 내용과 그 시사점", 경북대학교 법학논고 제32권, 2010.

김지홍, 디지털 포렌식 절차모델에 대한 새로운 접근, 서울대 석사논문, 2015.

김혜경/김택수, 선진국의 법과학 체계 및 입법례 비교, 2014.

노명선, "디지털 증거의 증거능력에 관한 판례 동향과 분석(I)", 수사연구, 2014.

노명선, "해외 판례 동향", Forensics 2011.

노명선, 국제기준에 적합한 디지털 포렌식 기술교육의 표준모델 개발, 2012.

노명선/백명훈, 디지털 포렌식, 2016.

대검찰청, 압수수색 관련 판례의 태도 및 외국 증거법제 도입가능성 연구, 2014.

대검찰청, 과학수사 실무매뉴얼.

래리 다니엘/라즈 다니엘(백제현 역), 포렌식 전문가와 법률가를 위한 디지털 포렌식, 2012.

박희일/윤종성/이상진, "디지털 포렌식 수준 평가지표 개발에 관한 연구", 정보보호학

회 논문지 Vol.24, no.5, 2015.

박희일/윤종성/이상진, “디지털 포렌식 수준 평가지표 개발에 관한 연구”, 정보보호학회논문지, 2015.

변정수, “한국형 디지털 증거분석 표준화: 경찰청 디지털 증거처리 표준가이드라인 및 증거분석 전문매뉴얼의 고찰”, 디지털 포렌식 연구, 2007.

사이버안전국 디지털 포렌식 센터, 현장수사관을 위한 디지털 증거 압수수색 길라잡이, 2016.

신지호/최낙범, “경찰 디지털 포렌식 조직구조와 업무과정 개선방안에 관한 연구 - 거점분석실과 전문상담관 제도를 중심으로”, 경찰학 연구 제16권 제3호, 2016.

이경렬, “디지털정보 관련 증거의 압수·수색 규정의 도입방안 연구”, 홍익법학 제13권 제3호, 2012.

이동윤, 디지털 포렌식 도구를 위한 ISO/IEC 9126 기반의 품질평가모델, 숭실대 석사논문, 2014.

이상미, “관련성 없는 디지털증거 삭제 시 이중해쉬를 이용한 무결성 입증방안”, 제12회 광주전남 법학교수검찰 실무연구회 자료집, 2016.

이완규, “디지털 증거 압수수색과 관련성 개념의 해석”, 법조 제686권, 2013, 152면.

이원상, “온라인 수색에 대한 고찰 - 독일의 새로운 논의를 중심으로, 형사법연구 제20권 제4호, 2008.

이원상, 사이버범죄에 있어서 형법의 역할과 시스템적 대처방안, 2003년 석사학위논문, 2003.

이원상/탁희성/송봉규, 디지털 포렌식 역량강화방안, 2012년 경찰청수탁과제, 2012.

임종인, 경찰의 차세대 디지털 포렌식 기반 구축방안, 2008.

전현욱/윤지영, 디지털증거 확보를 위한 수사상 온라인 수색제도 도입 방안에 대한연구, 2012년 대검찰청 용역보고서, 2012.

정교일, “디지털 증거의 압수와 공판정에서의 제출방안”, 형사법 신동향, 2010.

최재민/오정훈/이상진, “국내환경에 적합한 컴퓨터 포렌식 도구 검증용 이미지 구성방안 연구”, 디지털 포렌식 연구 제7호, 2010.

탁희성/이상진, 디지털 증거분석도구에 의한 증거수집 절차 및 증거능력 확보방안, 한국형사정책연구원, 2006.

탁희성/이인영/권준수/강도형/장준환, 뇌과학의 발전과 형법적 패러다임 전환에 관한 연구 II, 2014.

한국경영시스템(주), ISO 9001:2015 규격요구사항, 2015.

2. 외국문헌

Adam Teicher, "Weaving functional brain imaging into the tapestry of evidence: A case for functional neuroimaging in federal criminal courts", Fordham Law Review, Vol.80, 2011.

Aleksandar Valjarevic/Hein S. Venter, "Harmonised Digital Forensic Investigation Process Model", IFIP Advances in Information and Communication Technology, Vol.410, 2012.

Ankit Agarwal/Megha Gupta/Saurabh Gupta/Subhash Chandra Gupta, "Systematic Digital Forensic Investigation Model", International Journal of Computer Science and Security, Vol.5, Issue1, 2011

Association of Chief Police Officers, ACPO Good Practice Guide for Digital Evidence, ver.5, 2012

Brian Carrier/Eugene H.Spafford, "Getting Physical with the Digital Investigation Process", International Journal of Digital Evidence, Vol.2, Issue 2, 2003

Council of the Inspectors General on Integrity and Efficiency, Quality Standards for Digital Forensics, 2012.

Daniel B. Garrie/J. David Morrissy, "Digital Forensic Evidence in the Courtroom: Understanding Content and Quality", Northwestern Journal of Technology and Intellectual Property, vol.12, 2014.

David Watson/Andre Johes, Digital Forensics Processing and Procedures - Meeting the Requirements of ISO 17020, ISO 17025, ISO 27001 and Best Practice Requirements, 2013.

DFRWS, “A Road Map for Digital Forensic Research by Collective work of all DFRWS attendes”, The Digital Forensic Research Conference, DFRWS 2001 USA.

Emilio Raymond Mumba/H.S.Venter, “Testing and Evaluating the Harmonized Digital Forensic Investigation Process in Post Mortem Digital Investigation”, ADFSL Conference on Digital Forensics, Security and Law, 2014

ENFSI, Best Practice manual for the Forensic Examination of Digital Technology, ENFSI-BPM-FIT-01, ver.01, Nov.2015.

ENISA, Electronic evidence - a basic guide for First Responders, 2014.

Eoghan Casey, Digitak Evidence and Computer Crime-Forensic Science, Computers and the Internet, 2004, p. 175.

Eric Hilgendorf/ Brain Valerius, Computer- und Internetstrafrecht, 2. Auflage, 2012.

Forensic Science Regulator, Business Plan 2012 to 2017.

Forensic Science Regulator, Business Plan 2013/2014, ver.1.0

Forensic Science Regulator, Codes of Practice and Conduct : Appendix: digital Forensic Service, Issue1, 2014.

Forensic Science Regulator, Codes of Practice and Conduct for forensic science providers and practitioners in the Criminal Justice System, ver.2.0 2014.

Forensic Specialties Accreditation Board, Inc., Forensic Specialties Accreditation Board, Inc., 2011.

G.Palmer, “DTR-T001-01 Technical Report. A Road Map for Digital Forensic Research”, Digital Forensics Workshop(DFRWS), 2001.

Gary Palmer, "A road Map for Digital Forensics Research", DFRWS, Nov.2001.

Guidance Software, Encase Legal Journal, 2003.

H.M.A. van Beek/E.J. van Eijk/R.B. van Baar/M. Ugen, J.N.C. Bodde/A.J. Siemelink, “Digital forensics as a service: Game on”, Digital Investigation Vol. 15, 2015.

Home Office, Consultation on new statutory powers for the forensic science

regulator, 2013.

House of Commons Science and Technology Committee, Forensic Science, Second Report of Session 2013-2014 vol.1., 2013.

House of Commons Science and Technology Committee, Seventh Report of Session 2010-12, The Forensic Science Service.

ISO, International Standard ISO 9001 Quality Management System-Requirements, 2015.

ISO/IEC, International Standard ISO/IEC 17025; General requirements for the competence of testing and calibration laboratories , 2005.

ISO/IEC, International Standard ISO/IEC 27001 Information technology-Security techniques- Information Security management systems-Requirememts, 2013.

John Barbara, "Digital Evidence Accreditation: ASCLD/LAB sets a standard of Acceptability", Law Enforcement Technology Vol.31, Issue.2, 2004.

Kelly Anne Cole/Shruti Gupta/Dheeraj Gurugubelli/Marcus K Rogers, "A Review of Recent Case Law Related to Digital Forensics: The Current Issue", Proceedings of Conference on Digital Forensics, Security and Law, 2015.

Mark Reith/Clint Carr/Gregg Gunsch, "An Examination of Digital Forensic Model", International Journal of Digital Evidence, Vol.1, Issue 3, 2002.

Michael Donovan Kohn, Integrated Digital Forensic Process Model, 2012.

Michael J. Saks, "Explaining the Tension Between the Supreme Court's Embrace of Validity as the Touchstone of Admissibility of Expert Testimony and Lower Court's(Seeming) Rejection of Same," Episteme, Vol.5, 2008.

OLAF, Guidelines on Digital Forensic Procedures for OLAF Staff, 2016.

R.B. van Baar/H.M.A. van Beek/E.J. van Eijk, "Digital Forensics as a Service: A game changer", Digital Investigation 2014, vol. 11 Sup 1, 2014.

Robert M.and Bloom/Mark S. Brodin, Criminal Procedure(The Constitution and the Police), 5th ed. 2006.

Sean E. Goodison/Robert C.Davis/Brain A.Jackson, "Digital Evidence and the U.S. Criminal Justice System:Identifying Technology and other needs to more effectively acquire and utilize digital evidence", https://www.ncjrs.gov/pdffiles1/nij/grants/248770.pdf

Sean E. Goodison/Robert C.Davis/Brain A.Jackson, op.cit., https://www.ncjrs.gov/pdffiles1/nij/grants/248770.pdf

Sean E.Goodison/Robert C.Davis/Brain A. Jackson, "Digital Evidence and the U.S. Criminal Justice System-Identifying technology and other needs to more effectively acquire and utilize digital evidence", ; https://www.ncjrs.gov/pdffiles1/nij/grants/248770.pdf.

Sundresan Perumal, "Digital Forensic Model Based On Malaysian Investigation Process", International Journal of Computer Science and Network Security, Vol.9, No.8, 2009.

Thomas G. Field, Jr & Colleen M. Keegan, "Daubert's Significance", http://www.fplc.edu/RISK/vol4/fall/daubert.htm

T.Wilson/J.Slay, "Digital Forensics"; exploring validation, verification & certification", Systematic Approaches to Digital Forensic Engineering, 2005, First International Workshop on digital forensics, 2005.

U.S. Dept, of Justice, Digital Evidence in the Courtroom; A Guide for Law Enforcement and Prosecutors, NIJ Special Report, 2007.

U.S. Dept. of Justice, Electronic Crime Scene Investigation: A Guide for First Responders, 2001.

U.S. Dept. of Justice, Electronic Crime Scene Investigation: A Guide for First Responders, 2nd.ed. 2008.

U.S. Dept. of Justice, Forensic Examination of Digital Evidence: A Guide for Law Enforcement, NIJ Special Report, 2008.

U.S. Dept. of Justice, Regional Computer Forensics Laboratory Annual Report For Fiscal Year 2014.

U.S. Dept.of Justice, The Impact of Forensic Science Research and Develop-

ment, NIJ, 2015.

Yunus Yusoff, Rosland Ismail and Zainuddin Hassan, "Common Phases of Computer Forensics Investigations Models", International Journal of Computer Science & Information Technology, Vol.3, No.3, June 2011.

Venansius Baryamureeba/Florence Tushabe, "The Enhanced Digital Investigation Process Model", The Digital Forensic Research Conference, DFRWS 2004 USA.

Zdziarsko's blog of things, "The Importance of Forensic Tools Validation"; https://www.zdziarski.com/blog/?p=3112

3. 인터넷 사이트

http://biz.heraldcorp.com/view.php?ud=20161006000913

http://central.gutenberg.org/articles/defense_computer_forensics_laboratory

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.169.1878&rep=rep1&type=pdf

http://cpuu.postype.com/post/220456/

http://ec.europa.eu/anti-fraud/about-us/mission_en

http://endic.naver.com/popManager.nhn?sLn=kr&m=miniPopMain

http://forensic-proof.com/archives/3357

http://korea.emc.com/about/news/press/2014/20140612.htm

http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=102&oid=003&aid=0003689147

http://terms.naver.com/entry.nhn?docId=1987148&cid=43667&categoryId=43667

http://thefsab.org/

http://thefsab.org/files/standards_20110220.pdf

http://www.bbc.com/news/uk-35793073

http://www.cfreds.nist.gov/

http://www.cftt.nist.gov/
http://www.cftt.nist.gov/index.html
http://www.cftt.nist.gov/Methodology_Overview.htm
http://www.cftt.nist.gov/Methodology_Overview.htm
http://www.cftt.nist.gov/Methodology_Overview.htm
http://www.dc3.mil/digital-forensics/
http://www.dc3.mil/digital-forensics/digital-forensics#process; 2016.9.10.
http://www.dc3.mil/index#dc3
http://www.dfcb.org/about.html
http://www.dfcb.org/New_DFCB_Site/certification.html
http://www.dfrws.org
http://www.dfrws.org/about.html
http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_and_Advice_for_Manager_of_e-Crime-Investigation.pdf
http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf
http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf
http://www.digitalevidencepro.com/Resources/Approach.pdf
http://www.dmsc.moph.go.th/iso/upload/iso9001_2015.pdf
http://www.enfsi.eu/about-enfsi
http://www.enfsi.eu/about-enfsi/external-relations
http://www.enfsi.eu/about-enfsi/members
http://www.enfsi.eu/about-enfsi/structure
http://www.enfsi.eu/about-enfsi/structure/board
http://www.enfsi.eu/about-enfsi/structure/secretariat
http://www.enfsi.eu/about-enfsi/structure/standing-committees
http://www.enfsi.eu/about-enfsi/structure/working-groups/information-techn

ology
http://www.enfsi.eu/sites/default/files/documents/enfsi-bpm-fit-01_2.pdf
http://www.enfsi.eu/sites/default/files/documents/terms_of_reference_fitwg_v2_20141120_0.pdf.
http://www.forensicinstitute.nl/
http://www.forensicinstitute.nl/about_nfi/organisation_profile/history/
http://www.forensicinstitute.nl/products_and_services/index.aspx
http://www.forensicmag.com/article/2011/03/validation-forensic-tools-and-software-quick-guide-digital-forensic-examiner
http://www.ijde.org/archives/docs/IJDE_1.3.doc
http://www.leagle.com/decision/2005869325BR544_1800/GALAXY%20COMPUTER%20SERVICES,%20INC.%20v.%20BAKER
http://www.lka.polizei-nds.de/download/71669/Allgemeine_Info.pdf.
http://www.lka.polizei-nds.de/download/71674/Forensische_Informations-_und_Kommunikationstechnik.pdf.
http://www.lka.polizei-nds.de/download/71730/Qualitaetsmanagement.pdf.
http://www.lka.polizei-nds.de/kriminalitaet/kriminaltechnik/-856.html
http://www.nij.gov/about/pages/welcome.aspx
http://www.nij.gov/publications/Pages/publication-detail.aspx?ncjnumber=199408
http://www.nij.gov/publications/Pages/publication-detail.aspx?ncjnumber=210798
http://www.nij.gov/publications/Pages/publication-detail.aspx?ncjnumber=211314
http://www.nij.gov/publications/Pages/publication-detail.aspx?ncjnumber=213030
http://www.nij.gov/topics/technology/standards-testing/Pages/developing.aspx
http://www.nij.gov/topics/technology/standards-testing/pages/welcome.aspx
http://www.nsrl.nist.gov/

http://www.nsrl.nist.gov/new.html
http://www.nuclearforensics.eu/
http://www.publications.parliament.uk/pa/cm200607/cmhansrd/cm070712/wmstext/70712m0002.htm#07071262000011
http://www.theguardian.com/science/2011/sep/08/forensic-science-service-closure-damage
http://www.yonhapnews.co.kr/bulletin/2016/09/27/0200000000AKR20160927190400004.HTML?input=1195m
https://cryptome.org/2014/03/forensic-digital-best-practice.pdf
https://cyber.harvard.edu/digitaldiscovery/library/process/simon.html
https://ec.europa.eu/anti-fraud/sites/antifraud/files/docs/body/gip_18092013_en.pdf
https://en.wikipedia.org/wiki/Forensic_Science_Service
https://en.wikipedia.org/wiki/Forensic_Science_Service
https://pdfs.semanticscholar.org/bde1/bf7c149434639a938dd04b6883208d6c51ef.pdf.
https://www.bka.de/DE/DasBKA/OrganisationAufbau/Fachabteilungen/KriminaltechnischesInstitut/kriminaltechnischesinstitut_node.html
https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Kriminaltechnik/Kernkompetenzen/kernkompetenzen_node.html
https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Kriminaltechnik/kriminaltechnik_node.html
https://www.bka.de/SharedDocs/Downloads/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/ki2Flyer.html
https://www.courtlistener.com/opinion/2246387/united-states-v-bunty/
https://www.dfrws.org/sites/default/files/session-files/pres-the_enhanced_digital_investigation_process_model.pdf
https://www.dfrws.org/sites/default/files/session-files/pres-the_enhanced_digital_investigation_process_model.pdf

https://www.enisa.europa.eu/about-enisa
https://www.forensicinstitute.nl/about_nfi/Organisation-profile/Quality.aspx
https://www.forensicinstitute.nl/binaries/alg-leveringsvoorwaarden-diensten-(versie-mei-2015)-uk_tcm120-572668_tcm36-91104.pdf.
https://www.forensicinstitute.nl/binaries/brochure-cbrne-en-2011.def_tcm120-448796_tcm36-18845.pdf.
https://www.forensicinstitute.nl/binaries/brochure-kecida-en-ams-20110525-def_tcm36-19563.pdf
https://www.forensicinstitute.nl/binaries/brochure-memory-toolkit-mtk-en-ams-20110520-def_tcm120-448609_tcm36-21578.pdf.
https://www.forensicinstitute.nl/binaries/brochure-nfi-defraser_tcm120-563783_tcm36-21561.pdf.
https://www.forensicinstitute.nl/binaries/brochure-nfi-prnu-compare-professional_tcm36-21580.pdf
https://www.forensicinstitute.nl/products_and_services/consultancy_services/
https://www.forensicinstitute.nl/products_and_services/consultancy_services/Designing%20an%20efficient%20and%20practical%20working%20environment.aspx
https://www.forensicinstitute.nl/products_and_services/consultancy_services/Ensuring%20efficient%20operational%20processes.aspx
https://www.forensicinstitute.nl/products_and_services/consultancy_services/Generating%20forensic%20awareness.aspx
https://www.forensicinstitute.nl/products_and_services/consultancy_services/Preparing%20for%20Quality%20Assurance%20certification.aspx
https://www.forensicinstitute.nl/products_and_services/consultancy_services/Providing%20appropriate%20management%20training.aspx
https://www.forensicinstitute.nl/products_and_services/forensic_products/bonaparte.aspx
https://www.forensicinstitute.nl/products_and_services/forensic_products/

faraday-cage.aspx
https://www.forensicinstitute.nl/products_and_services/forensic_products/index.aspx
https://www.forensicinstitute.nl/products_and_services/forensic_products/nfi-memory-toolkit.aspx
https://www.forensicinstitute.nl/products_and_services/forensic_products/prnu-compare-professional.aspx
https://www.forensicinstitute.nl/products_and_services/forensic_services/
https://www.forensicinstitute.nl/products_and_services/forensic_services/CBRNe/index.aspx
https://www.forensicinstitute.nl/products_and_services/forensic_services/Fingermark_Individualisation/index.aspx
https://www.forensicinstitute.nl/products_and_services/forensic_services/Forensic_Big_Data_Analytics/index.aspx
https://www.forensicinstitute.nl/products_and_services/forensic_services/Forensics_in_Nuclear_Security_Programme/index.aspx
https://www.forensicinstitute.nl/products_and_services/forensic_services/Mobile_Phone_Data_Recovery/index.aspx
https://www.forensicinstitute.nl/products_and_services/forensic_services/Wildlife_Forensics/index.aspx
https://www.forensicinstitute.nl/products_and_services/training_workshops_courses/
https://www.forensicinstitute.nl/products_and_services/training_workshops_courses/key-benefits.aspx
https://www.forensicinstitute.nl/products_and_services/training_workshops_courses/participants.aspx
https://www.gov.uk/government/organisations/forensic-science-regulator/about
https://www.ncjrs.gov/pdffiles1/nij/grants/248770.pdf

https://www.nist.gov/content/computer-forensics-tool-testing-cftt-project
https://www.rcfl.gov/
https://www.rcfl.gov/about/about
https://www.rcfl.gov/services
https://www.utica.edu/academic/institutes/ecii/publications/articles/A0AC5A7A-FB6C-325D-BF515A44FDEE7459.pdf
https://www.courtlistener.com/opinion/199515/united-states-v-hilton/2016.9.7.
http://cyberbureau.police.go.kr/bureau/sub4.jsp?mid=040401
http://www.nfs.go.kr/main.action
http://www.spo.go.kr/spo/major/forensics/forensics01.jsp
http://www.kdfs.or.kr/
http://www.forensickorea.org/

Abstract

A Study on a Model Frame for the Integration of Digital Forensic Processes

Tak, Hee-sung · Lee, Won-sang

1. Purpose and Method

Digital forensic refers to technology-based methods and procedures for using digital equipment to elucidate and prove the facts about a certain act in court. To present digital data as legally valid evidence, its integrity, reliability, and authenticity needs to be ensured through technical means capable of addressing the physical and logical vulnerabilities of the digital data. Digital forensic is a comprehensive process consisting of the technical, procedural, and legal elements designed to maintain the evidentiary value of digital evidence across all stages from collection to disposal. In this sense, the field of digital forensic requires constant transformation in keeping with the advancement in the IT sector, and it should be open to new knowledge and technology. Digital forensic investigation, in particular, should be supported by a wide range of IT knowledge and technologies. To this end, a network of IT experts is required to grant instant access to knowledge and technologies required in the respective fields.

Korea has yet to develop common digital forensic guidelines for the relevant government agencies, with different agencies still operating different digital forensic systems under disparate guidelines. The lack of standardized procedures or good practices may give rise to issues with the reliability of

digital forensic analysis in Korea. It means the hard-earned forensic data may not be used as evidence at all. In addition, the lack of cooperation between agencies with digital forensic systems vastly restricts their abilities to acquire and use the rapidly changing knowledge and technologies.

In light of the above, this Study seeks to review the digital forensic systems in use at different criminal justice agencies in Korea, identify issues from their practical usage, and shed light on the improvements for the systems. Ultimately, the Study relates itself to developing processes suitable for the shorter life cycles of IT technologies and the speed and confidentiality of forensic investigation. To this end, the Study also seeks to propose an integrated digital forensic process model that will expand Korea's capabilities of digital crime investigations, by a comparative analysis of the digital forensic systems in the leading countries in the field, such as the United States and the United Kingdom. As for research methods, this Study first reviews the previous literatures on the basic framework of digital forensic, as well as the existing digital forensic process models. The Study also looks into the current digital forensic equipment and their operation at disparate government agencies in Korea, and explores the digital forensic processes required to handle digital evidence and their limitations through interviews with experts in the digital forensic field.

In addition, the digital forensic systems and processes in Korea are evaluated by comparing them with those of other countries-the United States, the United Kingdom, Germany, Netherlands, and the European Union-to come up with the future directions that may help establishing Korea's own forensic process.

Lastly, the Study proposes a new model frame for digital forensic process that improves the legal reliability of digital evidence, by considering multiple ways to link the key functions of the integrated digital forensic process with the relevant certification standards, standardization guidelines, technical processes, and legal processes,

2. Need for a New Approach to Digital Forensic

Early discussions on digital forensic focused on the reliability of forensic tools and findings. The focus subsequently shifted to "Chain of Custody," that is, proving the integrity of evidence by showing the continuity of the custody thereof. In recent years, discussions in the field shifted once again to the reliability of the overall digital forensic process. Technical advancement ironically led to more vulnerabilities in terms of securing the evidentiary value of digital data. The current situation warrants the need for scientific methods of proof capable of maintaining consistency and verifiability across different stages from collection to disposal of digital evidence. There has been a growing recognition of the need and significance of building a process to support the development and application those methods.

After the Federal Bureau of Investigation and other criminal justice agencies in the United States first began to investigate computer evidence in early 1984, the agencies realized that the processes and procedures selected for a specific investigation directly affects its outcome. This led to the adoption of official forensic processes by those agencies. The agencies realized early on that using an unsuitable process not only poses a risk of incomplete or invalid outcomes, but also leads to more serious risks of the evidence collected in arbitrary or unstructured manners not being admitted in courts.

As structured standard processes provide the appropriate mechanisms to be complied with by computer forensic investigators, a variety of new computer forensic investigation processes and improvements on existing models were developed and proposed in the past years.

As for the ways in which the digital forensic process models provide their procedural frames, some of them analyze the outcomes from the existing model and add new stages or break down existing ones, while others define their process frames by integrating or harmonizing the effective stages proposed by existing models. Digital forensic process models today increasingly rely on

the concepts of integration and harmonization, and emphasizes compliance with procedural standards. An idea increasingly shared by the digital forensic community is that the use of standardized procedures increase the likelihood of digital evidence being admitted in courts, and minimizes human errors in the overall forensic investigation process.

3. Comparative Analysis of Digital Forensic Systems and Processes in Effect

The Supreme Prosecutor's Office operates a national-level digital forensic center, where Digital Investigator Offices are tasked with performing digital forensic works. However, to meet the explosion of demands for digital forensic analysis, Digital Forensic Investigation Teams have been set up at seven district prosecutor's offices to support evidence collection and forensic analysis.

The Prosecution uses a system called D-NET to meet its digital forensic needs. D-NET is a digital investigation network which establishes online connections between digital investigation teams to provide rapid support, while facilitating digital forensic analysis and ensuring thorough control of the evidence. D-NET consist of an integrated task management system for the Digital Forensic Investigation System (DFIS II), a digital evidence control system, an integrated digital evidence analysis system (IDEAS), and a remote digital investigation coordination system. The Prosecution has developed and revised numerous regulations, guidelines, and manuals to ensure the legality of its digital forensic works, such as the Regulation on Evidence Collection and Analysis by Digital Forensic Investigators (revised on July 16, 2015), the Guidelines on the Digital Forensic Exhibit Collection Procedure (revised on July 16, 2015), the Guidelines on the Operation of the National Digital Investigation Network (revised on July 16, 2015), and the Forensic Investigation Manual.

The Digital Forensic Center at the Police Agency first began as a technical

support team within the Counter-Cyber Terrorism Center. The team was reorganized into the Digital Forensic Team in 2010, and further expanded into the Digital Forensic Center with the foundation of the Cyber Security Bureau in 2014. Article 27-4 of the Rules on Roles and Responsibilities of the Police Agency breaks down the roles in the Digital Forensic Center into Digital Forensic Planning, Technique Development, Mobile Forensic, and Computer Forensic. According to the Rules, the Center carries out a wide range of tasks including policymaking and support, IT environment analysis, development of new tracking techniques, tool development, development of analysis techniques for mobile devices, and development of evidentiary analysis of digital devices. The regulation providing for the digital forensic procedures for the Police is the Rules on the Collection and Handling of Digital Exhibits,[747] and the Digital Evidence Collection Guide for On-site Investigation and the Standard Guidelines for Digital Evidence Processing also provide guidance.

The researcher also interviewed digital forensic experts in individual or group interviews to find out the issues and limitations of the current digital forensic practices as experienced by the experts in their lines of work, and their general perception of digital forensic processes in Korea.

Interviews with individual digital forensic experts were carried out by personally visiting their offices. Group interviews were conducted with experts tasked with performing or supporting digital forensic works at government agencies, universities, and private organizations (law firms, digital forensic firms, etc.). Six experts from three government agencies were interviewed individually, and the group interviews were attended by fifteen experts.

The interview questions consisted of the structure of digital forensic works in the respective agencies, the overall digital forensic procedures, related guidelines, digital forensic tools, digital forensic experts, and their preparation by revision of the Criminal Procedure Act.

---

747) Police Agency Ordinance, No. 766, enacted on May 22, 2015

The interviewed experts pointed out the following limitations of the current digital forensic processes.

Firstly, the field of digital forensic suffers from a lack of forensic experts. The findings from the interviews suggest that the lack of experts is one of the major obstacles to meeting the requirements of procedural standards regarding digital forensic. Despite the increased demand for seizure and search of digital evidence from the field, the supply of experts dedicated to digital forensic investigation has remained at the same level, with some agencies even downsizing their forensic workforce. The lack of experts also makes it difficult to secure the reliability of the analysis results, by restricting the cross-verification of the analysis carried out by one forensic investigation by another.

The second limitation is related with the reliability of digital forensic tools. The interviews showed that most digital forensic experts - both on the field and in the academia - are keenly aware of the need to verify the digital forensic tools. With the current absence of any official procedure or body to confirm and verify the functional requirements for commercial tools and self-developed tools alike, the experts using those tools often find it difficult to trust the reliability and accuracy of those tools. As for the certification of digital forensic tools, the interviews experts pointed to the need for the adoption of a credible certification body. While the current level of IT expertise in Korea makes it possible to build a system to verify the accurate implementation of functional requirements for digital forensic tools, according to the experts, a private certification system is likely to give rise to questions about the credibility and expertise of those systems.

Thirdly, most government agencies are lacking in terms of the awareness on the standardization of digital forensic processes. The issue of digital forensic process standardization is seldom discussed in Korea, unlike Europe, the United States, and other leading countries in the field. Experts tasked with digital forensic analysis are not keen on the need for standardizing the processes. Most experts express reservations about ISO certification, arguing that the

requirements for ISO certification do not readily lend themselves to the actual digital forensic practices in Korea. Most of the interviewees were found to have given little thought to the issue. To the contrary, many interviewees argued that the processes currently in effect are fully capable of maintaining chain of custody, and standardization is not crucial in Korean courts because they seldom touch on the issue of process standards and certification.

Fourthly, Article 313 (2) of the Criminal Procedure Act as revised on May 29, 2016 provides that, even if a person who made a statement denies the authenticity of the statement before or during the trial, the statement is admissible as evidence if its authenticity is proven based on objective digital forensic data and assessments based on scientific analysis. The revised provision opens up new issues to be discussed in the future, such as the competence of digital forensic experts, verification of analysis results, and the proof of scientific analysis that provided the basis for the digital forensic data presented. Regarding this issue, forensic experts in government agencies are considering the related issues such as the need for court testimony training, verification of the reliability of scientific technologies applied to digital forensic, and the method to prove the reliability of analysis results. However, no meaningful preparation has been made regarding the said issues.

4. Digital Forensic Systems and Processes in Leading Countries

In the United States, the National Institute of Justice (NIJ), the Regional Computer Forensic Laboratory (RCFL) and the Defense Computer Forensic Laboratory (DCFL) are the leading organizations in the digital forensic field. These agencies either acquired an ISO 17025 certification, or is in the process of acquiring one. Guidelines and guides on digital forensic works include: Electronic Crime Scene Investigation: A Guide for first Responders, Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors, and Forensic Examination of Digital Evidence: A Guide for Law Enforcement.

In the United Kingdom, after the closure of the Forensic Science Service (FSS), digital forensic works were largely taken up by private forensic service firms and the Science Investigation Center of the Police. The transition gave rise to issues with acquiring ISO 17025 certification, and the Forensic Science Regulator (FSR) was created to provide advices and guidelines for forensic service providers to follow common standards. The FSR enacted the Code of Practice and Conduct. The Code follows the ISO/IEC 17025 standard, and specifies the requirements for a management system where forensic service providers can prove their capability to provide consistent results and services that satisfy the needs of customers in the criminal justice system. The United Kingdom also specifies the basic principles on digital evidence and the components of their digital forensic processes through the Good Practice Guide for Digital Evidence published by the Association of Chief Police Officers ACPO), Crime Business Area.

The European Union operates the European Network of Forensic Science Institutes (ENFSI) to share and exchange expert knowledge in the forensic field. The Network consists of two standing committees, Quality & Competence Committee and Research & Development Committee. The former develops policies for improving competence and competitiveness, provide advice to expert working groups and members centers, and provide other services related with best practices and the application of international standards. The Research & Development committee comes up with the research & development policies for the ENFSI, provide R&D advices to expert working groups and members centers, and promotes joint research projects between research centers.[748] The ENFSI has 17 expert working groups. Of the groups, the Forensic Information Technology (FIT) Group developed and distributed a digital forensic manual titled “Best Practice Manual for the Forensic Examination of Digital Technology”. The Manual lays out the frameworks for the relevant procedures, quality improvement principles, and approaches to training procedures and

748) http://www.enfsi.eu/about-enfsi/structure/standing-committees;2016.9.30.

forensic investigation, for the member centers of the ENFSI. The manual supports the application of internationally standardized procedures that considers the unique needs of different regions. In addition, the Guidelines on Digital Forensic Procedures for OLAF staff, Electronic evidence – a basic guide for First Responders is a digital forensic guide prepared for application in European countries.

The construction of digital forensic systems in the leading countries provide several implications for the corresponding efforts in Korea, which can be summarized in four parts. First, digital forensic needs to be performed in compliance with the international standards. The United States and European Countries carry out digital forensic works in accordance with the ISO standards and the Europe-specific ENFSI standards. The Europe Union mandates the application of and compliance with ISO standards in its digital forensic guidelines. Applying the standards specified in the digital forensic guidelines assures the quality of digital forensic analysis regardless of which agency performs the analysis, and courts will also see no problem in admitting them as evidence. Such application is also critical for using the analysis results in courts of other countries. For these reasons, digital forensic practices need to be aligned with the relevant international standards. Secondly, digital forensic bodies need to come up with the models that lend themselves to the specific needs of the bodies. However, these models need to be built through the customization of the relevant international and local standards, rather than creating a model which only suits their needs. A process model for Korea would ideally be based on the ENFSI or the US standards, as Korea has no local standards in this area.

5. Need for Integration of Digital Forensic Process

A digital forensic process should go further than an ordering of digital forensic works; it needs to accurately record the movement of digital evidence

through each stage of policies and systems applicable to the entire process, and incorporate the standardization requirements for the components of each stage. These efforts are required to maintain the suitable quality of the processes and procedures used in digital forensic works, and provide the courts with reliable analysis results. To this end, an integrated forensic process capable of managing and controlling the overall forensic works is required. The rationale for an integrated management and control of digital forensic procedures can be summarized as follows.

Firstly, when investigating a case involving digital evidence, investigators with legal knowledge and investigation experiences need to cooperate and collaborate with digital forensic investigators (analysts) with scientific knowledge and technical experience. Otherwise, the reliability of the evidence and the investigative procedures would be questioned. To ensure organic collaboration and mutual cooperation/support between the legal processes and the technical processes, the governance framework for digital forensic works inside investigative agencies need to be expanded to incorporate conventional investigation works into the digital forensic processes, thereby establishing feedbacks and interfaces between the processes at each stage within consistent policy/technical frames.

Secondly, the forensic processes need to adopt standardized criteria to verify the personal and technical quality required for digital forensic processes, so as to produce reliable results through those processes and maintain the evidentiary value of the acquired digital information.

Thirdly, the integration of digital forensic processes should ultimately lead to the acquisition of the certification of the digital forensic lab itself. This issues spans across the overall procedural requirements for digital forensic labs - procedural connectedness, tools and analysts. Acquiring a certification for a digital forensic lab would mean the verification of its procedures, tools, and personnel, which in turn means the reliability of the digital forensic works carried out by the lab. In this sense, certification of a digital forensic lab is

one of the most fundamental issues, which makes it all the more difficult to tackle.

6. Preliminary Considerations for the Integration of Digital Forensic Processes.

The overall processes of collecting, selecting, and analyzing digital data require technical knowledge, experience, and expertise based on scientific knowledge. To translate such scientific and technical expertise into reliability in the legal context, the digital evidence need to be subject to a separate judicial assessment, on the assumption that the science and technologies applied to the assessment are sound. Digital evidence are produced using certain tools suitable for digital technologies. Therefore, their reliability can be determined only based on the understanding of the scientific methods and technical principles applied to the overall processes of converting the exhibits to recognizable data, and presenting them to a court in a format that allows for proving the charges. While it would be unreasonable to expect judges, who lack the understanding of the science and technical methods involved, to determine the accuracy of those science and methods, they need to at least determine whether the science and methods satisfy the criteria regarding scientific soundness or their validity as applied technologies.

The advancement of digital technologies has accelerated the development of digital forensic technologies, and diversified their technical applications. These circumstances may give rise to the question of how we can expect to determine the legal credibility of a certain tool, expert, or process without subjecting them to official verifications. In addition, as explained above, the revision of the Criminal Procedure Act opened a way to prove a fact with digital forensic data based on scientific analysis. Therefore, the credibility of the scientific analysis needs to be substantiated in addition to the credibility of the digital forensic data themselves. This warrants the need for discussions on how to set up the legal tests for these issues in courts.

7. A Model Frame for the Integration of Digital Forensic Processes.

Ensuring the consistency and credibility of digital forensic processes should be preceded by building an integrated management system commonly applicable to the overall operation of the processes. The management system should have the capabilities to control and manage major factors that may affect the accuracy and credibility of the results from the digital forensic processes: the accuracy of documented procedures, personnel training, maintenance and improvement of the processes, environmental conditions for forensic works, and hardware, software, and equipment used for forensic works in the forensic body.

The integrated management system should be applicable to all areas and activities of a digital forensic body. The integrated management system represents a standardized operation procedure that incorporates all guidelines, procedures, regulations, standards, and certifications of a digital forensic body, and a consistent support for ensuring the reliability of digital evidence. This approach allows for the integrative management of digital forensic processes and procedures under a coherent system, and effective coordination of different areas of works, thereby ensuring the forensic processes are operated, reviewed, maintained, and controlled in a way suited to the related works.

A digital forensic body needs to abide by the following principles in building an integrated management system for digital forensic processes.

First, a digital evidence may not be altered across the overall digital forensic processes.

Second, qualifications and training records should be maintained for all personnel tasked with digital forensic works.

Third, all actions taken regarding a digital evidence should be thoroughly recorded.

Fourth, all laws and principles governing digital evidence should be complied

with.

In addition, as each digital forensic body needs to comply with the specific requirements of ISO certifications, these standards need to be maintained and managed through the integrated management system.

While the integrated management system comprehensively manages the policy and procedure requirements for the overall digital forensic processes, the process coordination system represents a more detailed and working-level coordination process under those policy and management requirements. In other words, a digital forensic body needs to develop a standardized work process which organically coordinates between the legal, technical, and policy sectors across the handling of cases involving digital evidence, and prepare a system where the different sections aid and support one another, and provide mutual feedbacks. The first step towards such development involves the coordination between the technical processes and legal processes. Also required is a authority control system and a feedback system between different forensic processes and works.

The specific considerations for the key processes are as follows. In the preparation and collection stages, a digital forensic body needs to establish the procedures for compliance with due procedure, packaging, transportation, and preservation of evidence. The analysis and extraction stages required the maintenance of digital forensic analysts' competences and expertise, as well as digital forensic tools and methodologies. The analysis outcomes should be verified and translated into a credible report in the presentation stage. The last stage, the court testimony stage, requires training forensic analysts for testimonies at courts and effective ways of testimony, so as to prevent the credibility of the outcomes from being undermined.

8. Policy Proposals for the Integration of Digital Forensic Processes

A. Proposals from the Forensic and Technical Perspective

A digital forensic body needs an integrated management system to carry out the overall legal, technical digital forensic procedures under coherent processes. In order to maintain the quality of forensic services, secure the integrity of evidence through the chain of custody, and ensure the reliability of the digital forensic as a whole, the system should be supported a number of sub-systems including the quality management system, the process coordination system, and the standard operation policy system. While the integrated management system offers the policy/management frames for process integration, the working-level integration of forensic processes is achieved through the process coordination system. Specifically, a network of processes needs to be established for each stage under the process coordination system, which will create a virtuous cycle of preparation, collection, investigation/analysis, presentation, testimony, and preservation/maintenance.

In order to ensure that digital forensic is accepted as credible technologies and procedures by the courts, the digital forensic community should begin discussing the need for certification under international standards, and the use of standardized guidelines for forensic processes. Considering the current circumstances surrounding Korean digital forensic today, even the key digital forensic bodies would experience difficulties with acquiring ISO certifications. However, considering the need to expand on the efforts to establish the technical and procedural standards for digital forensic in the future, and the requirements for accuracy and credibility for digital forensic data under the revised Criminal Procedure Act, acquisition of ISO certifications is absolutely necessary.

There is currently no procedure to test and officially verify whether the various digital forensic tools in use today satisfy their functional requirements

and produce accurate results. Therefore, except for a number of internationally accepted tools, any tool can be subject to questions about their accuracy and reliability in courts. The same goes to the reliability of the digital evidence produced using those tools. There is no such thing as a "perfect tool." Therefore, the verification of digital forensic tools need to focus on whether the inherent defect and error of a tool is within the permissible range for the purpose of ensuring the credibility of the analysis results. A viable and ideal course of action is to develop a digital forensic tool verification methodology based on the CFTT project of the NIST, and build public trust toward the digital forensic tools by publicly announcing the tests results.

Another criteria for determining the legal credibility of digital forensic is whether the forensic works are carried out by personnel with suitable expertise and skills. The digital forensic field in Korea still lacks a national-level agency tasked with verifying the competences of forensic experts. The only certification currently available in the country is the Digital Forensic Expert Qualification Test, a private-led qualification program accredited by the government. Although it has been accredited by the government, the qualification and the test contents are comprised of contents developed by the organization implementing the program, without any wide acceptance from the related fields or the application of certified criteria. This led to some questions about the credibility of the certification. Therefore, to ensure the public credibility of forensic experts as well as the credibility of the certifications, the government needs to set up a Certification Committee for Forensic Experts (tentative title) tasked with establishing the technical, legal, and ethical requirements for experts across diverse forensic areas, and have private certification bodies at least adopt the verification system for standard competence items proposed by the Committee.

B. Proposals from the Policy Perspective

Gaps between government agencies in collecting and handling digital forensic evidence may lead to issues of chain of custody. Even if the agency that collected the evidence maintained a suitable chain of custody, its reliability may be questioned if the subsequent agencies lack a suitable preservation procedure or the authorities for the analysis processes are not controlled properly. For this reason, forensic works at agencies authorized to conduct investigations need to be standardized in terms of the collection and handling of digital evidence, and a standardized method is required to prevent the discontinuation of the chain of custody for digital evidence handled by more than one agency.

In addition, the content of the evidence produced by a digital forensic analyst needs to be reviewed for their technical, legal, and procedural accuracy before presenting it to the court. In the final review of a digital forensic report, verification of technical accuracy holds the highest significance. If a technically produced result cannot be replicated by the other party, or the other party argues that the result was derived erroneously, the legal reliability of the evidence may be excluded even if the evidence itself holds an absolute importance in the case. Therefore, all final results produced by a digital forensic analyst should ideally be re-tested by a peer.

The Daubert test is most frequently cited as a test to determine the admissibility of scientific evidence. However, the case is not widely discussed in relation to digital forensic. However, Article 313 (2) of the Criminal Procedure Act as revised on May 29, 2016 provides that, even if a person who made a statement denies the authenticity of the statement before or during the trial, the statement is admissible as evidence if its authenticity is proven based on objective digital forensic data and assessments based on scientific analysis. This may result in the need for legal review of digital forensic data

in some cases. That is, the authenticity of digital evidence can be proven only if the reliability and accuracy of digital forensic data is proven in the first place. The reliability and accuracy of digital forensic data based on scientific analysis would need to be supported by the testimony of the forensic analyst. This leads to the need for setting up the legal test for the admissibility of expert testimony on scientific evidence. The Supreme Court of the United States consistently held that the Daubert test also applies to the results produced from digital forensic tools. Then, it follows that the soundness and effectiveness of the methods and technologies used to extract, analyze, and restore digital evidence, and the reliability of the resulting evidence, need to be legally reviewed under the Daubert test. However, some of the criteria under the Daubert test do not readily fit the nature of digital forensic. Therefore, the general test applicable to scientific evidence in general needs to be differently applied and interpreted for the digital forensic field.

연구총서 16-AA-01

디지털 포렌식 통합모델 구축에 관한 연구

발 행 | 2016년 12월
발 행 처 | 한국형사정책연구원
발 행 인 | 김 진 환
등 록 | 1990. 3. 20. 제21-143호
주 소 | 서울특별시 서초구 태봉로 114
전 화 | (02)575-5282
홈 페 이 지 | www.kic.re.kr
정 가 | 10,000원
인 쇄 | 한국장애인이워크협회 (02)2272-0307
I S B N | 979-11-87160-08-3 93360

연구원의 허락 없이 보고서 내용의 일부 또는 전체를 복사하거나 전재하는 행위를 금합니다.