https://doi.org/10.33778/kcsa.2022.22.5.021

디지털증거분석실의 도구·장비 구축 방안에 관한 연구★

신 수 민*, 박 현 민**, 김 기 범***

요 약

디지털 정보는 정보통신의 발달로 지속적으로 증가 및 다양화되는 추세이며, 이를 악용한 범죄 또한 증가하고 있다. 하지만, 국내의 디지털증거에 대한 처리 및 분석을 위한 환경 구축 사례는 미비한 실정이다. 조직마다 할당된 예산이 상이하고 고질적인 문제인 공간 확보의 어려움을 해소하지 못한 상태에서 구축된 디지털증거분석실은 초기 구성단계에서부터 참조할 수 있는 기준이 없다. 본 논문은 디지털증거분석실 구축 시에 필요한 사항을 도구·장비 중심으로 탐색적 연구를 진행하였다. 연구방법으로 디지털증거분석실 구축 경험 또는 디지털포렌식 분야 근무 경험이 풍부한 전문가 15명을 대상으로 포커스 그룹 인터뷰를 수행하였다. 그 결과 네트워크 구성, 분석관 컴퓨터, 개인 도구·장비, 이미징 장치, 전용 SW, 오픈소스 SW, 공용 도구·장비, 액세서리, 기타 고려사항의 9가지 영역에 대해 전문가들의 의견을 수렴하고 디지털증거분석실의 도구·장비 목록을 도출하였다. 나아가 디지털증거분석실 구축 발전방안으로 공간/도구·장비 목록 표준화, 디지털포렌식 도구·장비 민간 지원·위탁 체계 수립, 미래 디지털증거분석실 인프라 구조를 제시하였다. 이는 향후 디지털포렌식 기능을 신설하고 디지털증거분석실을 구축하고자 하는 기관/조직이 도구·장비 및 인프라 설계 등에 기여할 것이다.

A Study on the Methods of Building Tools and Equipment for Digital Forensics Laboratory

Su-Min Shin*, Hyeon-Min Park**, Gi-Bum Kim***

ABSTRACT

The use of digital information according to the development of information and communication technology and the 4th industrial revolution is continuously increasing and diversifying, and in proportion to this, crimes using digital information are also increasing. However, there are few cases of establishing an environment for processing and analysis of digital evidence in Korea. The budget allocated for each organization is different and the digital forensics laboratory built without solving the chronic problem of securing space has a problem in that there is no standard that can be referenced from the initial configuration stage. Based on this awareness of the problem, this thesis conducted an exploratory study focusing on tools and equipment necessary for building a digital forensics laboratory. As a research method, focus group interviews were conducted with 15 experts with extensive practical experience in the digital forensic laboratory or digital forensics field and experts' opinions were collected on the following 9 areas: network configuration, analyst computer, personal tools·equipment, imaging devices, dedicated software, open source software, common tools/equipment, accessories, and other considerations. As a result, a list of tools and equipment for digital forensic laboratories was derived.

Key words : Digital Forensics Laboratory, Digital Forensics, Tools/Equipment, Focus Group Interview, Special Judicial Police Officer

접수일(2022년 11월 29일), 수정일(2022년 12월 11일), 게재확정일(2022년 12월 27일)

★ 본 연구는 2021년 대검찰청 연구용역과제 "디지털포렌식 랩(DF Lab) 구축 표준 모델 연구"에서 수행한 결과 일부를 수정·보완하였음(S-2021-1601-000)

* 성균관대학교 과학수사학과 박사과정(주저자)

** 성균관대학교 과학수사학과 석·박사통합과정(공동저자)

*** 성균관대학교 과학수사학과 부교수(교신저자)

1. 서 론

디지털 정보는 정보통신의 발전으로 정보화 사회에서 필수 불가결한 요소로 자리 잡고 있다. 4차 산업혁명으로 인해 AI, Big-data, Cloud, IoT 등의 신기술 도입으로 데이터 사용량이 급증했고, 코로나 19 팬데믹은 모든 측면에서 디지털 전환을 가속화하고 있다[1]. 하지만 디지털 정보 활용의 확대 및 기술 가속화 현황은 '10년 6,247건에서 '20년 63,935건으로 약 10배 이상 증가하였다[2]. 디지털증거 분석 수요 증대에 따른 디지털포렌식의 중요성은 커져가고 있으나, 법정에서는 매체 독립성, 대량성, 비가시성·비가독성·잠재성, 네트워크 관련성, 복원성, 취약성 등과 같은 디지털증거의 특성을 제대로 반영하지 못하므로 증거 능력 인정에 대한 한계점을 보인다[3]. 디지털증거 능력 확보를 위해서는 인력, 도구, 증거 처리 및 보관 장소, 증거 수집·분석 후 법정에 제출하기까지의 절차 등이 유기적으로 상호 연계되어야 한다[4]. 따라서, 증거능력에 대한 한계점을 보완하고 인정받기 위해서는 디지털증거 처리 전 과정에 대해 신뢰성을 보장할 수 있는 환경구성이 필수이다. 국내에서는 디지털증거분석실 구축을 통해 디지털증거의 신뢰성을 보장하기 위한 여건 조성이 지속적으로 추진되고 있다. 경찰청은 18개소, 대검찰청은 13개소의 디지털증거분석실을 운용 중에 있으며[5][6], 디지털증거분석실의 신뢰도를 위한 ISO/IEC 17025 인증을 확대하고 있다. 경찰청(KOLAS), 대검찰청(KOLAS), 한국저작권보호원(ANAB), 국립과학수사연구원(KOLAS)이 ISO/IEC 17025 인정을 받았다[7][8]. 국내의 많은 기관에서도 디지털포렌식 기능을 보유하고 있다<표 1>[22]. 하지만 각 기관/조직마다 기능, 규모 및 할당된 예산이 상이하고 고질적인 문제인 공간 확보의 어려움을 해소하지 못한 상태에서 구축된 디지털증거분석실은 초기 구성단계에서부터 참조할 수 있는 기준이 부족하고 기 구축 기관/조직에 협조/지원 하에 제한적으로 이뤄지고 있다. 또한 디지털포렌식이 수사기관에서 출발을 하다 보니 관련 내용이 비공개로 유지되는 점, 운영 형태가 비효율적인 점, 중복적인 투자로 인한 예산 낭비가 발생하는 점 등의 문제가 있다. 따라서, 디지털포렌식 도구·장비를 표준화 또는 목록화하여 효율적이고 적정한 기능을 보장하고 법정에서 증거 능력도 확보할 수 있는 체제 구축이 필요하다. 본 논문에서는 이러한 문제의식을 시작으로 디지털증거분석실 구축 시 도구·장비에 대한 탐색적 연구를 통해 고려할 수 있는 사항들을 도출하고자 한다. 연구방법은 디지털포렌식 전문가 15명을 대상으로 5차에 걸쳐 포커스 그룹 인터뷰를 진행하였다. 네트워크 구성, 분석관 컴퓨터, 개인 도구·장비, 이미징 장치, 전용 SW, 오픈소스 SW, 공용 도구·장비, 액세서리, 기타 고려사항의 9가지 영역에 대해 전문가들의 의견을 수렴하였다.

<표 1> 디지털포렌식 유관기관 현황(2021.7 기준, 민간분야 제외)

구분	부처(기관명)	구분	부처(기관명)	구분	부처(기관명)	구분	부처(기관명)
1	감사원	12	국군정보사령부	23	무역위원회	34	중소벤처기업부
2	게임물관리위원회	13	국립과학수사연구원	24	문화체육관광부	35	중앙선거관리위원회
3	경기도	14	국립농산물품질원	25	병무청	36	철도사법경찰대
4	경찰청	15	국립수산물품질관리원	26	서울출입국·외국인청	37	특허청
5	고용노동부	16	국방부 검찰단	27	서울특별시	38	한국저작권보호원
6	고위공직자범죄수사처	17	국방부 조사본부	28	식품의약품안전처	39	해군검찰단
7	공군군사경찰단	18	국세청	29	신호기술연구소	40	해군군사경찰단
8	공군본부	19	군사안보지원사령부	30	예금보험공사	41	해병대군사경찰단
9	공정거래위원회	20	금융감독원	31	육군본부	42	해양경찰청
10	관세청	21	금융위원회	32	육군중앙조사단	43	환경부
11	국군사이버작전사령부	22	대검찰청	33	제주특별자치도		

본 논문의 구성으로 제2장에서는 디지털증거분석실 도구·장비 산출 및 선정과 관련된 선행연구를 살펴보고, 제3장에서는 연구방법으로 디지털증거분석실 포렌식 도구·장비에 대한 탐색적 연구를 위해 포커스 그룹 인터뷰를 수행한다. 제4장에서는 포커스 그룹 인터뷰 결과를 분석하고 디지털증거분석실 도구·장비를 도출한다. 제5장에서는 발전방안에 대해 살펴보고 제6장에서는 해당 연구의 결론 및 향후 연구방향에 대해 제시한다.

2. 선행연구

Lawrence 등[9]은 2인 이하 기준의 소규모 디지털증거분석실을 구축할 때 소요되는 최소항목의 도구 및 장비 목록을 도출하고, 이에 대한 초기 도입비용과 유지보수 비용 등을 구분하여 제시하였다. 크게 컴퓨터와 모바일 포렌식으로 구분하였으며, 상용 및 오픈소스 제품을 적절히 반영한 결과 초기 도입비용으로 $8,575 ~ $22,052, 유지보수 비용으로 $2,478 ~ $6,419를 제시하였다. O'Connor 등[10]은 디지털포렌식 전문가에 대한 심층 인터뷰를 수행하여 디지털포렌식 도구 선택 기준을 도출하고 기술적, 관리적, 법적 범주로 분류하였다. 또한, 각 기준 별 중요도 등급을 부여함으로써 선택 시 어떤 기준이 우선적으로 고려되어야 하는지를 제시하였다. Hibshi 등[11]은 사용자 편의성을 중점으로 디지털포렌식 도구 고려사항에 대해 인터뷰 및 설문조사를 실시하여 115명의 응답에 기초하여 분석을 진행하였다. 전문성 및 도구수준, GUI와 CLI, 보고서 및 문서화 기능, 도구 사용 시 사용자 교육 필요 여부, 사용자 인터페이스, 워크플로우 및 기타 사용성 및 기술적 문제에 대한 의견이 제시되었다. Brooke Nodeland 등[12]은 사이버 포렌식 랩 구축과 관련하여 목록 및 초기비용을 산정하였다. Lawrence [9]의 연구와 접근방식은 유사하나, 하드웨어와 소프트웨어로 구분하여 분석하였으며 스타트업을 위한 포렌식 도구·장비에 대한 권장사항을 제시하였다는 점에서는 다소 차이가 있다. Román 등[13]은 14종의 디지털포렌식 SW에 대해 분석하였으며 평가지표로 가격, 지원하는 디스크 이미지, 지원하는 파일시스템, 파일분석 기능, 포렌식 분석 기능, 보고서 및 내보내기의 6가지 항목으로 평가하였다. Ghazinour 등[14]은 디지털포렌식 도구 목록과 속성을 매트릭스 형태로 비교·분석하여 조사·분석 시나리오별 활용 가능한 도구들이 차이가 있음을 주장하였다. R Padmanabhan 등[15]은 모바일 디지털포렌식 도구 중 오픈소스(Autopsy, SIFT)와 상용(MOBILedit! Forensic, UFED)을 비교 분석하여 오픈소스의 상용 제품 대체 가능성을 검토하였다. 앞서 언급된 Ghazinour 등[14]의 논문과 같이 디지털포렌식 분석 시 오픈소스와 상용 제품 조합의 필요성을 잠재적으로 나타내고 있다. Jiyoon Ham 등[16]은 디지털포렌식 이미징 도구·장비 29종에 대한 업데이트 기간, 물리적·논리적 디스크 이미지 획득 가능 여부, 사용자 정의 섹터 선택 지원 여부, RAW(DD) 지원 여부, 가상 디스크 이미지 지원 여부, AFF 지원 여부, MD5·SHA1·SHA2·SHA3 해싱 지원 여부 등을 비교·분석하였다. 국외 문헌의 경우 디지털포렌식 도구·장비 목록 도출에서부터 예산 산출, 도구·장비 선택 기준, 특징에 대한 상호 비교·분석 등 다양한 관점에서 접근이 이뤄졌다. 국내 문헌의 경우 도구 개발, 검증, 활용 등[17, 18, 19]에 대한 연구가 중점적으로 진행되었다. 하지만 국내 문헌 검토 결과, 디지털증거분석실 관점에서 필요한 도구·장비에 대한 목록 및 고려사항에 대한 연구는 미미한 편이다.

3. 연구방법

3.1 포커스 그룹 인터뷰

디지털증거분석실에 필요한 도구·장비 목록을 도출하기 위해 포커스 그룹 인터뷰를 채택하였다. 그 이유로는 디지털증거분석실 구축 사례가 많지 않은 점, 각 기관 별로 업무 목적에 따라 도구·장비 차이가 있는 점, 기술발전에 따른 디지털포렌식 SW 변화로 실 수요자의 의견이 요구되는 점 등을 고려할 때, 해당 연구 방법이 적합한 것으로 사려된다. 포커스 그룹 인터뷰는 질적 연구 방법론의 하나로 특정 주제에 대해 소수 그룹의 참여자들이 토의를 통해 다양한 의견들을 제시하고, 자료를 종합하여 설문지 문항 개발 또는 검토 등에 주로 활용한다[20].

3.2 연구 대상

연구 대상은 디지털포렌식 관련 경력이 5년 이상이거나 디지털증거분석실 유관 사업 참여 이력, 자격증 및 강의 이력 등을 고려하였다. 표본 모집 방법은 해당 기준 충족 인원을 선별하여 전화와 이메일 등으로 참여 의사를 확인하였다. 디지털포렌식 분야 종사 여부, 도구 사용 및 실무 참여 정도를 고려하였고, 인터뷰 대상자 서로가 알지 못하는 인원들로 구성하였다. 참여 인원은 경험적 범위가 6~12명이 적절한 것으로 논의되어 12명을 선정하여 포커스 그룹 인터뷰를 진행하였다[21]. 이후 도출된 도구·장비 목록의 추가적인 검증 및 의견 수렴을 위해 3명의 전문가를 대상으로 추가적인 인터뷰를 수행하였다.

<표 2> 포커스 그룹 인터뷰 참여자 일반사항

구분	성별	연령	소속	직책	경력	회차
참여자1	남	30대	포렌식 업체	대표	15년	1차
참여자2	남	30대	금융감독원	선임	9년	1차
참여자3	남	40대	경찰청	연구사	10년	2차
참여자4	남	40대	지방검찰청	수사관	13년	2차
참여자5	남	40대	포렌식 업체	이사	14년	2차
참여자6	남	40대	시·도 경찰청	경감	25년	3차
참여자7	남	40대	시·도 경찰청	경위	9년	3차
참여자8	여	40대	시·도 경찰청	경위	11년	3차
참여자9	남	40대	공공기관	과장	7년	4차
참여자10	남	30대	서울특별시	수사관	4년	4차
참여자11	남	30대	철도사법경찰대	수사관	4년	4차
참여자12	남	40대	철도사법경찰대	수사관	2년	4차
참여자13	남	40대	법무법인	전문위원	20년	5차
참여자14	남	40대	공정거래위원회	조사관	20년	5차
참여자15	남	30대	국방부 검찰단	수사관	15년	5차

3.3 연구 진행 및 절차

3.3.1 사전 준비

인터뷰 전 선행연구 검토를 통해 질문을 생성하고 진행절차 등을 작성하여 내부 연구진들을 대상으로 사전 검토를 실시하였다. 이후 논의를 통해 다음과 같은 최종적인 인터뷰 질문지를 작성하여 참여자들에게 사전에 제공하여 숙지할 수 있도록 하였다.

질문 1: 디지털포렌식 조사관/수사관 개인에게 지급되어야 할 “최소 도구·장비”는 어떤 것이 있어야 합니까?

질문 2: “이미징 도구·장비”의 수량, 용도, 사용하는 제품 및 고려사항에 대해 말씀해주세요.

질문 3: “디지털포렌식 워크스테이션”의 후보군 및 사양 등에 대해 자유롭게 말씀하여 주세요.

질문 4: “분석관 PC”가 필요하다고 생각하십니까?

질문 5: “분석 SW”에 대해 자유롭게 말씀해 주세요.

질문 6: “도구·장비 선택 고려사항”은 무엇입니까?

질문 7: “액세서리”는 무엇이 포함되어야 할까요?

질문 8: “오픈소스(무료) SW”가 도구·장비 셋에 포함되어야 합니까? 만약 그렇다면 어떤 SW를 추천하십니까?

질문 9: 디지털포렌식 조사관/수사관의 2~5인 규모 도구·장비는 무엇이 필요합니까?

질문 10: 5인 이하 팀 단위 도구·장비 구성은 무엇이 필요합니까?

3.3.2 포커스 그룹 인터뷰 실시

본 연구는 5회(1차: ‘21.8.10, 2차: ‘21.8.12, 3차: ‘21.8.26, 4차: ‘21.8.27, 5차: ‘22.12.25)에 걸쳐 비대면 화상회의(WebEx)로 안내자료를 사전 공유하여 내용을 숙지한 상태에서 이뤄졌다. 1~4차는 도구 목록 도출 및 디지털증거분석실 관련 의견을 수렴하였고, 마지막 5차는 4차까지 진행된 연구결과에 대한 검증을 위해 별도로 진행하였다. 포커스 그룹 인터뷰 순서는 연구 배경 및 목적, 인터뷰 참여자 소개, 관련 선행연구 소개, 진행 방식 안내 및 인터뷰 순으로 진행하였다. 인터뷰 시간은 각 차수별 약 2시간 정도에 걸쳐 진행되었다. 1차 인터뷰는 사전 준비된 질문지를 바탕으로 진행하였고, 그 결과 추가적인 의견 등을 종합하여 2~4차 인터뷰까지 ① 네트워크 구성, ② 분석관 컴퓨터, ③ 개인 도구/장비, ④ 이미징 장치, ⑤ 전용 SW, ⑥ 오픈소스 SW, ⑦ 공용 도구·장비, ⑧ 도구 및 액세사리, ⑨ 기타 고려사항과 같이 9가지 영역에 대한 주제를 선정하여 활용하였다. 인터뷰는 참여자들의 의견을 청취한 다음 별도의 추가 의견이 제시되지 않는 포화 시점까지 진행하였다. 인터뷰 종료 이후 내용 확인을 위해 재질문이 필요할 경우 유선 전화를 통해 추가 답변을 확보하였다.

3.3.3 자료 분석

본 연구의 인터뷰 내용은 화상회의(WebEX)에서 제공하는 기능을 사용하여 녹화가 진행되었다. 녹화된 자료는 영상을 제외하고 음성만을 mp3 형태로 별도 추출한 뒤, 네이버 크로바노트를 이용하여 발화자 단위 텍스트 파일로 변환하였다. 전체자료는 Microsoft Word 문서로 전환한 후 오탈자 수정·보완 작업을 거친 뒤 질적 자료 분석 소프트웨어인 Nvivo에 등록하여 분석하였다. 수집된 자료는 반복적으로 검토하면서 도구·장비와 경험적 단위를 코딩하였다. 자료 분석의 연구자 신뢰도 향상을 위해 동료 평가(Peer-Review)를 실시하여 검토 및 토의하는 과정을 통해 주요 이슈를 도출하였다.

3.3.4 결과 검증

도출된 도구·장비 목록 검증과 9개 영역 중 논의가 필요한 사항에 대한 의견을 수렴하기 위해 추가 인터뷰((5차: '22.12.17)를 수행하였다.

4. 연구결과

4.1 네트워크 구성

네트워크는 폐쇄망으로 구성하는 것에 적절하다고 하였으나, 물리적으로 분리된 별도 상용 인터넷망 구성하여 일반 검색 및 SW 업데이트를 할 수 있도록 해야 한다는 점에서 의견 차이가 있었다. 인터넷 불법 사이트 수사는 악성코드감염에 상시 노출되어 있으므로 업무용 인터넷망과 상용 인터넷망을 별도로 사용할 수밖에 없다. 반면에 지자체는 민생 범죄를 대상으로 수사가 이뤄지므로 상용 인터넷망을 통해 행정업무를 병행하는 네트워크 구성으로 사용하였다. NAS는 기본 장비로 반영하고, 6개월 이상 보관을 위한 별도 백업 서버가 필요하다는 의견이 존재하였다, 구체적으로 QNAP과 Synology 제품군을 제시하였다. 네트워크 기반 서버 처리 인프라에 대해서는 성능만 보장된다면 향후 적용 가능하다는 의견과 분석실로부터 케이블을 연장하여 사무실에서 작업하는 사례도 소개되었다.

☞ "최근에는 분석 자동화 방식을 적용하는데, 이미징을 뜨고 네트워크로 전송해서 NAS에 업로드합니다. 원격 접속으로 프로세싱한 후 그 결과에서 분석할 데이터만 개인 PC에 가져와서 분석하는 조직도 있습니다." (참여자 1)

☞ "소규모 특사경 1~2명의 경우는 서버급으로 구축하는 것이 부담되고 워크스테이션을 구비한 상태에서 NAS를 통해 개인이 관리합니다. 그런데 한 5~10명 정도 되면 서버에서 중앙관리하는 시스템 구성도 괜찮을 것 같습니다." (참여자 2)

☞ "NAS도 좋지만 SAN 스토리지 형태로 구성 시 장비의 생애주기 관리가 용이해서 관리소요가 줄어드는 장점이 있습니다." (참여자 15)

☞ "분석관 중에 서버에서 케이블을 길게 연장해서 본인 책상에서 작업하시는 분도 있습니다. 최근 사건들은 NAS에 보관하는데 오래된 사건들은 데이터 스토리지가 따로 있습니다. 그래서 보통은 6개월 정도 있다가 NAS에서 스토리지로 옮기는 데이터 백업 서버도 따로 있습니다." (참여자 7)

☞ "검찰 같은 경우에는 2013년도 경에 VM에다가 분석용 도구를 올려서 사용하는 방안을 시도했었습니다. 실제 구축이 됐는데 문제는 리소스 부족 및 속도 저하로 당시에는 기술이 현재에 비해 낮은 편이었습니다. 그래서 한 2년 정도 운영을 하다가 접었던 적이 있습니다." (참여자 5)

☞ "포렌식 센터 내부에 폐쇄망에서는 업무를, 인터넷망에서는 검색 및 불법사이트 조사 등을 합니다. 센터 인터넷망은 회사 메인 인터넷망하고 분리되어 있습니다." (참여자 9)

☞ "국가에서 클라우드 형태로 디지털 증거분석 인프라를 구축하거나, 업체 측에서 클라우드 기반 디지털포렌식 서비스를 제공해주는 방안도 고려해 볼 수 있겠습니다." (참여자 15)

☞ "어떤 특정 공간 내 자료 존재의 두려움으로 클라우드에 대한 거부감이 있습니다. 프로세싱 자원만 활용하고 증거 데이터는 각 기관이 보유하는 방안도 검토가 필요합니다." (참여자 14)

☞ "인하우스 형태로 클라우드를 구현할 경우 데이터 보관·삭제·복구 이슈가 문제 될 수 있습니다." (참여자 13)

4.2 분석관 컴퓨터

분석관 컴퓨터는 분석과 행정업무를 구분하여 장비를 준비할 것인지, 1대의 컴퓨터에서 2개 업무를 병행하여 처리할 것인지와 디지털증거분석실 내에 상용인터넷 컴퓨터 설치 여부에 대해 의견 차이가 존재하였다. 워크스테이션의 수량 및 사양 등에 대해서도 논의가 이뤄졌다. 1인 지급 수량으로 내·외부망 업무용 PC 각 1대, 컴퓨터 및 모바일 분석용 워크스테이션이 각 1대씩 도출되었다. 다만, 조직의 규모 및 특성에 따라 수량에 일부 차이가 있었다. 워크스테이션 지급 기준으로 1인당 1개 지급, 특사경에서 주로 구동하는 도구에 맞춰 지급, 개인별 지급은 하되 공용 워크스테이션을 별도 구비하는 의견으로 차이가 존재하였다. 노트북은 1인당 1대씩 제공하거나 공용으로 사용하기도 하였다.

☞ “디지털포렌식 분석관 워크스테이션을 각 2대씩 가지고 있는 걸 생각을 하고 있습니다. 1대는 컴퓨터용, 1대는 모바일용 또는 1대는 이미징 작업 동안 분석용으로 사용할 수 있습니다.” (참여자 2)

☞ “경찰의 경우는 분석망에 워크스테이션 2개가 연결되어 있습니다. 온나라 용도로 일반 PC가 하나 있고 인터넷도 하나 있습니다.” (참여자 3)

☞ “검찰은 분석망 워크스테이션 1대, 인터넷망 1대, 자체 이프로스망 내부망에 1대, 총 3개가 들어가는데 이건 개인 지급 장비고 모바일 같은 경우는 워크스테이션이 팀마다 다른데 한 3~4대씩 같이 놓고 공용으로 사용하고 있습니다. (참여자 5)

☞ “의미 있는 데이터를 도출하고 분석보고서 작성하는 시간도 필요하므로 업무 특성에 따라서 2대 또는 3대 정도가 괜찮을 것 같습니다.” (참여자 6)

☞ “저희는 업무용 2대, 분석용 워크스테이션 2대, 총 4대가 되는데 KVM 스위치를 통해 모니터 2대 놓고 전환하는 구성으로 쓰고 있습니다.” (참여자 9)

4.3 개인 도구 및 장비

개인 도구·장비는 컴퓨터의 경우 EnCase, FTK, X-Ways, AXIOM, 모바일의 경우 Macquisition(Cellebrite digital collector), UFED, MD-NEXT 및 MD-RED 등을 도출하였다. 또한, Chip-Off나 J-TAG는 사례가 적고 분석관의 숙련도 등을 고려할 때 2인 이하에게는 필요하지 않고 쉴드룸 역시 쉴드팩 또는 패러데이 팩으로 대체가 가능다는 의견이 주를 이루었다. 디지털증거분석실 구성 시 사용자 편의성을 우선순위로 하여 도구를 도입한 조직도 있었다. 지자체 특사경은 민생 범죄 수사로 인해 컴퓨터와 모바일이 대부분이며, CFT·DFT를 주로 사용하는 것으로 확인하였다.

☞ “X-Ways하고 EnCase, FTK 그 다음에 Falcon을 제일 많이 사용하고 있습니다. 모바일 같은 경우는 한컴 GMD의 MD-Next, MD-Red, 파이널 포렌식과 같이 국내 도구들은 국내 휴대폰에 대해서 분석이 잘 됩니다.” (참여자 3)

☞ “특사경 같은 경우에는 CFT·DFT라는 제품을 많이 사용합니다. 자격증, 법원의 증언, 상징성, 전문성 때문에 EnCase 같은 제품들은 기본적으로 들어가고 최근에는 AXIOM도 많이 사용합니다.” (참여자 4)

☞ “1명당 워크스테이션과 노트북 각 1대, 컴퓨터 SW는 EnCase랑 X-Ways만 있으면 될 것 같습니다. 그리고 Cellebrite digital collector가 괜찮은 것 같습니다. 모바일은 UFED도 괜찮지만 국내는 MD 시리즈가 잘 반영하고 있습니다.” (참여자 7)

☞ “컴퓨터 쪽은 EnCase, 모바일은 파이널 데이터 정도 사용하고 있습니다. 현재는 대검에서 지급한 CFT·DFT도 사용하고 있습니다.” (참여자 10)

☞ “Intella의 경우 현재는 잘 사용하지 않습니다. Nuix가 해당 제품의 기능을 포함합니다.” (참여자 13)

☞ “규모가 얼마되지 않은 조직은 Chip Off나 J-Tag은 수요가 적고, 업체에 위탁하여 처리합니다.” (참여자 14)

☞ “CFT·DFT는 수사/조사기관에만 배포하기 때문에 민간 조직에서 활용하기 어렵습니다. 이와 유사한 제품으로 DFARS Pro가 있습니다.” (참여자 15)

4.4 이미징 장치

이미징 장치는 제품군이 한정되어 있고 기본 장비로 인식하고 있었으나, 보유 수량과 활용 방식에 대한 의견 차이가 존재하였다. 압수수색 출동 장소에 따라 수량을 산정해야 한다는 의견이 제시되었고, 현장에서 이미징 작업이 많을 경우 논리적 방식을 우선적으로

채택하며, 논리적 이미징 도구는 CFT·DFT와 FTK Imager를 많이 사용하였다. 이미징 장치는 대다수가 Falcon 제품을 사용하고 있었으며, 외부용은 압수수색 간 이미징, 내부용은 완전삭제 및 이미징 용도로 사용하였다. 현장 출동의 경우 논리적 이미징을 통한 선별 압수 수요가 많고 CFT·DFT 개선 방안에 대한 의견도 제시되었다. 디지털증거분석실 규모가 10명이 초과할 경우 이미징 장치를 사건 단위로 구비해야 한다는 의견도 제기되었다. 또한, 저장매체 용량의 증대에 따라 현장 이미징의 활용도는 줄어들고 있다는 의견에 대부분 동의하였다. 휴대폰은 대부분이 원본 압수를 진행하는 것으로 확인되었다.

☞ “2개 이상을 구입한다면 서로 다른 장비를 구입하는 게 좋다고 생각합니다. 왜냐하면 디스크나 수집 장비가 하드웨어 특성을 탑니다.” (참여자 1)

☞ “논리적 이미징은 현장에선 CFT·DFT, 내부는 FTK Imager도 사용합니다.” (참여자 2)

☞ “현장에서 이미지 뜨려고 하면 예를 들어서 1TB 뜨는데 Falcon이 한 1시간 정도 예상합니다. 4TB를 복제하면은 한 3~4시간 정도 소요됩니다. Falcon Neo가 4개씩 연결합니다.” (참여자 3)

☞ “내부에서도 전처리실에 Falcon 비치해놓고 디스크를 와이핑을 한다든지 DVR 같은 경우는 디스크 대 디스크로 작업을 합니다.” (참여자 6)

☞ “한 3년치 통계를 내보면 1년에 약 150개 매체 정도를 작업합니다. 약 50회 정도 현장 출동하며, 거의 압수 영장입니다. 방문 판매업이 양이 많고 현장에 가면 PC가 많습니다. 대부업이라든가 아니면 상표법 위반, 식품 위생, 보건, 의약 순으로 있습니다. 지자체 기준으로 한다고 하면 기관당 1대 정도 있으면 될 것 같습니다.” (참여자 10)

4.5 전용 SW

EnCase는 기능 개선 및 성능 부족으로 근래에는 활용도가 부적합하다는 의견이 있었으며 법정에서의 인정 여부, 인지도, 시장 점유율 등을 고려하여 기본 도구에 포함해야 한다는 의견 차이가 있었다. 이외에도 컴퓨터 포렌식 전용 SW로 X-Ways, AXIOM, FTK 등이 추가로 제시되었다. 모바일 포렌식 도구는 MD 시리즈와 Cellebrite 제품군을 추천하였다. 또한, 교차 분석 및 검증 용도로 다수의 도구를 보유하는 것을 추천하는 의견도 존재하였다. 추가적으로 맥용 이미징을 위한 Cellebrite digital collector, 분석을 위한 Cellebrite Endpoint inspector, 메일 분석용 Intella, 문서암호 해독에 활용되는 Passware Kit, 영상 포렌식의 필요성 등이 언급되었다. 조직의 특성에 따라 공공분야에서 사용하는 메신저 분석을 위한 코드 개발의 필요성과 철도경찰대의 경우 영상 분석을 위한 도구 개발 등에 대한 의견도 있었다. PC와 모바일의 분석 비중은 기관에 따라 차이가 있었다. 조직/기관의 업무 특성에 따라 요구되는 SW에 차이가 있었다. 예를 들어, 불법 사이트 서버를 압수·수색하는 조직은 WAS나 DB에 대한 분석이 필요하므로 데이터베이스 포렌식 SW, CCTV 분석이 많은 조직은 영상복원 SW, 계좌 및 통신자료를 수사하는 조직은 별도 포렌식 SW를 사용하고 있었다. 지자체는 대검찰청에서 개발 중('22년 12월까지 구축 예정)인 ‘국가 디지털포렌식 클라우드 시스템’(이하 ‘NDFaaS’)을 통해 분석 서비스를 지원받고 있었다. NDFaaS는 국가 디지털포렌식 클라우드 시스템으로 증거분석·관리, 사건 관리, 빅데이터 처리 및 클라우드 플랫폼 구축을 목표로 하며, 디지털증거 통합분석 및 송치업무를 지원한다[22].

☞ “Mac 관련 획득을 지원하는 Cellebrite digital collector, 분석 도구인 Cellebrite Endpoint inspector가 있습니다. 메일 분석에 특화된 Intella, 암호를 해제하는 Passware Kit도 있습니다.” (참여자 4)

☞ ″공공의 경우 문서 추출 요구사항이 많고 기관들마다 메신저가 달라 개발을 통해 데이터를 직접 추출해야 분석이 가능합니다.” (참여자 7)

☞ “철도경찰대는 기관 특성상 CCTV 영상복원, 손상된 영상 파일 복구 SW를 사용합니다. 열차 내 설치된 블랙박스 또는 초동 수사 시 CCTV를 활용하는 수사가 거의 90% 이상입니다.” (참여자 12)

☞ “불법 사이트 또는 사설 게임 서버를 압수수색 하는 경우 PC 자체가 서버 역할을 하고 데이터베이스 및 서버 운영이 필요한 것들이 설치돼 있어서 데이터베이스 포렌식도 필요합니다. (참여자 9)

☞ “계좌 자료하고 통신자료들을 기관에서 각 은행이나 통신업체에서 받아서 각 수사단 별로 분석합니다. 대검에서 클라우드 시스템을 개발 중으로 현

재는 계좌 분석이 가능합니다." (참여자 10)

☞ "철도 사고 같은 경우는 CCTV보다도 열차가 운행할 때 생기는 전기신호 또는 열차 자체의 속도나 전압 같은 정보가 필요해서 별도로 열차 운행 정보 분석 프로그램이 필요합니다." (참여자 11)

4.6 오픈소스 SW

오픈소스에 대해서는 구매 및 유지비용이 없으며 개인에 따라 선호 도구에 차이가 있고, 기술 변화에 따라 활용 대상 도구가 달라질 수 있으며, 변호인 참관 시 제품 안정성 및 신뢰성 등을 이유로 사용하지 않는다는 조직도 존재하였다. 많이 활용하는 오픈소스 SW로는 이미징을 위한 FTK Imager, 파일 검색 용도인 Everything, 파일의 해시 값 계산 시 활용하는 HashMyFiles, 프로세스 모니터링을 하기 위한 Sysinternals의 Procmon, 데이터베이스 분석을 위한 SQLite 등이 언급되었다. 대부분이 국가보안기술연구소에서 제작한 CFT·DFT를 사용하고 있었다. 오픈소스 활용 가이드 제공 방안으로 치트시트 및 명령어 셋 정리·공개, 기능별 해시태그 부착 등의 아이디어가 제시되었다.

☞ "오픈소스라는 게 1년만 지나도 유행하는 제품이 다릅니다. 때문에 오픈소스는 사실상 리스트업으로 제공하는 게 중요할 것 같습니다." (참여자 1)

☞ "DEFT든지 SIFT 같은 경우는 업데이트가 잘 안 되는 것 같고. Paladin는 상용화됐는데 수사기관 쪽에는 무료로 제공되는 것 같습니다. 이미징 도구는 FTK Imager, 그리고 Nirsoft쪽 오픈소스 도구도 많이 쓰고 있습니다." (참여자 5)

☞ "FTK Imager, Arsenal Image Mounter, MFT 분석 및 Sysinternals의 Process monitor, RegMon, Autoruns 등도 많이 사용합니다. 루트킷 찾아내는 GMER도 많이 사용합니다. 네트워크는 Network Miner나 WireShark도 있습니다." (참여자 7)

☞ "여러 가지 불법 복제물들이 있는데 영화, 웹툰, 드라마 등 동영상 파일들을 빠르게 검색하는 everything 도구를 사용합니다. 그리고 해시를 구할 수 있는 HashMyFiles도 사용합니다." (참여자 9)

☞ "Sysinternals의 프로세스 모니터라든지 이런 도구도 활용하고 있습니다. 데이터베이스를 추출하기 위해서 SQLite를 사용하기도 합니다." (참여자 9)

☞ "조직 규모 및 예산에 따라 상용 SW를 사용하지 못할 경우 오픈소스가 대안이 될 수 있습니다. 상용 SW에서 제공하지 않는 기능을 오픈소스가 지원해주는 경우도 있습니다." (참여자 15)

4.7 공용 도구·장비

증거보관함과 CCTV, 네트워크 및 서버/VPN, 증거물 촬영 보조장비 등이 공용 장비로 제시하였다. 케이스 관리 시스템은 2인 또는 5인 이하에는 엑셀로 관리가 가능하지만 조직 규모가 증가할 경우 케이스 관리 시스템이 필요하다는 의견에 동의하였다. 이외에도 증거물의 냄새를 제거용도인 흄후드, 공기청정기, PC 에어컴프레셔, 프로젝터, 트레일러 등을 제시하였다. Chip-Off 및 J-Tag은 소규모 조직에는 적절하지 않다는 의견이 대다수였다. 요청 사례가 1년에 몇회 되지 않고 최근에 출시되는 모델은 암호화 기술을 적용하므로 도입 비용 대비 효익이 낮다는 의견이었다. 또한, 상위 부서/조직의 시스템과의 연계 또는 분석 지원이 필요하다는 의견도 있었다.

☞ "이미징 장비와 같이 수집과 관련된 모든 도구들은 공용으로 하는 것이 좋을 것 같습니다. 5인 이상 네트워크 기반 증거처리 인프라의 서버급 장비들도 공용으로 봐야 합니다." (참여자 1)

☞ "휴대폰 물리 복구 장비 금액이 7천만 원이 넘습니다. 1년에 1~2건 정도의 수요로 대검에 분석의뢰하는 게 나을 것 같습니다." (참여자 2)

☞ "증거 보관용 키락, 보안 CCTV, 비디오카메라, GPS 등 장비도 포함되어야 합니다." (참여자 5)

☞ "저희는 디지털증거 통합 관리시스템을 쓰고 있습니다. 이전에는 2~3명 근무 시 증거물 관리 대장을 엑셀로 작성하여 분석관이 접수부터 증거물 반환까지 수기로 작성했습니다." (참여자 8)

☞ "증거물 촬영 시 업무용 핸드폰이 가장 효율적이라고 생각합니다. 다만, 경찰과 같이 주취자들을 대응해야 하는 상황일 경우에는 바디캠이 필요할 수 있습니다." (참여자 14)

☞ "압수수색 시 돈을 이체받을 수 있는 가상자산 지갑이나 콜드 월렛(Cold Wallet)도 검토해볼 필요가 있습니다." (참여자 13)

4.8 액세서리

정전기 방지 봉투 규격 및 유형에 대한 의견과 모바일 액세서리는 케이블과 SD 및 USIM 리더기가 공통적으로 도출되었다. 현장 출동용 캐리어, 압수수색용 박스, 드라이버 셋과 함께 현장 출동용 키트 목록이 필요하다는 의견을 확인하였다. 추가로 핸드폰 멀티충전기, 증거물 건조용 드라이어, 일정 전압 수치를 유지시켜주는 레귤레이터, 멀티탭, 정전기 방지 장갑, 휴대용 마우스·키보드 세트 등의 목록을 도출하였다. 또한, 참관실 내 TV 크기와 증거물 봉인 해제 시간을 기록하기 위해 GPS 시계를 활용하는 방안도 제시되었다.

☞ “드라이버 킷은 아이픽스 프로 툴킷, 현장용 하드디스크 독, 휴대용 프린터, 외장에 붙일 수 있는 케이블 셋이 필요합니다.” (참여자 1)

☞ “모바일 쪽에 안드로이드 C-Type 5핀, 15핀, 30핀 케이블 및 SD·USIM 카드리더기가 포함되어야 합니다. 정전기 방지 봉투 및 충격 완충제가 포함된 봉투도 필요합니다.” (참여자 4)

☞ “하드웨어 M.2, SATA라든지 케이블 특성을 많이 탑니다. 또한 각종 젠더들도 많이 필요합니다. 레귤레이터도 필요합니다.” (참여자 7)

☞ “증거물 촬영은 개인 폰으로 찍어서 자료 이동하는 것이 더 빠릅니다.” (참여자 8)

☞ “75인치 TV를 참관실에 설치했습니다. 참관인들 방문 용도 외에 CCTV 영상 확인 및 업무용 PC를 통해 회의용으로도 활용합니다.” (참여자 11)

☞ “조직에 따라서 임의제출 형태로 논리적 이미징이 아닌 파일 형태로 받아오기도 하기 때문에 보안 USB도 반영되어야 합니다.” (참여자 13)

4.9 기타 고려사항

현실적으로 가장 어려운 점이 공간 확보의 문제이므로 2인 또는 5인 이하 구성 시 구획 분할 및 할당, 그에 맞는 도구·장비가 고려되어야 한다는 의견이 제시되었다. 추가적으로 공간 구성 원칙 수립, 전처리실 필요 여부, 접수실과 참관실 내의 CCTV 녹화 유무, 참관실의 구성 및 참관인과의 이격 대책 등이 논의되었다. 보안 관련 이슈로 참관실 내부 시야 차단 대책, 분석실로 이동 시 출입 통제 방안(디지털 도어락, 공무원증 활용), 기타 보안대책(출입 통제구역 표지판 및 출입자 명부 비치)과 증거보관실 대안으로 금고 또는 이중케비닛 활용 사례, CCTV 화면을 확대해서 참관인실에 표출하는 사례 등이 소개되었다. 디지털증거분석실 대부분이 독립된 시설이 아닌 조직의 건물 내에 위치하기 때문에 자체 UPS보다는 통합 시설의 인프라 요소를 활용하고 있었다.

☞ “2인 기준으로 분석실과 참관/참여실은 기본으로 들어가야 됩니다. 그리고 전산실은 2인 규모에 항온항습기를 대신 분석실 내 별도 Rack을 통해서 구축하는 방법도 있습니다.” (참여자 4)

☞ “기본적으로 증거물은 CCTV 시야 밖으로 빠져나가지 않도록 범위를 도식화해서 최소 몇 군데 설치해야 하는 기준이 필요합니다. 반대로 분석관 자리는 개인 프라이버시를 고려하여 CCTV 시야가 가지 않도록 해야 합니다.” (참여자 5)

☞ “국제 인정 ANAB 심사 시 망 분리뿐만 아니라 공간의 분리도 점검했습니다. 카페트에 대한 정전기 방지 여부 등도 확인했습니다.” (참여자 9)

☞ “UPS 전원은 서버 등 정보시스템은 상시전원공급라인에 연결되어 있고 시설 내에서 제공하는 UPS에 연결돼 있습니다.” (참여자 10)

4.10 디지털증거분석실 도구·장비 도출

포커스 그룹 인터뷰 결과, 디지털증거분석실 구성에 필요한 도구·장비 목록을 도출하였다<표 3>. 크게 컴퓨터와 모바일 영역으로 구분하여 필요한 하드웨어, 소프트웨어, 악세사리 등으로 분류하였으며, 인터뷰 간 언급된 기관의 특성을 고려한 특정 수사·조사에 필요한 도구들에 대해서는 특화 영역에 반영하였다. 디지털증거분석실 내에 공동으로 활용이 가능한 도구·장비들은 공용 영역으로 구분하고 현장 출동용 키트, 증거물 촬영, 공용 이미징 장치, 접수/전처리, 참여/참관, 보관, 전산/네트워크, 안전/보안, 사무, 시설/인프라, 기타 항목으로 세분화하였다. 이렇게 도출된 목록은 기존에 도구·장비 목록의 범위에서 한 단계 더 나아가 시설·환경 관점까지 확대한 것으로서 디지털포렌식 기능을 신규로 구성하거나 기존에 디지털증거분석실을 운영·유지하는 조직/기관들이 이를 참조하여 개선할 수 있는 장점이 있다.

<표 3> 포커스 그룹 인터뷰 결과 도출된 디지털포렌식 도구·장비 목록(안)

구분			도구·장비 목록
컴퓨터	HW		• 워크스테이션 • 쓰기 방지 장치(설치/휴대) • PC / 노트북(내부/인터넷) • 모니터(보안 필름)
	SW	포렌식	• CFT·DFT(수사/조사 기관에만 제공), AXIOM, X-Ways, EnCase, FTK • PasswareKit • Cellebrite digital collector • Cellebrite Endpoint inspector
		기반/지원	• Vmware • Windows/Mac OS • MS-Office(Excel, Powerpoint, Word) • 한글 문서편집기
	악세사리		• 케이블, 드라이버 키트, 이동식 외장하드/USB, HDD독, KVM 스위치
모바일	HW		• 모바일 복구 장비(J-Tag, Chip-off)
	SW		• Cellebrite UFED • MD-Next, MD-RED • Final Mobile Forensic
	악세사리		• SD 카드리더기, USIM 리더기 • 핸드폰 케이블(C-Type, 5/15/30핀등) • 휴대폰 멀티 충전기(10구) • 모바일 액세서리 키트
특화	SW		• Nuix • ChainAnalysis • Sentinel • I2 • 기관의 특성을 고려한 분석 SW(공공메신저, 철도 등)
공용	현장 출동용 키트		• 가방 또는 캐리어 또는 박스 • 노트북(CFT·DFT, FTK Imager 등 포함) • 물리적 쓰기방지장치 • 간이 키보드/마우스 • 휴대용 프린터 • 정전기 방지 봉투/가방 • 보안 USB • 외장형 USB/CD-ROM • 외장형 저장장치(SSD, HDD) • 부팅가능 USB/CD 매체 • 케이블, 젠더, 드라이버 킷, 플라이어, 멀티탭, 손전등 • 메모장 및 도구(CoC 문서) • 바디캠 or 업무용 핸드폰 or 디지털카메라
	증거물 촬영		• 접이식 카메라, GPS 시계, 캠코더, 조명, 증거물 촬영 보조장비(증거물 비치판 등)
	공용 이미징 장치		• TX-1, Falcon
	접수/전처리		• 패러데이팩 • 쉴드팩 • 라벨지 • 봉인지 • 정전기 방지 봉투
	참여/참관		• 무선 키보드/마우스 세트 • 대형 모니터
	보관		• 증거물 보관함 또는 박스 • 내화금고 • 캐비닛 • 시건장치(Key-Lock)
	전산/네트워크		• 스토리지 : NAS(Synology, QNAP 등) or SAN(DAS) • 스위칭 허브/라우터 • 공용 워크스테이션 • Rack(서버, VPN, DRM, 백업솔루션)
	안전/보안		• 화재감지기/연기탐지기 • 화재진압 소화기 • 항온항습기 또는 온/습도 경보장치 • 자가전력(건전지, 배터리) 비상조명등 • 누수감지기 • 로깅이 되는 인원출입 통제 시스템(지문, 카드키, PIN번호 등) • CCTV(NVR, 서버 등)
	사무		• 빔프로젝터 • 세절기 • 공기청정기 • 복사기 또는 디지털복합기
	시설/인프라		• TPS(통신)/MDF(메인)/EPS(전기)/IDF(중간) • UPS 또는 비상발전기
	기타		• 드라이어 • 흄후드 • 에어컴프레셔 • 핸드 카트 • 보호(통제, 제한)구역 표지판 • CCTV 촬영 안내 표지판 • 가상자산 계좌번호 or 콜드월렛

5. 발전방안

5.1 디지털증거분석실 공간/도구·장비 목록 표준화

디지털증거분석실은 각 기관/조직별 할당 예산이 다를뿐더러, 공간 확보 또한 쉽지 않은 실정으로 이에 대한 기준 수립이 필요하다. 공간의 경우 설계 시부터 디지털포렌식 기능을 고려하지 않을 경우 대부분의 기관/조직이 기존에 보유한 시설 내 일정 영역을 재활용하는 형태로 운용하고 있다. 또한, 디지털포렌식 도구·장비의 규모와 수량 등을 고려하지 않고 일반적인 행정업무 공간 기준에서 할당을 하다 보니 실제 분석관이 사용할 수 있는 영역은 매우 열악한 상황이다. 도구와 장비 역시 기관/조직에서 할당된 예산에 맞춰 구매·운용함으로 인해 일부는 부족하거나 외부 지원을 통해 분석의뢰를 해결하는 경우도 존재한다. 이에 따라 디지털증거분석실 구성 시 소요되는 공간/도구·장비에 대한 기준을 수립할 필요가 있다. 도구·장비의 경우 참조할 수 있는 표준 목록 및 예산을 제시하고 각 기관/조직의 특성과 환경에 맞게 선별적으로 채택할 수 있도록 하는 것도 하나의 방법이 될 수 있다. 이처럼 디지털증거분석실 구성을 위한 공간/도구·장비 목록의 표준화는 국내 디지털포렌식 기능을 신설하거나 유지·개선하고자 하는 기관/조직의 예산 및 공간 확보 시 참조 근거가 될 수 있으므로 향후 연구 시 고려되어야 한다.

5.2 디지털포렌식 조직/기관 육성

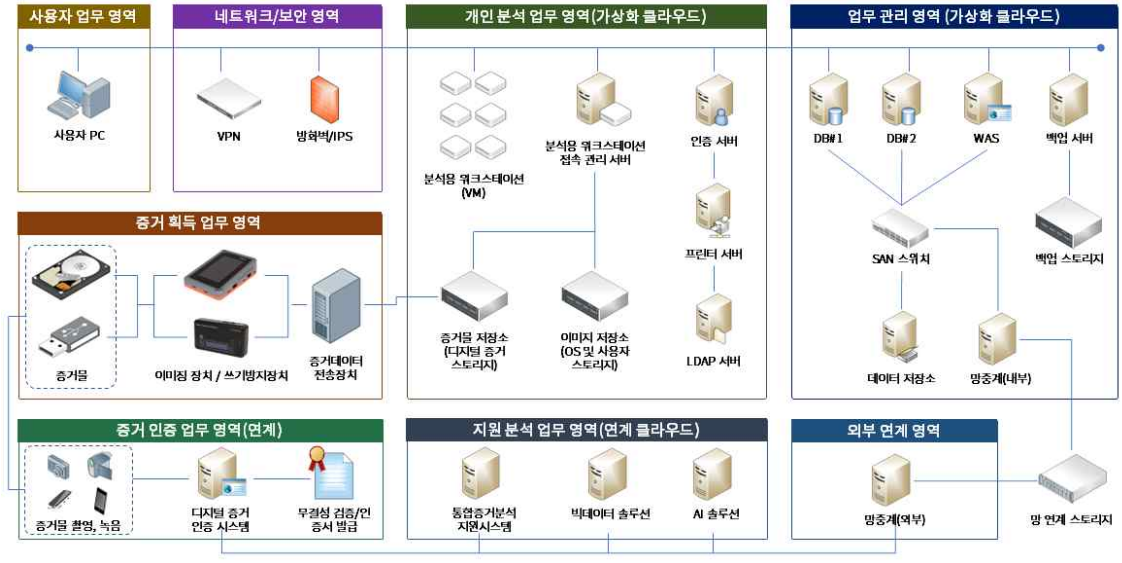
경찰청 디지털포렌식 센터의 경우 특사경 뿐만 아니라 출입국, 감사원, 철도, 지자체 등 다른 국가기관에 대한 디지털증거분석 의뢰를 협력 차원에서 지원하고 있다. 하지만, 증거분석 이외에 도구·장비에 대한 지원은 미비한 실정이다. Nuix와 Chainalysis의 같이 고가의 구매·유지 비용이 소요되는 도구·장비들은 특사경이나 지자체에서 자체적으로 구비하거나 활용이 어렵고, 소규모의 디지털포렌식 조직은 요청되는 증거분석 형태에 대응하는 적절한 도구·장비를 상시적으로 갖추기에는 한계가 존재한다. 이러한 문제들은 단기적으로는 유관 수사기관 및 협력업체 지원을 통해 임시방편의 형태로 해소가 가능할 수 있으나 중·장기적으로는 적절하지 않다. 대안으로 디지털포렌식 도구·장비를 민간업체로부터 리스/렌트 형태로 활용하는 방안, 디지털포렌식 서비스를 케이스 건별로 위탁하는 방안, 일정 예산 범위 내에서 필요에 따라 도구·장비를 업체로부터 자유롭게 지원받는 방안 등 디지털포렌식 기업의 지원·위탁 체계를 수립하여 증가하는 디지털증거분석 수요를 민간 시장과의 공유를 통해 해소할 필요가 있다. 디지털포렌식 업무를 민간에게 지원·위탁하는 정책 체계를 개편·확대가 선행됨으로써 업체와의 기술 교류는 물론이거니와 디지털포렌식 기업을 확대·육성하고, 시장을 선순환할 수 있도록 생태계를 조성해야 한다. 아울러 영국의 FSR의 사례와 같이 민간 기업의 디지털포렌식 서비스 품질 수준을 유지하고 지속적으로 모니터링할 수 있는 대응책 또한 강구해야 할 것이다.

앞서 기술한 민간 위탁 외에도 국가적으로 디지털증거분석 도구·장비 지원 창구와 방법을 다각화할 필요가 있다. 국가와 민간이 협업하여 클라우드 환경에서 디지털포렌식 전처리가 가능토록 인프라를 지원해주는 방안, 증거분석 업무 지원에서 도구·장비 대여, 분석/실습용 이미징 파일 제작 및 공유, 경찰 또는 대검찰청의 디지털증거분석 플랫폼 연계 등을 통한 통합 지원 방안 등을 강구해야 한다. 또한, 시시각각으로 변화는 오픈소스의 경우, 주기적으로 디지털포렌식에 활용가능한 도구 목록을 공개하고 이를 사용하는 방법을 공유할 수 있는 환경에 대한 지원도 필요하다. 어떤 아티팩트에 대해 획득과 분석이 필요할 경우 기관/조직의 상황에 따라 상용 도구·장비를 활용하기 어려운 상황을 염두해두어 오픈소스 SW 목록과 치트시트 및 명령어 셋, 기능 별 해시태그 부착 등을 정리·공개하는 등 포탈 형태로 관리한다면 산·학·연의 참여를 늘릴 수 있고, 이를 기반으로 디지털포렌식에 대한 다양한 활동을 공유할 수 있다. 예를 들어, KISA의 사이버 보안 취약점 정보 포탈과 같은 정보공유 체계의 활용 사례를 참조할 수 있을 것이다. 디지털포렌식 신규 아티팩트 발굴 포상제를 적용함으로써 드론, IoT 기기와 같이 다양화, 대량화된 디지털 장치에 대한 아티팩트 DB를 국가적으로 구축하고 공유할 경우, 산업계에서는 이를 참고하여 디지털포렌식 제품에 대한

사업 육성에 기여할 수 있으며, 학계 및 연구분야에서도 교육자료 활용 및 연구개발에 활용할 수 있다. 다만, 취약점에 이용될 수 있거나 민감한 내용을 처리할 수 있는 정보에 대해서는 접근권한을 차등 부여하거나 수사기관/조직만의 별도의 페이지를 운영하여 공개할 수 없는 중요 사례에 대한 공유 또한 가능할 것이다. 더불어 신규 아티팩트가 식별·등록되었을 경우 분석관들이 상호 교차 검증할 수 있는 환경을 조성·제공함으로써 제시된 아티팩트에 대한 분석관의 전문성을 제고할 수 있는 방안도 고려되어야 한다. 나아가 소프트웨어 기술자 경력관리시스템 사례를 개선하여 분석관들의 교차검증 및 아티팩트 등록·개선 이력 등을 관리할 수 있는 플랫폼을 제공함으로써 법정에서 전문가 증언 시 분석관의 경험을 증빙할 수 있는 자료로 활용이 가능하다.

5.3 디지털증거분석실 미래 설계방안

디지털증거분석실은 소규모 형태가 대다수이며, 디지털증거를 처리하는 업무 특성 상 폐쇄형 네트워크 구성이 주를 이루고 있다. 이에 따라, 현재는 개별 워크스테이션에서 증거 분석을 진행하고 NAS를 통해 증거물을 관리하는 정도에서 그치고 있다. 하지만, 앞으로 기술발전에 따라 증거를 복합적으로 처리하고 고성능의 클라우드 기반 하드웨어에서 분산처리를 하는 형태로 인프라 구조를 개선시킬 필요가 있다. E-Discovery의 경우 Lit i View, Relativity와 같이 웹기반 환경에서 증거물을 분석하고 다수의 분석관들이 동시 접속해서 협업을 할 수 있는 방식을 도입·확대하는 방안도 고려해볼만 하다. 더불어 대검찰청의 '국가 디지털포렌식 클라우드 시스템'(이하 'NDFaaS')의 사례와 같이 클라우드 기반에서 사건·증거관리 및 분석을 진행할 경우 소규모 기관의 예산의 중복 지출을 최소화할 수 있고, 고성능의 하드웨어 자원을 사용할 수 있으며, 빅데이터·AI 기술을 활용함으로써 효율적인 증거분석이 가능할 것이다. 나아가 워크스테이션 급의 가상머신이 도입될 경우 분석관은 개인 PC에서 클라우드 상의 개별적인 가상 워크스테이션에 접속하여 작업함으로써 업무영역과 분석영역을 분리할 수 있다. 사용자 이미지 저장소와 운영환경을 별도 스토리지에 저장하여 마운트하는 방식으로 동작하기 때문에 디지털증거분석실 공간 활용 및 예산 절감 효과 또한 얻을 수 있다. 증거 획득 업무 영역은 향후 유·무선 네트워크 인프라 고도화 및 증거 획득 속도 개선이 이루어진다는 전제 아래 현장에서 데이터를 획득함과 동시에 증거물 저장소로 실시간으로 업로드하여 절차의 간소화를 달성할 수 있을 것이다. 더불어 국립과학수사연구원의 디지털증거물 인증서비스(DAS) 개념을



(그림 1) 차세대 디지털증거분석 인프라 구성도(안)

개선하여 획득과 동시에 증거물에 대한 원본성을 보증하고 이를 분석 업무영역에서 즉각적으로 활용할 수 있다면 디지털증거에 대한 무결성과 증명력도 확보할 수 있다. 여기에 케이스 및 증거관리 영역을 웹 기반 형태로 구현함으로써 엑셀 형태의 수작업으로 이뤄지던 행정상의 불편함과 분석관 인사이동에 따른 케이스 인수인계 절차의 어려움 또한 개선할 수 있다. 추가적으로 케이스 히스토리 유지, 통계 분석 등을 통한 실적 관리 및 케이스 공유 기능을 통해 관련 조직 간의 사건 정보를 상호 확인할 수 있다는 점에서 장점이 있다.

6. 결 론

본 논문은 국내에서 디지털증거분석실 구축 시 소요될 수 있는 도구·장비에 대해 탐색적 연구를 수행하였다. 디지털포렌식 전문가 15명을 대상으로 5차에 걸친 포커스 그룹 인터뷰를 통해 디지털증거분석실의 네트워크 구성, 분석관 컴퓨터의 사양, 개인에게 필요한 도구 및 장비, 이미징 장치, 전용 SW, 오픈소스 SW, 공용 도구·장비, 도구 및 액세사리, 기타 고려사항 등에 대해 심도 있는 분석을 진행하였다.

연구결과, 컴퓨터(HW, SW, 액세사리), 모바일(HW, SW, 악세사리), 특화 SW, 공용 도구 및 장비(현장 출동용 키트, 증거물 촬영, 공용 이미징 장치, 접수/전처리, 참여/참관, 보관, 전산/네트워크, 안전/보안, 사무시설/인프라, 기타)를 도출하였으며, 차세대 디지털증거분석 인프라 구성, 공간/도구·장비 목록 표준화, 민간 위탁 및 국가 지원 체계 수립에 대해 논의하였다. 디지털포렌식 도구·장비에 대한 연구는 여전히 많은 과제를 남기고 있다. 법정에서의 신뢰성을 인정받을 수 있는 기능에 대한 검증뿐만 아니라 운영환경인 디지털증거분석실에 대한 공인 인증, 도구·장비를 활용한 디지털포렌식 전문가의 숙련성 등 복합적인 요소들이 유기적으로 연계되어야 하기 때문이다.

본 연구는 디지털증거분석실을 구축함에 있어 일반적인 도구·장비의 범위를 벗어나 시설/환경 요소, 보안, 인프라 구조 등 다양한 관점에서 고려해야 할 요소들을 도출하였다는 점에 의미가 있다. 또한, 향후 차세대 디지털증거분석실 구축 방향에 대한 시사점을 살펴보았다는 점에서도 주목할만 하다. 하지만 본 연구 또한 한계점은 존재한다. 도구·장비 목록 도출 이외에 선택하는 기준과 이유 등에 대한 분석 및 예산안 산출 등을 진행하지 못했다는 점과 5인 이하 기준으로 인터뷰가 진행됨에 따라 중·대규모 디지털증거분석실 설계 시 반영해야 할 사항은 일부 고려되지 않은 점 등이 아쉬움으로 존재한다. 또한, 포커스그룹 인터뷰 방식의 편승효과, 후광효과 등의 일부 어려움이 존재한다. 추가적으로 도출된 도구·장비 목록이 적절한지에 대한 검증 부분은 향후 연구에서 실제 구축 및 도입 사례 분석 등을 통해 구체적으로 모색해 나가야 할 것이다.

참고문헌

[1] Korea Data Agency, 2020 Data Industry White Paper(23), pp. 8-30, 2020.12.

[2] National Police Agency, Digital Evidence Analysis Status(https://www.police.go.kr/user/bbs/BD_selectBbs.do?q_bbsCode=1025&q_bbscttSn=20210929074259890&q_tab=&q_code=&q_detailCode=&q_searchKeyTy=sj___1002&q_searchVal=%EB%94%94%EC%A7%80%ED%84%B8&q_rowPerPage=10&q_currPage=1&q_sortName=&q_sortOrder=&, Search date: 2022.03.14.)

[3] Byung-Min Park, Judicial Policy Research Institute, Research on Improving Search and Seizure of Digital Evidence_Focusing on Discussions of Legislative Measures, pp. 16-19, 2021.3.

[4] Yang-Sub Kwon, A Study on Korean Digital Forensic Investigation Procedure and Construction of Verification System, Journal of Digital Forensics 15(1), pp. 67-82, 2021.3,

[5] Jang Yoon-sik, National Police Agency, Digital Forensics Laboratory Standard Design Study, p.129, 2017.10

[6] Korea Maritime & Ocean University Industry-University Cooperation Foundation, A study on cybercrime countermeasures according to changes in the maritime environment based on ad

vanced technology, p.139, 2021

[7] Korea Laboratory Accreditation Scheme(KOLAS) - Authorized Agency Search - Search laboratory (https://www.knab.go.kr/usr/inf/srh/InfoTestInsttSearchList.do, Search date: 2022.3.14.)

[8] ANSI National Accreditation Board(ANAB) - Directory Of Accredited Organizations - Search - Korea Copyright Protection Agency Digital Forensic Center (https://search.anab.org/?__hstc=4076783.bbcd7009c961d220b5a5fbfb857fdf74.1645512838108.1645512838108.1647222145934.2&__hssc=4076783.3.1647222145934&__hsfp=1858334220, Search date: 2022.3.14.)

[9] Lawrence, Troy, Umit Karabiyik, and Narasimha Shashidhar. "Equipping a digital forensic lab on a budget." 2018 6th International Symposium on Digital Forensic and Security (ISDFS). IEEE, 2018.

[10] O'Connor, Rory V. "Software selection: towards an understanding of forensic software tool selection in industrial practice." International Journal of Technology, Policy and Management 5.4, pp. 311-329, 2005.

[11] Hibshi, Hanan, Timothy Vidas, and Lorrie Cranor. "Usability of forensics tools: a user study." 2011 Sixth International Conference on IT Security Incident Management and IT Forensics. IEEE, 2011.

[12] Nodeland, Brooke, and Scott Belshaw. "Establishing a criminal justice cyber lab to develop and enhance professional and educational opportunities." Security and Privacy 3.5, e123, 2020.

[13] Roman, Rodrigo Fernando Morocho, et al. "Digital forensics tools." International Journal of Applied Engineering Research 11.19, pp. 9754-9762, 2016.

[14] Ghazinour, Kambiz, et al. "A study on digital forensic tools." 2017 IEEE international conference on power, control, signals and instrumentation engineering (ICPCSI). IEEE, 2017.

[15] Padmanabhan, Radhika, et al. "Comparative analysis of commercial and open source mobile device forensic tools." 2016 Ninth International Conference on Contemporary Computing (IC3). IEEE, 2016.

[16] Jiyoon Ham, Joshua I.James, "A Feature Comparison of Modern Digital Forensic Imaging software", The Journal of The Institute of Internet, Broadcasting and Communication (IIBC) Vol. 19, No. 6, pp. 15-20, Dec. 31, 2019.

[17] Donghyun Kim, Jaehyeok Han, Sangjin Lee. A study on forensic analysis for Windows search utility Everything. Journal of Digital Forensics, 14(3), pp, 279-289, 2020

[18] Seung-Kyu Kim, Mu-Seok Kim, Gu-Min Kang. "A Study on the Development of Mobile Forensic Tool for the Response to Hidden Camera Crime." Journal of Digital Forensics, 14(3), pp. 290-304, 2020

[19] Kim, Min-Seo, and Sang-jin Lee. "Development of Windows forensic tool for verifying a set of data." Journal of the Korea Institute of Information Security & Cryptology 25.6, pp. 1421-1433, 2015

[20] Morgan, D. L., "The focus group guidebook: focus group kit 1". Thousand Oaks, CA: Sage, 1998.

[21] DAVID L. MORGAN(Transferred to the Korean Society of Qualitative Research Nursing), Focus groups as qualitative research, Gunja Publishing House, p.42, 2007.

[22] Supreme Prosecutor's Office Scientific Investigation Division, Law and Science: December issue, pp 50-56, 2021.12

〔저자소개〕

신 수 민 (Su-Min Shin)

2016년 2월 동국대학교 국제정보보호대학원 정보보호 석사
2021년 ~ 현재 : 성균관대학교 과학수사학과 박사과정
2017년 ~ 현재 : 한국국방연구원 정보기반팀 사이버보안 담당

관심분야 : 디지털포렌식, 정보보호, 디지털증거분석실, 디지털포렌식 도구/장비, ISO/IEC 17025, 17043, 27001
email : shin1121@g.skku.edu

박 현 민 (Hyeon-Min Park)

2016년 8월 : 백석대학교 정보보호학사
2018년 9월 ~ 현재 : 성균관대학교 과학수사학과 석박통합과정
2020년 1월 ~ 4월 : 대전선거관리위원회 디지털포렌식분석요원

관심분야 : 보이스피싱, 디지털포렌식, 안티포렌식, 가상자산포렌식
email : phm1189@naver.com

김 기 범 (Gi-Bum Kim)

2009년 2월 : 고려대학교 정보보호대학원 공학석사
2017년 2월 : 고려대학교 정보보호대학원 공학박사
2014년 ~ 2020년 : 경찰대학 경찰학과 교수요원
2020년 3월 ~ 현재 : 성균관대학교 과학수사학과 부교수

관심분야 : 디지털포렌식, 정보보호, 사이버범죄수사, 국제개발협력
email : freekgb02@gmail.com