디지털 포렌식 활용 및 대응

지도교수 : 이강호
연 구 자 : 윤창민

< 목 차 >

요 약

디지털 포렌식의 정의 및 종류 디지털 포렌식을 활용하여 사건 사고들을 해결한 사례들을 알아보았다. 디지털 포렌식이란 컴퓨터 범죄와 관련하여 디지털 장치에서 발견되는 자료를 복구하고 조사하는 법과학의 한 분야이다. 다양한 산업에서의 디지털 포렌식을 활용한 사례들을 알아보고 향후 디지털 포렌식 과제에 대해 국가적 차원의 대응 방향 및 국내 환경에 맞는 포렌식 대응 방안에 대해 알아보았다. 임베디드 포렌식 분야는 특정 디지털 장치에 대해 범죄 사건에 필요한 증거를 수집하여 분석할 수 있도록 소프트웨어나 하드웨어적인 방법을 이용하는 조사 방법이다. 최근의 임베디드 시스템의 다양성에 대응하여 학계에서도 활발한 연구를 통해 새로운 범죄 환경에 재빨리 대응해야 한다. 지금 현대사회에는 많은 디지털 기기가 쓰이고 있는 만큼 그만큼의 디지털 범죄가 일어날 가능성이 크다고 느낀다. 우리에게 친숙하고 이제는 없어서는 안 되는 디지털 기기, 그만큼 장점도 있고 단점도 있는 것 같다.

1. 서론

1.1 디지털 포렌식의 정의

디지털 포렌식 (Digital Forensic Science, 디지털 법과학)은 컴퓨터 범죄와 관련하여 디지털 장치에서 발견되는 자료를 복구하고 조사하는 법과학의 한 분야이다. 디지털 포렌식이라는 용어는 원래 컴퓨터 포렌식의 동의어로 사용되었지만 디지털 데이터를 기억할 수 있는 모든 장치에 대한 조사를 포함하여 확장되었다. 1970년대 후반과 1980년대 초의 가정용 컴퓨팅 혁명에 뿌리를 둔 이 분야는 1990년대에 우연히 진화했으며 21세기 초가 되어 국가 정책으로 관장되었다.

포렌식(Forensic)이라는 단어는 고대 로마 시대의 포럼(Forum)과 공공(public)이라는 라틴어에서 유래했으며 '법의학적인, 범죄 과학 수사의, 법정의, 재판에 관한'이라는 의미를 가지고 있는 형용사이다. 즉, 단순히 말해 포렌식이라는 단어는 범죄 수사와 관련한 모든 기술을 의미한다. 이러한 포렌식 분야 중 하나인 디지털 포렌식은 범죄 수사를 위해 디지털 장비의 분석 등을 하여 증거를 수집하는 행위 등을 통칭하는 용어이다.

디지털 증거물을 분석하여 수사에 활용하는 과학 수사 기법의 총칭. 마치 부검하듯이 디지털 기록 매체에 복원 프로그램을 사용하고 암호 등 보안을 해제하고, 메타데이터까지 활용하거나 하드디스크 내부에 삭제 로그를 저장하는 스왑 파일(스왑 폴더라고 하기도 한다)에서 삭제 로그를 복원해 디지털 기기의 사용자나 이를 통해 오간 정보를 추적, 조사한다. 원본의 손상을 봉쇄하기 위해 이미지를 뜨는 것이 일반적이라고 한다.

해킹(크래킹)과 디지털 포렌식은 언뜻 보면 비슷해 보이지만 다르다. 해킹은 불법적으로 접근 권한 등을 얻어 정보를 추출해 악이용하는 것이고 디지털 포렌식은 수사 영장이나 데이터 소유주의 동의를 받은 뒤 디지털 기기에 저장된 증거를 추출하거나 추출된 증거를 분석하는 작업이다. 암호를 해제하는 작업 등은 기술적으로는 크래킹과 다를 게 없지만 포렌식은 합법적으로 이루어진다. 자신의 개인 컴퓨터를 직접 크래킹하는 것이 불법이 아닌 것과 비슷하다. 다만 영장 등의 아무런 법적 근거 없이 디지털 포렌식을 하는 것은 불법 수사이다.

형사소송법 개정안으로 인하여 디지털 기기의 증거 능력이 확대되었다. 여담으로 이 개정안을 만든 사람은 촛불은 바람 불면 꺼진다는 말로 유명한 김진태 의원인데, 당시 자신의 트위터에 "이번 법 개정으로 앞으로의 간첩 수사에 도움이 될 것"이라며 자화자찬하기도 했는데 박근혜-최순실 게이트가 터지고 이때 최순실의 태블릿에 들어 있던 문서 파일들을 최순실이 부정할 때, 김진태가 개정한 법률 덕분에 증거로 인정받게 되면서 본의 아니게 수사에 큰 도움을 주게 되었다.

우리나라의 디지털 포렌식은 90년대 경찰의 해킹 수사대가 수사에 활용하며 시초가 되었으며, 현재 경찰청 디지털 포렌식 센터가 전국적으로 최대의 규모를 가지고 있다. 그 외에도 검찰, 국정원, 군 등이 각 발전을 위해 노력 중이다.

주요어: 법과학, 디지털 증거, 해킹

2. 본론

2.1 디지털 포렌식의 종류 및 사건 사례

디지털 포렌식의 종류는 다음과 같이 있다.

1) 컴퓨터 법과학: USB 드라이브, SD 드라이브 등등 복원

2) 모바일 장치 법과학: 내장된 GPS / 위치 추적 또는 셀 사이트 로그 범위 추적, 내장된 통신시스템(예:GSM)

3) 네트워크 법과학: 정보 수집 및 로컬 및 WAN/인터넷의 네트워크 트래픽을 모니터링하고 분석 패킷 레벨 분석법

4) 데이터 분석 법과학: 금융 범죄로 인한 사기 행위 패턴을 발견 분석 구조화된 데이터 조사

5) 데이터베이스 법과학: 데이터베이스와 관련된 포렌식 / 인로그, 데이터베이스 내용, RAM의 타임라인 구축 및 복구

2.2 사례

디지털 포렌식을 이용하여 사건을 해결한 사례들을 알아보자.

2.2.1 원세훈 자택 화염병 투척 사건

원세훈 전 국정원장 자택에 누군가가 화염병을 투척한 사건이 일어났다. 이후 경찰은 CCTV 자료를 분석하여 사건 발생 2주 만에 모 대기업의 과장으로 근무 중이던 임모 씨를 긴급체포하게 되었다. 하지만 일이 순탄하게만 해결되지는 않았다. 낮은 화질로 인해 용의자의 얼굴 식별이 확실하지 않아 여러 장소에서 촬영된 CCTV가 모두 한 사람임을 밝히기 위해 경찰은 '걸음걸이 기법'을 제시한다. 최신 기술의 투입으로 순탄할 줄만 알았던 사건. 하지만 검·경은 수집 과정에서 가장 중요한 것을 지키지 못해 결국 증거 채택에 실패, 무죄로 결론이 나게 되었다. 그럼 여기서 검찰과 경찰이 놓쳤던 가장 중요한 점은 과연 무엇이었을까? 이 전까지 경찰에 CCTV 영상의 자료를 수집하는 과정은 단순히 영상자료를 탐색한 뒤 이를 복사하여 가져가는 방식으로 진행되었었다. 하지만 중요한 증거자료가 쉽게 복사가 되고 수정을 하게 되면 최종 자료의 원본성이 지켜지기가 힘들었다. 그 점을 막기 위해서는 저장장치 봉인은 필수이다. 결국 경찰이 수집한 자료는 수집할 때도 해당 디스크를 이미징하여 원본성을 지키지 않았고, 증거로 제출할 때도 다수의 복제 과정과 미봉인 등의 실수를 하게 된다. 디지털 포렌식을 통해 얻은 자료가 법정에서 증거능력을 얻을 수 있게 하기 위해서는 가장 중요한 3대 요건인 원본성과 재현성, 신뢰성을 반드시 지켜야 한다.

결국 수차례의 복사와 관리 소홀로 인하여 증거에 대한 원본성을 보존하지 못한 결과, 가장 중요한 증거자료로 판단되었던 CCTV 영상은 증거능력을 잃게 되었다. 긴 재판 끝에 임모 씨는 무죄판결을 받게 되면서 사건은 종결이 되었다. 모든 알리바이와 최첨단 기술을 동원했음에도 증거관리의 소홀이 결국 무죄를 만들어 버린 것이다. 임 씨의 무죄판결 이후 원세훈 자택 화염병 투척 사건은 '원세훈의 자작극'과 '말도 안되는 법집행' 이라는 의견으로 나뉘어 갑론을박이 진행되고 있다. 어찌 되었건 원세훈 자택 화염병 투척 사건의 진행 과정 덕에 디지털 포렌식에서 증거관리(원본성)의 중요성을 다시 한번 깨닫게 한 좋은 교훈이 되었던 것 같다.

2.2.2 디지털 포렌식의 3대 요건

1) 원본성

디지털증거를 수집, 분석, 제출하는 과정에서 수정이나 변조 없이 원본과 동일하다는 사실을 증거수집 당시의 해시값[1]으로 입증하는 것을 말한다.

2) 재현성

누구든지 동일한 분석 도구를 이용해 동일한 분석 순서와 분석 방법으로 검증하였다면 항상 동일한 분석 결과가 산출되어야 함을 뜻한다.

3) 신뢰성

대검찰청이나 경찰청, 국정원 등에서 사용하는 공인된 분석프로그램을 이용해 만들어진 디지털 포렌식 결과 보고서를 하는 것을 말한다.

2.2.3 숙명여자고등학교 쌍둥이 시험지 유출 사건

숙명여고에 다니는 쌍둥이는 1학년 때 중위권의 성적이었지만, 2학년 때 나란히 전교 1등으로 급상승을 하며 '교무부장인 아버지가 일으킨 기적'이라며 인터넷 커뮤니티를 통해 빠르게 확산되어 서울시교육청에서 특별감사에 나섰다.

심증은 가지만 물증이 없어 경찰에 수사를 요청한 결과 시험 정답을 미리 적은 것으로 보이는 메모지와 함께 시험지를 받자마자 외우고 있던 답안을 바로 메모해놓은 듯한 흔적이 발견되었다. 많은 정황을 담은 증거들이 발견되었음에도 불구하고, 피의자 측에서는 '커닝 목적이 아닌, 시험 종료 후 채점을 위해 따로 적어놓은 것이다'라며 부정적인 의견을 내비쳤다. 사실상 작성 시점이 확인되지 않았다는 점이 문제였다. 하지만 동생의 휴대폰을 디지털 포렌식한 결과, 시험 전에 촬영된 것으로 확인된 영어 과목 서술형 답안이 공개되어 시험지를 유출하는 모습이 찍힌 것이 아니더라도 확실하게 혐의를 입증할 수 있게 되었다.

디지털 포렌식 덕분에 물증을 두고도 발뺌하는 숙명여고 쌍둥이에게 더욱 확실한 물증을 제시해 빼도 박도 할 수 없는 확실한 전세를 굳혔다고 봐도 무방하다. 사소한 사건부터 대한민국을 뒤흔든 중요한 사건들까지 키 역할을 했던 디지털 포렌식, 이제 민간에서도 전문적인 디지털 포렌식의 분석이 확산되고 있다. 디지털 포렌식을 통해 많은 걸 바꿔 가는 추세인 것이다.

주요어: 원본성, 재현성, 신뢰성

3. 다양한 산업에서의 디지털 포렌식 활용

다양한 산업영역에서 디지털 포렌식 기술을 실제 활용하고 있거나 새롭게 요청하고 있다. 디지털 포렌식을 이용한 산업에는 다음과 같은 것이 있다.

1) 문화 컨텐츠 산업: 멀티미디어 포렌식, 포렌식 워터마킹, IPTV 포렌식
2) 소프트웨어 산업: 소프트웨어 포렌식
3) 자동차 산업: 블랙박스 포렌식
4) 금융산업: 금융사고 분쟁 해결
5) 의료산업: 의료사고 분쟁 해결

---

1) 해시값: 복사된 디지털 증거의 동일성을 입증하기 위한 암호 같은 수치인 디지털증거의 지문

6) 회계법인: 포렌식 어카운팅
7) 법무법인: E-Discovery 등 민사소송 대응
8) ISP업체: 기술적 보호조치로서의 디지털 포렌식
9) 보험회사: 보험사고 발생 시 증거수집

3.1 활용사례 - 산업기밀 유출 탐지

3.1.1 데이터 유출 방법의 변화

-데이터 형태의 변화
-데이터 크기 증가
-정보통신 기술의 발전

3.1.2 디지털 데이터 유출의 유형 분류

[사진 1] 디지털 데이터 유출의 유형

3.1.3 데이터 유출 흔적 분석

-데이터 유출의 유형 별로 다양한 흔적을 확인 가능하다.
(물리 메모리, 파일 시스템, 레지스트리, 기타 로그 파일들에 대한 포렌식 분석을 통해 데이터 유출의 흔적 파악 가능)

3.2 활용사례 - 문서 위조 판별

3.2.1 기존의 문서 위조 판별 방법

문서의 글씨, 도장의 진위 판별에 초점을 맞춘다.
최근 다양한 형식의 디지털 문서 파일이 생성되고 있다.(새로운 문서 위조 판별 방법 필요)

3.2.2 디지털 문서 위조 판별 방법

문서 파일 내부의 시간 정보(파일 내부의 저장 형식을 정확히 알지 못하면, 조작하기 어려움)

이전 작업 내역

+ 이전에 수정 또는 삭제된 데이터 확인 가능(Office, PDF 등)
+ 문서 작성 순서 파악(PowerPoint 슬라이드 생성 순서 등)
+ 해당 응용프로그램으로 확인할 수 없으며, 내부 저장 형식에 대한 이해 필요

3.3 활용사례 - 영상 분석

3.3.1 적용 기술

양복 위치에서의 '영상 대조'를 변화시킴

윤곽선이 뚜렷이 나타나도록 영상 처리

3.4 활용사례 - e-Discovery

3.4.1 미국 민사소송의 전자증거 개시 제도

Zubulake v. UBS Wrburg LLC(2005)

• 성차별 관련 소송에서 원고 Zubulake는 피고 USB Warburg사가 관련 증거를 제출하지 못했다며 소송제기

• 피고 측 변호사는 구두로 직원들에게 소송 관련 자료들에 대한 Litigation Hold를 명령했지만, 직원들에 의해 백업테이프 상의 전자메일들이 삭제

• 법원은 전적으로 변호사의 책임은 아니지만, 피고 측 변호사가 직원들에게 어떻게 증거를 보호할지에 대해 적절히 설명하지 못해 삭제된 전자메일들이 포함되었던 백업테이프를 보호하지 못하였으므로 결과적으로 Litigation Hold 명령에 실패했다고 판결

• UBS사에게 소송비용을 포함하여 상대편 변호사 비용 및 Deposition 비용을 부담할 것을 판결

• 변호사들에게 합리적 수준의 조치를 위할 것을 요구하는 e-Discovery 책임에 관한 가이드라인을 제시

Coleman Holdings, INC.V.Morgan Stanley(2005)

• 원고 Coleman Holdings는 Morgan Stanley가 자사와 SunBeam사의 합병과 관련된 이메일을 제출하지 못했다며 소송 제기

• 원고 측은 해당 이메일이 Morgan Stanley사가 Sunbeam사의 회계부정사실을 알고 있음을 증명하고 있는 증거라고 주장

• 피고 측은 비록 문서보존명령을 내리긴 했지만, SEC 규정의 2년간 보존 의무를 어기고 12개월 만에 이메일 삭제

• 법원은 피고가 증거를 고의로 훼손했다고 판단하여 Morgan Stanley사에 15억 달러 배상 판결

Samsung Electronics Co., Ltd. v. Rambus (2006)

• 2006년 2월 샌프란시스코 연방법원은 Rambus가 제기한 삼성전자의 가격 담합 의혹을 인정, 삼성전자에게 관련 서류들을 모두 만들어 제출하라는 명령을 내림

• Rambus는 재판 과정에서 삼성전자가 일부 중요한 문건에 대한 고의적 혹은 불성실한 행위가 있었다며, 이는 FRCP(Federal Rules of Civil Procedure)를 위반한 것이라고 주장

• 법원은 삼성이 직원들에게 보존할 것들과 관련 문서들을 파괴시키지 말 것에 대한 조치를 충분히 행하지 않았다고 판단하여 삼성 패소

• 삼성전자는 Rambus와의 소송 끝에 5년간 7억 달러의 액수의 로열티를 지급하는 것으로 판결

Qualcomm, Inc. v. Broadcom, Inc. (2008)

• 2005년 시작된 Broadcom사와의 특허소송의 e-Discovery 과정에서 200,000페이지에 달하는 관련 전자메일과 전자문서 제출에 실패

• Qualcomm사 변호사들이 소송 증거 보존 실패의 책임 및 소송증거 은닉 행위에 참여했다는 명확한 증거가 밝혀짐

• Qualcomm사 소송 패소 상대편 변호사 비용 850만 불 지불 판결

• Qualcomm사 변호사들 또한 변호사 윤리규정 위반으로 징계

Phillip M. Adams & Assoc. LLC v. Dell, Inc. (2009)

• Adams는 자사가 보유한 플로피 디스크 결함 발견 기술을 Asus가 도용했으며, Asus가 핵심정보를 훼손했다고 주장

• Asus는 해당 이메일 자료 제출 실패에 대해 당시 이메일 시스템은 아카이빙 기능이 없었으며, 장기적 보존이 요구되는 가치는 개인 임직원들이 판단, 개인 PC에 저장했다고 반론

• 법정은 Asus가 증거 보존 의무를 다하지 못한 것에 대해 이메일 증거 훼손혐의 인정

3.5 활용사례 - 지적재산권[저작권]분쟁

3.5.1 디지털 저작권 포렌식 수사

저작권 위반 혐의에 대한 관련 증거 수집 및 조사, 분석 지원

• 저작권 위반 혐의를 증명할 수 있는 디지털 증거에 대해 디지털 포렌식의 증거 수집 및 분석 방법을 이용하여 증거 분석 결과물에 대한 신뢰성 확보 문화체육관광부, 웹하드, 클럽운영자, 헤비업로더 수사 전개

• 온라인상 저작권 침해 사범 강력 단속 위해 2010년 디지털 저작권 포렌식 시스템 구축

• 포렌식 시스템은 네트워크 등의 디지털 소스로부터 정보를 수집·분석·보존하여 법적 증거물로 활용

• 2010년 7월부터 12월까지 저작권특별사법경찰이 기획 수사를 전개, 저작권 보호 대상인 영화 파일 등 디지털 콘텐츠를 불법으로 복제하여 대량으로 웹하드 사이트에 유통시킨 헤비업로더 48명과 이들의 불법복제물 올리기를 조장한 웹하드 업체 대표 4명을 저작권법 위반 혐의로 검찰에 송치

• 이 사건으로 39억 7천만 원의 범죄수익금 산출

3.5.2 소프트웨어 포렌식

소프트웨어 지적재산권 분쟁의 해결을 위한 기술로 활용

• 소프트웨어 지적재산권의 침해 여부 및 정도를 판단하기 위해 사용

• 소프트웨어 관련 증거자료의 분석을 통해 프로 소스코드와 실행코드의 복제 여부 및 복제율 산정

• 프로그램 원시코드의 작성자 확인

• 소프트웨어 소스코드 및 복제코드의 확인

• 소프트웨어 저작자 및 저작물의 식별

• 코드블럭의 위치변경, 변수 및 함수 이름의 변경과 같은 소스코드의 조작 등에 원본과 동일 또는 유사한 소스코드를 탐지

3.5.3 프로그램 복제(유사)도 감정 사례

동영상 학습 프로그램 저작권 침해 사건(2008)

• 피고소인이 고소인의 회사를 퇴사한 이후, 동종의 사업체를 설립하고 사업을 영위

• 고소인은 피고소인이 등록, 사용하고 있는 동영상 교육프로그램이 자신의 회사에서 개발한 프로그램을 무단으로 절취하여 사용한 것이라고 주장하여 위원회에 감정을 의뢰

• 고소인 프로그램 중 피고인 등록 프로그램과 중복되는 부분의 정도를 소스코드 및 사용자 인터페이스의 유사도로 확인

• 소스코드 유사도는 원본 기준 96.9%, 인터페이스 유사도는 원본 기준 79.5%로 법원은 고소인의 승낙 없이 프로그램의 상당 부분을 복제하거나 개작한 것으로 보고 저작권 침해에 있어서 고의를 인정하여 유죄로 판단

3.5.4 콘텐츠 보안 프로그램(2006)

• 피고소인은 고소인 회사의 이사 겸 프로그램 개발자로 근무 중 회사 내부의 경영권 분쟁으로 인하여 퇴사한 후 피고소인 회사를 설립

• 고소인 측 콘텐츠 보안 프로그램 M1과 유사한 프로그램인 M2를 피고소인 회사가 개발·판매함에 따라, 고소인 회사는 영업 이익 침해를 이유로 피고소인을 컴퓨터 프로그램보호법 위반 주장

• 감정 결과, 전체적인 프로그램 구현방식에 있어서 원고의 M1 프로그램은 일반 응용프로그램 방식을 사용하고 있는 반면, 피고의 M2 프로그램은 컴포넌트 기반 방식을 사용하며 각 구성부분별 기본기능은 유사하나 이는 디지털 콘텐츠 보안 프로그램의 특성이며 기능별 구현방식이 다르므로 전체 유사도는 11.5%로 판결

• 원·피고의 각 프로그램 사이에 실질적 유사성은 없음으로 판결

3.5.5 웹 애플리케이션 개발 솔루션(2007)

• 피고 회사의 K는 원고 회사의 개발자로 근무하던 중 원고 회사를 퇴사하여 피고 회사로 이직 후, 피고 회사가 원고의 프로그램인 A와 동종의 프로그램인 B 등을 개발하여 영업. 이에 원고는 피고를 상대로 법원에 컴퓨터프로그램저작권침해 정지의 소를 제기

• 감정 결과 A와 B 그리고 B'의 전체소스 유사도는 각각 5.65%와 0.38%로 나타났으며, 6개 컴포넌트 간의 유사도는 B와 B'에서 각각 1.37%와 0.25%인 것으로 나타남

• 법원은 원·피고 각 프로그램 사이의 실질적 유사성이 있다고 볼 수 없기 때문에 원고의 청구 기각

3.6 활용사례 - 자동차 블랙박스

3.6.1 자동차 블랙박스 포렌식 기술

사고 발생 전(Pre-Crash)

-자동차 주행 데이터, 시스템 상태 정보, 속도, 엔진 회전수, 브레이크 상태, 안전벨트 여부

사고 순간(During a Crash)

-속도, 탑승자 안전장치(SRS) 데이터, 운전자 에어 입력값

사고 발생 후(Post-Crash)

-자동 충돌 경보

3.6.2 실시간 블랙박스 무결성 보장 기술

• 블랙박스에 저장되는 데이터는 악의적인 목적에 의해 데이터가 위/변조될 수 있다.

-사고의 가해자와 피해자가 뒤바뀔 수 있다.

• 블랙박스에 저장된 데이터가 원본인지 아닌지 구분하기 위한 방법 무결성 보장 기술 개발이 필요하다.

• 고속으로 생성되는 데이터의 무결성을 실시간으로 보장하는 기술 개발이 필요하다.

4. 향후 디지털 포렌식 과제와 전망

1) 디지털 포렌식 활용에 대한 법적/기술적 도전

사이버 망명: 정치적인 사유나 불법적인 목적으로 자국 내 서버에서의 자유로운 인터넷 이용에 제한을 받는 사용자가 이메일, 블로그 등 인터넷 서비스의 주 사용 무대를 국내법의 효력이 미치지 못하는 해외 서버로 옮기는 행위

데이터 피난처: 위키리크스가 접속차단을 피해 스위스로 서버를 이전한 것처럼 특정 국가에서 금지된 데이터 제공 서비스를 지속하기 위해 법적 규제를 피해 데이터 서버를 해당 규제로부터 안전한 곳으로 이전하는 행위

2) 아이폰 앱스토어

아이폰 앱스토어 서버는 미국에 위치하여 본사에서 직접 관리하고 있으며, 국내의 경우 앱스토어 관련 부서도 없는 상황이다.

저작권 침해나 모바일 악성코드 관련 문제가 발생하더라도 법적 대응이 어렵고 신속한 침해 대응과 복구가 어려우며, 관련 증거 확보 시에도 어려움이 예상된다.

3) 클라우드 컴퓨팅

장소 독립적인 특성을 갖는 클라우드 서비스는 데이터의 저장 위치를 특정하기 어렵고, 해외에 산재되어 있을 가능성도 존재하므로, 디지털 수사나 이디스커버리 업무 수행 시 법적 문제 등 어려움을 겪을 수 있다.

4) 블랙베리 스마트폰

스마트폰 블랙베리의 End-to-End 보안 기능은 블랙베리에서 전송되는 메시지가 이통사 서버를 거치지 않고 캐나다 RIM사의 자체 서버를 통해 암호화된 후 전송되므로 디지털 수사 및 감청 수행 시 어려움이 예상된다.

실제 아랍에미리트와 사우디아라비아 정부는 국가 보안상 이유로 블랙베리 스마트폰을 퇴출 시켰다.

4.1 국가적 차원의 대응 방향

1) 디지털 포렌식 법률 및 제도 정비
2) 디지털 포렌식 표준 개발 및 매뉴얼 배포
3) 디지털 포렌식 인력 양성 사업 지원
4) 디지털 포렌식 기술 연구개발 지원 및 디지털 포렌식 지식 공유
5) 국가 간 디지털 증거 및 디지털 수사 관련 협력 강화

주요어: 디지털 포렌식, 데이터, 정보자산

4.2 국내 환경에 맞는 포렌식 대응 방안

4.2.1 임베디드 포렌식

임베디드 포렌식 분야는 특정 디지털 장치에 대해 범죄 사건에 필요한 증거를 수집하여 분석할 수 있도록 소프트웨어나 하드웨어적인 방법을 이용하는 조사 방법이다. 최근의 임베디드 시스템의 다양성에 대응하여 학계에서도 활발한 연구를 통해 새로운 범죄 환경에 재빨리 대응해야 한다.

이처럼 다양한 임베디드 시스템의 등장은 디지털 포렌식 관점에서 중요한 시사점을 지닌다. 개괄적인 임베디드 포렌식 분야는 크게 임베디드 시스템에 대한 데이터 수집 및 증거 획득 방안 안티 포렌식 관점에서 발생할 수 있는 데이터 은닉에 대한 분석 복구 방안 등으로 크게 나눌 수 있다. 안티 포렌식 관점에서의 임베디드 포렌식은 포함된 플래쉬 메모리나 하드디스크와 같은 저장장치에 대해 기존 파일시스템이나 운영체제가 사용하는 파티션 외에 사용자가 추가로 파티션을 생성한 다음 여기에 데이터를 은닉하는 방법이 있다. 일반적인 증거 수집 관점에서는 임베디드 시스템의 사용 기록이나 시간 정보를 활용한 타임라인 분석 등에 이용하여 정황 증거를 파악할 수 있는 실마리를 제공할 수 있다. 마지막으로 일반적인 개인 컴퓨터나 데스크 탑과 동일한 기능을 가진 임베디드 시스템은 리눅스 운영체제를 설치하여 해킹 시스템으로 변경하여 이용될 수 있으므로 이에 대한 포렌식 분석 및 증거 획득 기술이 필요하다.

본 절에서는 기존의 보편화된 모바일 기기 이외에 최근 새롭게 등장한 임베디드 시스템에 대한 디지털 포렌식 연구 동향과 보안 이슈를 다룬다. 앞서 간략히 설명한 임베디드 시스템에 대해 시스템의 종류별로 분류하고 포렌식 관점에서 분석 방안이나 이슈에 대해 설명한다.

4.2.2 비디오 콘솔 게임기

최근에 등장한 가정용 비디오 게임기는 마이크로소프트가 출시된 이후로 그 성능과 XBOX 기능이 일반 개인용과 동일하다. 즉 방식의 하드디스크를 저장 장치로 지니며

인터넷을 PC, IDE 통한 네트워크 통신이 가능하도록 이더넷 카드를 포함하고 있다.

이러한 하드웨어 환경은 게임을 실행하기 위해 설치된 운영체제 외에 리눅스를 설치할 수 있어 리눅스 기반의 개인 컴퓨터에서부터 서버나 기타 다양한 서비스를 제공하는 임베디드 시스템 FTP으로서 사용될 수 있다. 따라서 학계에서도 이러한 가정용 비디오 게임기에 대한 범죄 수사의 중요성을 인식하고 대상에 대한 증거 수집 및 분석 방안에 대한 연구를 진행하고 있다. 또한 최근 출시된 이나 소니사의 플레이스테이션은 일반적인 개인 컴퓨터보다 뛰어난 성능을 가져 리눅스 환경에서 암호 검색 전용시스템으로도 개발되는 등 다양한 목적에 이용되고 있다.

주요어: 임베디드

5. 결론

지금 현대사회에는 많은 디지털기기가 쓰이고 있는 만큼 그만큼의 디지털 범죄가 일어날 가능성이 크다고 느낀다. 우리에게 친숙하고 이제는 없어서는 안되는 디지털기기, 그만큼의 장점도 있고 단점도 있는 것 같다. 이 디지털 포렌식에 관련한 자료를 찾으면서 우리에게 익숙한 것에서의 위험성을 절실히 느꼈다.

참고문헌

https://ko.wikipedia.org/
https://namu.wiki/
https://post.naver.com/viewer/postView.nhn?volumeNo=17326752&memberNo=37693066
https://post.naver.com/viewer/postView.nhn?volumeNo=17098885&memberNo=37693066
http://www.cisokorea.org/data_file/board/Digital
http://jcher.iptime.org/