디지털 포렌식

32기 조현서

서론

디지털 포렌식은 예전부터 관심을 크게 가졌던 분야라서, 나중에 기회가 된다면, 심도있게 공부해보고 싶다고 항상 생각해왔는데, 이번 새로운 SSR에서 이를 주제로 잡아 깊이 다뤄보고 싶어서 주제로 선정하게 되었다. 사이버 범죄와 해킹 사건이 점점 빈번해지고, 정교해지고 있는 상황 속에서, 디지털 포렌식의 중요성이 점점 각광받고 있다. 수많은 뉴스, 드라마, 영화와 같은 매체 속에서도 많이 등장하는 만큼, 누구나 한 번쯤은 들어봤을 만한 널리 알려진 기법이다. 그러나 단순히 유명한 기술이라는 이유만으로 관심을 가지게 된 것은 아니다.

작년에 여러 공부를 하면서, 느낀 점은 실제 사이버 범죄 수사와 보안 사고 대응에 있어서, 단순히 공격 행위 자체를 막는 것만으로는 충분하지 않다는 것을 느꼈다. 공격자의 흔적을 추적하고, 침해 경로를 분석하며 피해 규모를 파악하는 등의 과정을 통해, 유사한 공격의 재발을 방지할 수 있으며, 법적 대응을 위한 증거로 활용하는 과정이 필수적이라는 것을 깨달았다. 디지털 포렌식은 사이버 범죄뿐만 아니라 기업 정보 유출 사건, 데이터 복구 등 다양한 분야에서도 중요한 역할을 한다. 기업 보안팀에서는 침해 사고가 발생했을 때, 포렌식 기법을 활용해 내부 데이터를 분석하고, 금융권에서는 불법 거래나 신용카드 정보 유출을 추적하는 데 포렌식 기법이 활용된다고 한다. 이처럼 다양한 활용 가능성과 실무적 중요성을 고려했을 때, 단순히 개념적으로 이해하는 것을 넘어, 실제로 디지털 포렌식이 어떻게 활용되는지 심층적으로 살펴보고 싶다. 포렌식 도구 활용, 로그 분석, 파일 복구 기법 등을 집중적으로 살펴보고, 실제 사건 사례를 분석하면서 깊이 탐구해보고자 한다.

본론

1〉 디지털 포렌식의 개념과 주요 기법

1. 디지털 포렌식의 정의와 원칙

우리 주위에는 많은 디지털 제품을 볼 수 있는데, 이러한 모든 디지털 기기에서 이뤄지는 전원 작동, 수정, 삭제 등 모든 행위는 디지털 흔적이 남는다. 디지털 포렌식은 사이버 범죄, 해킹 사고, 데이터 유출 등의 사건이 발생했을 때, 이러한 디지털 증거를 수집, 분석, 보존하여 법적 증거로 활용할 수 있도록 하는 과정을 의미한다.

하지만 디지털 증거는 위/변조가 쉽기 때문에, 법적 증거 자료로 채택되기 어려움이 있다. 따라서, 디지털 증거가 법적 증거로 인정받기 위해서는 기본 5대 원칙을 지켜야 한다고 한다. 첫 번째는 “정당성의 원칙”이다. 획득한 증거자료가 적법한 절차를 준수해야 하고, 위법한 방법으로 수집된 증거는 법적 효력을 상실한다는 원칙이다. 이는 형사소송법[제308조의 2(위법수집증거의 배제)]에 언급되어 있고, 위법한 방법으로 수집된 증거에 의하여 발견된 증거 또한 증거능력이 인정될 수 없다고 한다. 두 번째, “무결성의 원칙”이다. 이는 수집한 증거가 의/변조되지 않았음을 증명할 수 있어야 한다. 일반적으로 수집 당시의 데이터에 대한 해시값과 법정 제출 시점에서의 데이터 해시값이 같다면 해시함수의 특성에 따라 무결성이 입증된다고 한다. 세 번째, “재현의 원칙”이다. 이는 누구든지 동일한 분석 도구를 이용하여 동일한 분석 순서와 분석 방법 등으로 검증하였을 경우, 항상 동일한 분석 결과가 산출되어야 한다는 원칙이다. 법정에서 증거를 제출하려면 피해 직전과 같은 조건에서 현장 검증을 실시하거나, 재판이나 법정의 검증 과정에서도 동일한 결과가 나와야 한다고 한다. 네 번째, “신속성의 원칙”이다. 이는 모든 과정은 지체없이 신속하게 진행되어야 한다는 원칙이다. 특히, 휘발성 증거의 수집 여부는 신속한 조치에 의해 결정되므로 모든 과정은 지체 없이 진행되어야 한다고 한다. 추가적으로 설명을 덧붙이자면, 주요 휘발성 데이터는 레지스터 및 캐시 정보, ARP 캐시, 메모리, 임시 파일 시스템, 디스크, 원격 로그 및 모니터링 데이터, 네트워크 토폴로지 등이 있다고 한다. 다섯 번째, “연계 보관성의 원칙”이다. 증거물 획득 → 이송 → 분석 → 보관 → 보관 → 법정 제출의 각 단계에서 담당자 및 책임자를 명확히 해야 하는 등 일련의 과정이 명확해야 하며 추적이 가능해야 한다는 원칙이다. 이를 ‘절차 연속성’ 혹은 ‘연계 보관성(Chain of Custody)’이라고 한다.

2. 주요 분석 기법

디지털 포렌식에서는 다양한 분석 기법이 사용되는데, 주로 많이 사용되는 기법 위주로 조사해보았다.

첫 번째, "디스크 포렌식"이다. 이는 물리적인 저장장치인 하드 디스크, 플로피 디스크, CD-ROM 등 각종 보조 장치의 데이터를 복구하고 분석하는 기법이다. 주로 파일 시스템 분석을 통해 공격자가 어떤 데이터를 변경하거나 삭제했는지 추적한다고 한다. 대표적인 기술은 '데이터 카빙', '파일 복구', '타임라인 분석'이 있다. 추가적으로 '데이터 카빙(Data Carving)'이란 파일 시스템의 정보 없이 비 할당 영역에서 파일을 추출하는 기법이다. 이는 파일의 시그니처, 조각난 수에 따라 단편화된 부분을 복구할 수 있다고 한다.

두 번째, "메모리 포렌식"이다. 이는 컴퓨터 하드웨어 중 주 기억장치(RAM)에 남아있는 데이터 흔적을 분석하는 기법이다. RAM은 휘발성이 강하지만 프로세스 정보, 네트워크 연결 정보, 악성코드 파일 정보, 시스템 관련 데이터 구조, 사용자 활동 정보 등의 고유의 독특한 정보가 남아있다. 따라서 메모리 포렌식의 주 목적은 악성코드와 관련있는 데이터를 추출하고, 어떻게, 어떤 이벤트가 발생했는지 등의 RAM 에 남아있는 악성코드 감염과 관련된 다양한 흔적을 분석하여 침해 사고 대응과 분석 과정에서 이용하는 것이라고 한다. 주로 휘발성 데이터를 다루기 때문에 사고 발생 후, 신속한 메모리 덤프가 필수적일 것으로 보인다. 대표적인 기술에는 'Volatility 프레임워크 활용', '프로세스 및 네트워크 연결 분석'이 있다고 한다.

세 번째, "네트워크 포렌식"이다. 이는 네트워크 트래픽을 모니터링 및 분석하여 비정상적인 통신이나 해킹 시도를 탐지하는 기법이다. 주로 DNS 터널링, C2 서버 통신, 피싱 공격 등의 증거를 포착해낸다. 대표적인 기술은 '패킷 캡쳐', '로그 분석', 'DPI(Deep Packet Inspection)'이 있다. 내가 이때까지 많이 활용해본 버프 스위트나 와이어샤크를 이용해 네트워크 통신 분석한 것도 네트워크 포렌식의 일부로 볼 수 있다는 것을 알 수 있었다.

네 번째, "이메일 포렌식"이다. 이는 피싱 공격, 내부 정보 유출, 스팸 메일을 분석하여 악성 링크 및 첨부파일을 추적하는 기법이다. 메일 헤더 분석을 통해, 발신자의 IP 주소 및 메일 경로를 추적한다고 한다. 대표적인 기술은 'SPF, DKIM, DMARC 분석', '이메일 헤더 분석'이 있다. '메일 서버 등록제(SPC)'은 도메인에서 이메일을 보낼 수 있는 메일 서버를 지정한다고 한다. 이를 통해, 수신 메일 서버는 내 도메인에서 전송된 것처럼 보이는 수신 메일이 내가 승인한 서버에서 전송된 것인지 확인할 수 있다고 한다. '도메인 키 식별 메일(DKIM)'은 발신자가 암호화 키를 사용하여 이메일 메시지에 서명할 수 있도록 해주는 표준이라고 한다. 이메일 공급자가 이러한 서명을 사용하여, 메시지가 전송 중에 타인에 의해 수정되지 않았는지 확인한다고 한다.

다섯 번째, “모바일 포렌식”이다. 이는 스마트폰, 태블릿에서 디지털 증거를 수집하고 분석하는 기법을 말한다. 삭제된 메시지, 앱 사용 기록, GPS 데이터 등을 복원하여 사용자 활동을 추적한다. 대표적인 기술을 ‘JTAG 분석’, ‘Chip off 분석’, ‘루팅/탈옥 환경 분석’이 있다. ‘JTAG’ 이란 디지털 회로에서 특정 노드의 디지털 입출력을 위해 직렬 통신 방식으로 출력 데이터를 전송하거나 입력 데이터를 수신하는 방식을 말한다고 한다. 이를 통해, 암호화된 데이터도 덤프 후 복호화 시도가 가능해진다고 한다. 또한, 루팅이 불가능한 최신 기기나, 법적 절차를 따라야 하는 수사기관에서는 이를 많이 활용한다고 한다. ‘칩오프(Chip Off)’란 디지털 기기의 NAND 플래시 메모리를 물리적으로 분리하여 데이터를 추출하는 포렌식 기법을 말한다. 이는 기기가 물리적으로 손상되었을 때 뿐만 아니라 OS가 삭제한 데이터까지도 복구가 가능하게끔 한다고 한다.

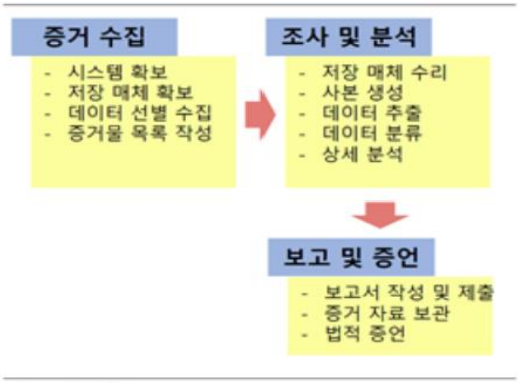
여섯 번째, “클라우드 포렌식”이다. 클라우드 환경에서 저장된 데이터와 로그를 분석하여 침해 흔적을 확인한다. 일반적 포렌식은 분석 환경이 동결되어 있는 것과는 다르게, 클라우드 포렌식은 고정되지 않은 플랫폼을 분석하고, 분석해야 할 하드웨어를 다른 프로세스와 사용자가 공유해서 사용한다. 또한, 수색 영장으로 서버를 압수해도 다른 사람의 데이터도 저장되어 있기 때문에 이 데이터가 외부로 유출되면 포렌식 실무자가 법적 책임까지 져야할 수도 있다고 한다. 그 외에도, 서버가 물리적으로 존재하는 위치도 문제가 될 수 있다. 따라서, 해당 국가의 사법부와 공조가 필요하다는 어려움이 있다. 이를 악용하기 위해, 수색을 법적으로 허가하지 않는 국가의 클라우드 서버에 데이터를 숨기는 경우도 많다고 한다. 주로, 로그인 정보 확인, 사용자 데이터 수집/분석, 사용여부 분석의 조사 활동을 한다고 한다.

3. 대표적인 포렌식 도구

수많은 포렌식 도구들이 많지만, 실제로 실무에서 많이 활용되는 도구들 위주로 조사해보았다.

사용 목적	도구	
디스크 및 파일 분석	- Autopsy	: 오픈 소스 포렌식 도구 / 하드 디스크 분석 및 파일 복구에 사용
	- FTK (Forensic Toolkit)	: 강력한 검색 기능과 이미지 분석 기능 제공
	- EnCase	: 법 집행 기관에서 주로 사용 / 데이터 분석과 증거 보존 기능에 특화됨
메모리 분석	- Volatility	: 메모리 덤프 분석을 통해 실행 중인 프로세스, 네트워크 연결, DLL 로딩 정보 등 분석
	- Rekall	: Google에서 개발한 메모리 포렌식 도구
네트워크 분석	- WireShark	: 패킷 캡처 및 트래픽 분석을 통해 의심스러운 통신을 탐지
	- NetworkMiner	: 네트워크에서 수집된 패킷을 분석하여 공격의 흔적을 파악
	- Snort	: 침입 탐지 및 트래픽 분석 기능을 제공하는 오픈 소스 도구
모바일	- Cellebrite UFED	: 스마트폰 데이터 복구 및 분석을 위한 상용 도구
	- Oxygen Forensic Detective	: 모바일 기기 및 클라우드 서비스에서 데이터를 추출하고 분석
	- Magnet AXIOM	: 모바일과 클라우드 및 컴퓨터 포렌식을 지원하는 다기능 도구
클라우드 및 이메일 분석	- Google Takeout & Microsoft eDiscovery	: 클라우드 서비스에서 사용자 데이터 다운로드 및 분석
	- X1 Social Discovery	: SNS 및 이메일 데이터 분석을 위한 도구
종합적인 포렌식 플랫폼	- The Sleuth Kit (TSK)	: 파일 시스템 분석 및 증거 수집을 위한 도구 모음
	- X-Ways Forensics	: 디스크, 메모리, 네트워크 분석을 포함한 종합 포렌식 도구

4. 포렌식 조사 과정



자료: 감사원

디지털 포렌식 조사는 체계적인 절차를 따라 진행되며, 일반적으로 “증거 수집(Evidence Collection) → 보존(Preservation) → 분석(Analysis) → 보고서 작성 및 법적 대응(Documentation & Legal Considerations)”의 순서로 이루어진다고 한다. 각 단계에서 신뢰성과 무결성을 유지하는 것이 가장 중요하다고 한다.

“증거 수집” 단계에서는, 말 그대로 사건과 관련된 디지털 증거를 수집하는 과정을 말한다. 이 단계에서는 가능한 모든 관련 데이터를 확보해야 하며, 무결성을 유지하는 것이 핵심이라고 한다. 저장 장치에서 데이터를 수집하고, 휘발성 데이터를 빠르게 확보하고, 시스템 및 네트워크 로그를 수집하고, 이메일, 소셜 미디어 데이터 등 필요한 증거를 확보해야 한다. 이때, 원본 데이터를 직접 조작하지 않고, 증거를 복제하여 사용해야 하고, 증거가 변조되지 않도록 체계적으로 기록해야 한다.

“보존” 단계에서는, 수집한 증거가 훼손되거나 변조되지 않도록 원본 상태 그대로 유지해야 한다. 확보한 디지털 증거가 법적 효력을 유지하려면 무결성 보장이 필수적이다. 이때, 수집한 데이터의 무결성을 보장하기 위해 원본과 동일한 복사본을 꼭 생성해야 한다고 한다. 이를 통해, 해시값을 사용하여 증거가 변경되지 않았음을 검증하고, 수집된 증거를 안전한 저장소에 보관하여 외부 접근을 차단시켜야 한다고 한다. 이 단계에서는 원본 데이터를 직접 분석하거나 변경하지 않도록 꼭 주의해야 하며, 연계 보관성(Chain of Custody)을 문서화하여 증거의 신뢰성을 유지해야 하는데 힘써야 한다고 한다.

“분석” 단계에서는, 수집한 증거를 기반으로 공격의 경로를 추적하고, 범죄의 흔적을 발견하는 단계이다. 공격자가 어떤 수법을 사용했는지, 피해 범위는 어느 정도인지 등을 분석하여 결론을 도출해야 한다고 한다. 이때, 파일, 로그, 메모리 등의 데이터를 분석하여 공격 흔적을 추적하고, 삭제된 파일이나 은닉된 데이터를 복구하여 증거를 확보한다.

분석 과정에서 증거를 훼손하지 않도록 신중하게 접근해야 하며, 법적 증거로 활용될 수 있도록 모든 과정과 결과를 기록해야 한다고 한다.

“보고서 작성 및 법적 대응” 과정에서는, 분석한 내용을 체계적으로 정리하여 보고서를 작성하고, 법적 증거로 활용할 수 있도록 문서화해야 한다. 문서화 과정에서 포렌식 절차를 준수했음을 입증해야 한다고 한다. 사건 개요, 수집된 증거, 분석 결과 등을 정리하여 보고서로 작성해야 하고, 법적 증거로 사용될 수 있도록 분석 과정과 방법을 상세히 기록해야 한다고 한다. 법적 효력을 유지하기 위해, 문서화 과정에서도 절차를 엄격히 준수해야 하고, 객관적인 사실만을 기반으로 작성해야 한다고 한다.

2〉 디지털 포렌식의 활용 사례

1. 실제 사이버 범죄 수사 사례 & 기업 보안에서의 포렌식 활용

1) 소니 픽처스 해킹 사건 (2014년)

2014년, 본인들을 “Guardians od Peace” 라고 칭하는 해킹 그룹이 소니 픽처스 엔터테인먼트를 해킹하고, 직원 정보, 영화 미공개 파일, 내부 문서를 유출하였다. 공격자는 랜섬웨어를 사용해 주요 시스템을 마비시키고, 영화 ‘더 인터뷰’의 개봉을 취소하라고 요구하였다. 이 과정에서 네트워크 로그 분석을 통해, 공격자가 북한 해킹 그룹 “라자루스”와 관련이 있음을 발견해냈다. 또한, 악성 코드의 코드 패턴을 분석하여 이전 북한 해킹 사례와 유사한 점을 확인해내었고, 공격자의 내부 침투 경로를 추적하여 초기 감염 지점을 찾아낼 수 있다고 한다.

2) 콜로니얼 파이프라인 랜섬웨어 사건 (2021년)

2021년 5월, 미국 최대 송유관 운영업체 “콜로니얼 파이프라인(Colonial Pipeline)”이 러시아 기반 해킹 조직 "다크사이드(DarkSide)"의 랜섬웨어 공격을 받았다. 해커들은 회사를 마비시키고 비트코인 75 BTC(약 440만 달러)의 몸값을 요구했다고 한다. 이때, 랜섬웨어 감염 경로를 분석하여, VPN 시스템이 해킹된 것이 원인임을 확인할 수 있었다고 한다. 또한, 암호화된 파일과 비정상적인 트래픽을 분석하여 공격자의 서버 위치를 파악할 수 있었고, 비트코인 블록체인을 추적하여 해커들이 받은 몸값을 일부 회수하는 데 성공하였고 한다.

3) 모건 스탠리 데이터 유출 사건 (2015년)

2015년, 미국 금융 기업 “모건 스탠리(Morgan Stanley)”에서 고객 35만 명의 정보가 유출되는 사건이 발생했다. 내부 직원이 고객 정보를 빼돌려 불법적으로 공유한 것으로 드러났는데, 이때 내부 직원들의 시스템 접속 로그를 분석하여 비정상적인 데이터 다운로드 패턴을 발견하였고, 데이터 복사 및 전송 내역을 추적하여 범인을 특정할 수 있다고 한다. 이메일과 외부 저장 장치 사용 기록을 조사하여 정보 유출 경로를 파악할 수 있었다고 한다.

4) 야후(Yahoo) 대규모 해킹 사건 (2013-2014년)

2013년과 2014년에 걸쳐 “야후(Yahoo)”는 30억 개의 사용자 계정 정보가 유출되는 해킹 공격을 당했다고 한다. 이 사건은 인터넷 역사상 최대 규모의 데이터 유출 사고로 기록된 사건이라고 한다. 이때, 데이터베이스 접근 기록을 분석하여 공격자의 초기 침입 시점을 추적하여서, 계정 정보가 유출된 경로를 찾아내고, 공격자가 특정 국가의 지원을 받았음을 확인할 수 있었다고 한다. 또한, 해킹된 데이터가 다크웹에서 판매되고 있음을 포착하여, 추가 피해를 방지하기 위한 대응책을 마련하였다고 알려져 있다. 야후는 이 사건으로 인해, 3억 5천만 달러의 기업 가치 하락을 경험했고, 해킹 대응 실패에 대한 비판을 피할 수 없었다고 한다. 이후 보안 정책을 강화했으며, 사용자 비밀번호 암호화 및 다중 인증 시스템을 도입하였다고 한다.

5) 마리오트 호텔 고객 정보 유출 사건 (2018년)

2018년, 글로벌 호텔 체인점 “마리오트(Marriott)”에서 약 5억 명의 고객 정보가 유출되는 사고가 발생했다. 공격자는 2014년부터 호텔 예약 시스템에 침입하여 고객들의 여권 정보, 신용카드 정보를 수집했다고 알려져 있다. 이때, 네트워크 포렌식을 통해, 장기간 지속된 APT 공격임을 확인할 수 있었다고 한다. 또한, 로그 분석을 통해, 공격자의 움직임을 추적하고 어떤 시스템이 감염되었는지 파악할 수 있었다고 한다. 이후, 마리오트는 데이터베이스 암호화 및 접근 통제 시스템을 강화하여 추가적인 피해를 방지하였고, 사이버 보안 강화 및 고객 데이터 보호 정책을 도입했다고 한다.

2. 금융권 및 법 집행 기관에서의 포렌식 적용 사례

1) 금융 사기 탐지 – 스위프트(SWIFT) 네트워크 해킹 사건 (2016년)

2016년, 해킹 그룹이 방글라데시 중앙은행(Bangladesh Bank)의 SWIFT 네트워크를 해킹하여 8천 1백만 달러를 불법 이체하는 사건이 있었다. 공격자는 위조된 금융 거래 요청을 생성하여 국제 송금을 시도했다고 알려져 있다. 이때, 은행 네트워크 로그 분석을 통해, 공격자의 침입 경로를 식별하였다고 한다. 그 후, 트랜잭션 데이터를 조사하여 비정상적인 금융 거래 패턴을 발견할 수 있었다고 한다. 수사팀은 국제 금융 거래 흐름을 추적하여 자금이 필리핀, 스리랑크 등으로 송금되었음을 확인할 수 있었다. 이후, 은행 시스템에 대한 포렌식 조사가 더욱 강화되었다고 한다.

2) 법 집행 기관 – FBI 아동 착취 사이트 다크웹 수사 (2015년)

2015년, FBI는 다크웹에서 운영되던 아동 착취 사이트 "Playpen"을 적발하고 폐쇄하였다. 해당 사이트는 다크웹에서 Tor 네트워크를 이용해 운영되었으며, 수천 명의 사용자가 활동 중이었다고 한다. 수사팀은 Tor 네트워크를 분석하여 사용자의 IP 주소를 추적하였고, 서버 로그와 사용자 활동 데이터를 분석하여 사이트 운영자를 특정하였다고 한다. 그 후, 법적 절차를 준수하며 서버를 압수하고 데이터 증거를 확보하여, 200명 이상의 용의자를 체포하였다고 한다. 해당 사건은 다크웹 범죄 수사에서 디지털 포렌식이 결정적인 역할을 했던 사례로 평가받는다고 한다.

3〉 디지털 포렌식 – 실무에서의 한계점

디지털 포렌식은 사이버 범죄 대응 및 보안 사고 분석에 필수적인 기술이지만, 실무에 여러 한계점이 존재한다고 한다.

1. 데이터 양의 폭발적 증가

현대의 IT 환경에서는 방대한 양의 데이터가 생성되며, 디지털 포렌식 과정에서 이를 효율적으로 분석하는 것이 큰 관건이라고 한다. 빅데이터 시대에서 방대한 로그 및 파일 분석의 어렵다는 것이다. 기업 시스템, 클라우드 환경, IoT 기기 등에서 생성되는 데이터의 양이 점점 기하급수적으로 증가하면서, 모든 데이터를 분석하는 것이

불가능할 정도로 방대해지고 있다. 따라서, 로그 데이터, 네트워크 트래픽, 파일 시스템 등의 데이터가 지나치게 많아 중요한 증거를 신속하게 찾는 것에 어려움이 크다고 한다. 사고 발생 후 빠른 대응이 이루어져야 하지만, 수많은 데이터를 일일이 분석하는 데 시간이 너무 많이 소요된다는 것이다. 수집된 데이터를 분석하는 데 필요한 컴퓨팅 리소스 부족 문제가 발생하고, 그렇다고 수작업으로 모든 데이터를 분석하기에는 현실적으로 불가능하다. 또한, 로그 데이터 중에 노이즈가 많아서 필요한 증거를 선별해내는 과정에서도 시간이 많이 소요된다고 한다.

현재 이러한 문제점에 관한 여러 해결책들이 제시되고 있다. AI 및 머신러닝 기반의 자동 로그 분석 시스템 도입을 통한 분석 속도 향상, 빅데이터 분석 기술을 활용하여 중요한 증거만 선별적으로 분석하는 필터링 기법 개발, 클라우드 포렌식 기술을 동비하여 데이터 분산 처리 및 원격 분석 기능 강화 등 여러 시도 중인 방안들이 있다고 한다.

2. 암호화 및 익명화 기술의 발전

공격자들이 점점 더 정교한 기술을 사용하여 자신의 신원을 숨기고, 포렌식 분석을 방해하는 사례가 증가하고 있다고 한다. 특히, 암호화 및 익명화 기술의 발전으로 인해 공격자의 행적을 추적하는 것이 더욱 어려워지고 있다고 한다. VPN, Tor(다크웹)과 같은 익명화 기술을 이용하면 공격자의 실제 IP 주소를 추적하기 어렵다고 한다. 또한, 공격자들은 하드디스크, 파일, 통신 데이터를 강력한 암호화 기법으로 보호하여서, 추가적인 복호화 작업도 요구한다. 클라우드 스토리지, 암호화된 메신저 등을 통해 데이터를 유출하는 경우, 포렌식적으로 분석이 매우 어렵다는 허점 또한 있다고 한다. 실제로 실무적인 측면에서는, 해커들이 파일을 암호화하고, 세션 종료 후 자동 삭제하는 기술을 사용하여 증거를 남지기 않는다고 한다. 메모리에서만 실행되는 악성코드도 많이 발견되고 있는데, 이들은 디스크에 흔적을 남기지 않아서 분석이 까다롭다고 한다. 특히, 랜섬웨어 공격에서는 공격자가 암호화된 데이터를 해독할 수 있는 키를 가지고 있기 때문에, 피해자가 몸값을 지불하지 않는 한 데이터 복구가 불가능하다고 한다.

이러한 문제점에 대한 해결책 역시 여러 개 제시되고 있다. 실시간 네트워크 분석을 통해, VPN, Tor 사용 패턴을 탐지하고, 악성 트래픽을 차단하는 기술 개발, 포렌식 단계에서 메모리 분석을 강화하여, RAM 내 실행 흔적을 찾아 복구하는 기법 활용, 법 집행 기관과 협력하여, 암호화된 데이터에 대한 법적 접근 권한을 확보하는 제도 마련 등의 방안이 제시되고 있다고 한다.

3. 법적 이슈 및 개인정보 보호 문제

디지털 포렌식은 법적 증거를 확보하는 과정에서 개인정보 보호법과 충돌하는 경우가 많다. 포렌식 분석을 수행하는 과정에서 개인정보를 포함한 데이터를 수집해야 하지만, 이는 법적으로 문제가 될 수 있다고 한다. EU의 GDPR과 같은 강력한 개인정보 보호법이 적용되면서, 기업과 기관이 데이터를 무단으로 수집하는 것이 불법이 되었고, 일부 국가에서는 디지털 증거 수집 과정이 사생활 침해로 간주될 수 있어서 법적 논란이 발생할 가능성이 있다. 클라우드 환경에서는 데이터가 국가 간 이동이 가능하므로, 해당 국가의 법적 관할권이 모호해지는 문제가 있다고 알려져 있다. 이는 실무적인 부분에서, 특정 사건에서 증거 확보를 위해 개인 이메일, SNS 기록을 분석하는 것이 법적으로 허용되지 않을 수 있다. 또한, 회사 내부에서 포렌식 조사를 진행할 때도, 직원 동의 없이 데이터를 수집하면 법적 문제가 발생할 가능성이 있다. 클라우드 데이터 포렌식의 경우에는 클라우드 서비스 제공자의 협조 없이는 증거 수집이 불가능하다고 한다.

이 역시도 여러 해결방안들이 제시되고 있다. 법적 절차를 준수하면서 디지털 증거를 수집하기 위한 법적 가이드라인 강화, 개인정보 보호를 침해하지 않으면서 수사할 수 있도록 법원 영장 기반의 증거 수집 절차 도입, 클라우드 포렌식 분야에서 국제 공조를 통해 데이터 접근 권한을 조율하는 법적 협약 마련 등이 시도되고 있다고 한다.

4. 신종 공격 기법 등장

공격자들은 기존 포렌식 기법을 우회할 수 있는 새로운 공격 방법을 지속적으로 개발하고 있다. 특히, 파일리스 공격과 같이 디스크에 남기지 않는 기법이 등장하면서, 기존 포렌식 기법만으로는 공격을 추적하는 것이 어려워지고 있다. 파일리스 공격은 악성코드가 디스크가 아니라 메모리에서 실행되므로, 전통적인 파일 분석 방식으로는 탐지할 수 없다고 한다. 폴리모픽 멀웨어는 실행될 때마다 코드가 변형되기 때문에, 서명 기반 탐지 기법이 전혀 통하지 않는다고 한다. 또한, 클라우드 기반 공격은 공격자가 클라우드 환경에서 악성 코드를 실행하면, 포렌식 분석이 불가능하거나 데이터 접근 권한이 제한될 수 있다. 이는 공격자가 운영체제 내 정상 프로세스를 악용하여 공격하는 경우, 악성 행위를 구별하기 어렵다. 또한 클라우드 기반 악성코드는 기업 내부 서버가 아닌 외부 환경에서 실행되므로, 기존 포렌식 방법으로는 분석이 어렵다고 한다.

이를 해결하기 위해 여러 시도 중인 방안들이 있다. 파일리스 공격 대응을 위해 메모리 포렌식 및 행동 기반 탐지 기술 강화, 머신러닝을 활용하여 비정상적인 시스템 활동을 자동으로 탐지하는 보안 솔루션 도입, 클라우드 환경에서 발생하는 공격을 분석하기 위한 클라우드 포렌식 기술 개발 등이 있다.

결론

1〉 느낀 점

이번 SSR을 통해서, 디지털 포렌식과 관련된 법적인 부분들에 대해서 새롭게 배울 수 있었던 것 같다. 또한, 실제 사례들을 살펴보며, 포렌식 기법이 실무에서 어떤 식으로 적용되는지 이해할 수 있었던 것 같다. 디지털 포렌식의 실무적인 한계점에 대해 조사하면서, 현재 포렌식 기술이 해결해야 할 어려움들을 인식할 수 있었던 계기가 되었다. 한 번도 포렌식을 직접 해본 적이 없다고 생각하였었는데, 생각보다 포렌식이라는 분야가 엄청 넓어서, 그동안 내가 했던 것들이 포렌식이구나! 하고 놀라웠던 것 같다.

2〉 다음 제출 계획

이번 SSR을 통해 디지털 포렌식에 대한 기본 개념과 사례들을 살펴볼 수 있었지만, 실습을 진행하지 못한 것 같아서 아쉬웠던 것 같다. 아마 다음 SSR에서는 주로 실습 내용을 주로 다뤄보려고 한다. 특정 포렌식 기법 혹은 도구를 테마로 정하여, 여러 실습을 진행하는 것을 계획 중이다. 혹은 시중에 나와있는 여러 포렌식 CTF 문제들을 많이 접해보며, 다양한 도구나 접근 방향들을 익혀보는 것을 계획에 세우고 있다.

3〉 참고자료

KISA, [2021년 KISA Report 10월호_5] 모바일 포렌식 연구 및 조사의 동향과 발전방향

대검찰청, 형사소송법 개정과 개인정보보호법의 시행에 따른 디지털 증거 압수수색의 신뢰성 확보 방안에 관한 연구(2012)

숭실대학교 이규안, JTAG 방식을 이용한 모바일 포렌식 기법 연구 (2010)

https://scienceon.kisti.re.kr/srch/selectPORSrchArticle.do?cn=DIKO0011922070#

군산대학교 곽병선, 디지털 포렌식 수사의 문제점과 개선방안 (2011)

https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE01643646