https://doi.org/10.33778/kcsa.2023.23.5.045

익명 네트워크 기반 블록체인 범죄 수사방안 연구★

한 채 림*, 김 학 경**

요 약

IT 기술의 발전으로 따른 디지털 기기 사용의 보편화와 함께, 익명 통신 기술의 규모 또한 기하급수적으로 증가하고 있다. 이러한 상황에서 특히, 다크 웹(Dark web)과 딥웹(Deep web) 등 익명성을 보장하는 보안 메신저가 디지털 범죄의 온상지가 되고 있다. 익명 네트워크를 이용한 범죄 행위는 사용 기기에 로컬 데이터를 거의 남기지 않아 행위 추적이 어렵다. 미국 연방형사소송규칙과 영국 수사권한법에서는 온라인 수색 관련 법 및 제도 도입을 통해 대응하고 있으나, 한국은 관련 법의 부재로 인하여 수사적 대응 또한 전무한 실정이다. 종래의 (해외에서 사용되는) 온라인 수색 기법은 프로세스가 종료되면 아티팩트(Artifact) 수집을 할 수 없고, 메모리에만 데이터를 저장하는 악성코드에 대응할 수 없으며, 민감 데이터 식별이 어렵고, 무결성이 침해된다는 기술적 한계가 확인된다. 본 논문에서는 기본권 침해를 최소화하는 방향에서 물리 메모리 데이터 분석을 통한 익명 네트워크 사용자 행위 추적 기반 블록체인 범죄 수사방식의 국내 도입 방안을 제안한다. 클로링을 통해 수집한 다크 웹 사이트 사용자의 행위를 추적해 물리 메모리의 잔존율과 77.2%의 합의 성공률을 확인함으로써 제안 방안의 수사로서의 실효성을 입증하고자 하였다.

A Study on the Crime Investigation of Anonymity-Driven Blockchain Forensics

Han, Chae-Rim*, Kim, Hak-Kyong**

ABSTRACT

With the widespread use of digital devices, anonymous communication technologies such as the dark web and deep web are becoming increasingly popular for criminal activity. Because these technologies leave little local data on the device, they are difficult to track using conventional crime investigation techniques. The United States and the United Kingdom have enacted laws and developed systems to address this issue, but South Korea has not yet taken any significant steps. This paper proposes a new blockchain-based crime investigation method that uses physical memory data analysis to track the behavior of anonymous network users. The proposed method minimizes infringement of basic rights by only collecting physical memory data from the device of the suspected user and storing the tracking information on a blockchain, which is tamper-proof and transparent. The paper evaluates the effectiveness of the proposed method using a simulation environment and finds that it can track the behavior of dark website users with a residual rate of 77.2%.

Key words : Anonymous network, Blockchain, Digital evidence, Network forensic, Online search

접수일(2023년 11월 01일), 게재확정일(2023년 12월 07일)

* 성신여자대학교/융합보안공학과(주저자)
** 성신여자대학교/융합보안공학과(교신저자)

★ 본 연구는 2023년 산업보안 논문경진대회 동상 수상작을 수정·보완한 논문임을 밝힌다.

1. 서 론

IT 기술의 발전에 따라 디지털 기기가 보편화되면서 이를 매개로 한 범죄가 지속해서 증가 및 지능화되고 있다. 특히 디지털 범죄는 수사기관의 추적을 피하고자 다크 웹(Dark web)과 딥웹(Deep web) 내 익명 네트워크를 이용하는 양상을 보이기까지 하고 있다. 2018년 '웰컴 투 비디오(W2V) 사건'과 각종 마약 유통 및 성 착취물 유포 사건이 조명되면서, 익명 네트워크 기반 범죄는 중대 범죄로 자리 잡게 되었다. 익명 네트워크 범죄는 사용 기기에 로컬 데이터를 남기지 않아 행위 추적이 어렵고, 완전한 삭제가 어렵다. 이에 대해 독일, 미국과 영국에서는 온라인 수색을 법제화하여 실무에 활발히 활용하고 있으나, 국내에는 관련 법이 불비한 실정이다.

종래 해외에서 사용하는 온라인 수색 기법은 프로세스가 종료되면 메모리의 휘발성으로 인해 아티팩트(Artifact)를 수집할 수 없으며, 메모리에만 데이터를 저장하는 악성코드에 대응할 수 없고, 민감 데이터 식별이 어려우며, 무결성이 침해된다는 기술적 한계를 가지고 있다. 따라서 종래 온라인 수색 기법의 한계점을 보완한 국내 온라인 수색 제도 도입의 당위성이 존재하며, 이를 위해서는 정보의 자기 결정권 및 통신 비밀의 자유에 있어 기본권 침해에 대한 법적 근거의 요구 또한 필요하다.

본 연구에서는 독일(Online Durchsuchung)·미국(NIT: Network Investigative Technique)·영국(Equipment Interference)의 온라인 수색 기법에 대해 고찰하고, Operation Pacifier, 이른바 Playpen 사건에 사용된 온라인 수색(NIT) 코드와 Operation Venetic 사건에 사용된 장비 분석을 통해 온라인 수색 기법의 기술적 한계를 도출하고, 기본권 침해성 여부를 검토한다. 특히, 종래 수색 제도의 한계를 개선하기 위하여 물리 메모리 데이터 분석을 통한 익명 네트워크 기반 블록체인 다크 웹 범죄 수사방안을 제안하며, 범죄의 개방성·익명성을 고려한 실무지침 마련을 통해 국내 온라인 수색 도입에 관한 입법적 담론에 있어 개인의 기본권 침해를 최소화하였다.

본 연구의 주요 기술·정책적 기여점은 다음과 같다.

· 물리 메모리 데이터 분석을 통한 대응 방안으로써 종래 수색 기법의 메모리 휘발성 문제 개선 및 난독화 해제된 실행코드 추출

· 민감 데이터 식별 가능 및 암호화 이전·복호화 이후 데이터 획득

· 블록체인 기반의 안티-포렌식 기술로 공격 시간 유추 및 무결성 침해 문제 개선

· 익명 네트워크 범죄 수사 과정에서 발생 가능한 기본권 침해 방지

본 논문의 구성은 다음과 같다. 2장에서는 온라인 수색을 소개하고, 해외의 온라인 수색 기법을 활용한 수사사례를 검토한다. 3장에서는 익명 네트워크 기반 블록체인 다크 웹 범죄 수사방안을 제시하고, 4장에서는 익명 네트워크 커뮤니티의 물리 메모리 잔존율을 통해 수사방안으로서의 정합성을 입증한다. 마지막으로 5장에서 결론을 맺는다.

2. 온라인 수색 해외 법제 및 기술 그리고 기술의 한계

온라인 수색은 국가가 정보 주체가 사용하는 정보기술시스템에 기술적 수단을 개입하여 비밀리에 데이터를 수집하는 행위를 의미한다. 여기에서 데이터 수집 행위란, 수사기관이 정보통신망을 통해 정보 주체의 시스템에 저장된 데이터를 비밀리에 복제하거나, 감시하는 절차를 포함할 수 있다. 국가기관은 소프트웨어 및 하드웨어의 취약성을 이용하여 사용자의 컴퓨터에 원격 접속 후, 사용자의 작업을 감시하거나, 기기의 작동을 방해한다. 온라인 수색의 목적은 해킹을 통한 확보된 증거로 범죄혐의를 입증하는 것이므로, 타 감청 수단과 비교해 기본권 제한이 가장 높은 수사 처분이다[1].

2.1 온라인 수색 법률

2.1.1 독일

독일에서 온라인 수색은 범죄 예방과 수사 영역에서 각각 분리되어 규정되어 있다. 전자는 정보기술시스템에서의 비밀침입(Verdeckter Eingriff in informationstechnische Systeme)으로 연방범죄수사청법(Gesetz uber das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Lander in kriminalpolizeilichen Angelegenheiten)에서 규정되고[2], 후자는 Online-Durchsuchung으로 형사소송법(Strafprozessordnung)에서 규정된다[3]. 연방범죄수사청법은 모바일을 활용한 위치 및 정보 확인, 비밀리에 장비를 이용한 주거지 감청 등을 규정 대상으로 포함한다. 형사소송법에서는 통신 감청 및 정보 주체에 대한 정보기술시스템 내 악성코드 등 기술적 수단을 통한 감시라는 표제어로 규제되어 있다. Online-Durchsuchung를 활용한 대표적 수사사례는 Boystown(2021) 사건 등이 있다.

독일 연방수사청(Bundeskriminalamt, BKA)은 세계 최대 아동 포르노 다크 웹 플랫폼 '보이스타운(Boystown)'을 폐쇄하였다. 유럽연합 법집행협력청, 이하 유로폴(Europol)은 독일과 합동 조직을 구성하고, 네덜란드, 미국, 스웨덴, 캐나다, 호주 등과 공조하여 작전을 수행하였다. 수색에 사용된 기술적 수단은 공개되지 않았으나, 유로폴은 몰도바 공화국의 서버를 통하여 범죄자의 IP 주소를 획득하였고, 롤리펍(Lolipub)과 보이즈펍(BOYSPUB)의 채팅 서비스를 통하여 아동 성폭력 이미지와 동영상을 공유한 정황을 파악하였다.

2.1.2 미국

미국의 경우 온라인 수색은 통상 역외 압수수색 형태로 진행된다[4]. 연방형사소송규칙 제41장에서 온라인 수색의 영장 발부에 관한 법적 근거가 규정되어 있다. 실무상으로는 사용자의 식별 정보를 비식별화한 정보 주체의 기기에 접근하기 위하여 사용하는 방법이나 도구를 의미하는 '네트워크 조사 기법(Network Investigative Technique, NIT)'를 사용한다[5]. 네트워크 조사 기법(NIT)을 활용한 수사사례는 Operation Torpedo(2011)[6], Operation Pacifier(2015), Operation Trojan Shield(2021) 등이 있다.

2.1.3 영국

영국은 해킹을 통해 시스템에 비밀리에 침입하여 증거를 압수수색하는 처분을 장비 간섭(Equipment Interference)으로 개념화한다. 장비 간섭은 수사권한법(Investigatory Powers Act, IPA)[7]에서 대상특정 검사영장(Targeted Examination Warrant, TEW)과 대상특정 온라인 수색영장(Targeted Equipment Interference Warrant, TEIW)으로 규정되어 있다[8]. 온라인 수색 실무지침(Equipment Interference – Codes of Practice, EICP)[9]에서는 수집 대상을 장비데이터(Equipment data)와 시스템데이터(System data), 확인데이터(Identifying data)로 분류하고 있다. 장비 간섭을 활용한 대표적 수사사례는 Operation Venetic(2020) 사건 등이 있다.

2.2 온라인 수색의 기법 및 한계

본 연구에서는 온라인 수색 코드가 공개된 (미국) Operation Pacifier 사건과 (영국) Operation Venetic 사건의 기술적 분석과 (미국) Operation Trojan Shield 사건 검토를 통하여 종래 온라인 수색 기법 및 기술적 한계를 도출한다.

2.2.1 Operation Pacifier

Operation Pacifier, 이하 Playpen 사건은 다크 웹에서 운영된 아동 성 착취 사이트 'Playpen' 폐쇄를 위한 작전이다. 연방수사국(Federal Bureau of Investigation, FBI)은 토르(Tor) 히든 서비스를 통해 다크 웹 사이트에 접속한 사용자의 서버 위치와 정보를 추적하기 위하여 버퍼 오버플로우

(CVE-2013-0633)[10]와 메모리 손상(CVE-2013-0634)[11] 취약점을 이용한 온라인 수색(NIT)을 진행하였다.

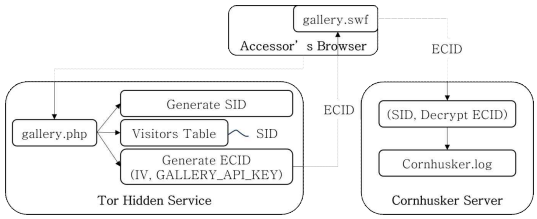
온라인 수색 코드(NIT) 분석을 위한 실험 환경은 다음과 같다. 본 연구에서는 사건과 동일한 네트워크 환경을 구성하기 위하여 토르(Tor) 익명 네트워크를 사용하였다. 토르 네트워크는 가드 노드(Guard Node), 릴레이 노드(Relay Node), 엑시트 노드(Exit Node)를 거쳐 다크 웹과 접속자를 연결함으로써 접속자의 익명성을 보장한다. 해당 연결에 사용되는 회로는 10분마다 갱신되어 사용자의 IP 추적을 어렵게 한다. 우분투(Ubuntu) 22.04 가상 머신을 사용하여 토르 웹 사이트와 콘허스커(Cornhusker) 서버를 동작시켰다. 콘허스커 서버는 토르 웹 사이트에 접속한 사용자와 온라인 수색 코드로부터 수집한 IP 주소를 비교하기 위한 로그와 트래픽을 수집하기 위한 서버로, 아파치(Apache web-server), MySQL 데이터베이스(MySQL Database)와 Twisted 프레임워크(Twisted Framework) 22.10[12]를 사용하여 구성하였으며, 이더넷(Ethernet) 네트워크로 클라이언트(client)와 서버를 연결하였다. JPEXS 플래시 디컴파일러(JPEXS flash decompiler) 18.4.1[13]를 사용하여 리버스 엔지니어링을 진행하였으며, swf 플래시 파일을 컴파일하기 위하여 Haxe 플래시 컴파일러(Haxe Flash Complier) 4.3.1[14]가 사용되었다.

온라인 수색의 프레임워크는 (Figure 1)과 같다. 토르 히든 서비스 서버와 토르 웹 사이트는 HTTP 프로토콜(Hypertext Transfer Protocol)을 통한 단방향 통신이, 콘허스커 서버와 토르 웹 사이트는 웹 소켓 프로토콜(Websocket Protocol, Apache)을 통한 양방향 통신이 이루어진다.

토르 히든 서비스에서는 웹 사이트에 접속한 사용자가 웹 페이지를 요청할 때마다 사용자 식별을 위한 세션 ID(Session ID, SID)를 난수 생성하였다. 사용자가 요청한 웹 사이트 간의 유사성을 비교하기 위하여 활동 로그를 생성해 SQLite 데이터베이스 내 visitors 테이블에 저장하였다. 세션 ID가 초기화 벡터(Initial Vector, IV)와 공유키 값(GALLERY_API_KEY)을 통해 암호화되는 결괏값을 ECID(Encrypted Session Identifier)라고 설정하였다[15.] ECID는 버퍼 오버플로우와 메모리 손상 취약점이 포함된 SWF 파일에 생성되고, 이때 해당 값은 세 개의 서버에 각각 다르게 저장된다.

토르 웹 사이트는 GALLERY_API_KEY로 정의된 공유키를 사용하고, 생성된 세션 ID를 암호화한 값을 비밀키로 사용하여 접속자를 식별한다. 웹 페이지 접속자와 온라인 수색 코드로부터 수집한 IP 주소의 유사성을 비교하기 위하여 ECID와 온라인 수색 코드를 통해 사용자 시스템에서 생성한 ECID를 사용하여 문자열을 생성하였고, 파이썬(Python)의 difflib 라이브러리[16]를 사용하여 비교하였다. 모든 시퀀스 요소 중 일치되는 항목의 비율에 2를 곱한 값으로 유사도를 계산하였으며, 유사도가 90% 이상일 때 동일 사용자로 판단하였다.

콘허스커 서버에서는 세션 ID와 IP 주소를 포함한 로그를 생성한다. IP 주소와 토르 웹 사이트로부터 전송받은 ECID 값을 복호화하여 로그에 접속하고, visitors 테이블의 세션 ID 값을 비교하여 유사도를 측정하였다.



(Figure 1) NIT 온라인 수색 프레임워크

Operation Pacifier 사건에서 사용된 온라인 수색 코드로 압수한 정보는 <Table 1>과 같다. 온라인 수색 코드를 통해 접속자의 IP 주소, MAC 주소, 운영체제, 사용자의 활동을 식별할 수 있도록 온라인 수색 코드가 생성한 고유 식별자, 온라인 수색 코드의 설치 여부, 장치 식별에 사용되는 호스트 이름, 활성화된 운영체제의 접속자 이름을 수집하였다.

〈Table 1〉 NIT로 수집된 정보

Section	Collected Data
1	Host name
2	IP address of the accessor
3	MAC address of the accessor
4	Name of the active operating system accessor
5	Operating system of the accessor
6	Unique identifier generated by the NIT
7	Whether NIT is installed

온라인 수색 코드 분석과 리버스 엔지니어링을 통한 NIT는 플래시 취약점을 활용한 접근이기 때문에, 애플리케이션이 차단되면 접속자의 IP 주소, SID 및 운영체제 정보수집이 불가하며, 메모리가 휘발되어 아티팩트(artifact)를 수집할 수 없다. 익명 네트워크 내 다크 웹 범죄가 고도화·지능화됨에 따라, 민감 데이터를 암호화하여 저장하거나 TEE에 보관하는 등 다양한 보안 기법이 사용되는데, NIT는 이러한 보안 기법에 대응하기에는 역부족한 실정이다.

2.2.2 Operation Trojan Shield

Operation Trojan Shield 사건은 마약 밀매를 공조한 캐나다 보안업체인 팬텀 시큐어(Phantom Secure)를 폐쇄하기 위한 작전이다. 연방수사국(FBI)은 메일, 위치 정보 및 전화 등의 기능을 무력화하기 위한 암호화 채팅 애플리케이션 '아놈(ANOM)'을 이용하여 온라인 수색을 진행하였다. 아놈은 그래핀 OS(Graphene OS) 기반 애플리케이션으로, 개인의 PIN(Personal Identification Number)을 입력하여 기기 내 모든 정보를 삭제한다. 해당 수사에서는 프록시(proxy) 서버를 통해 아놈과 FBI 서버를 연결하여 기기에 전송되는 모든 메시지를 개인키로 복호화하였고, 각 기기의 식별번호를 통하여 접속자를 식별하였다.

해당 작전은 파일 시스템 기반의 포렌식 기법으로, 난독화된 형태의 실행코드가 추출되며, 민감 데이터를 식별할 수 없다.

2.2.3 Operation Venetic

Operation Venetic 작전은 영국 국립범죄수사청(National Crime Agency, NCA)에서 범죄에 관한 정보 교환에 사용되고 있다고 보도된 암호화 채팅 시스템 인크로챗(EncroChat)에 malware을 삽입하여, 수천 건의 범죄자 및 범죄 도구 등을 압수한 사건이다. 인크로챗은 암호 통신을 지원하는 OTR 프로토콜(Off-the-Record Messaging) 기반 메시징 앱으로, 수사기관은 안드로이드 기기에 인크로챗을 탑재하여 볼륨 버튼과 함께 전원 버튼을 눌러서 부팅할 경우 수사기관의 서버를 통한 익명 통신을 할 수 있는 암호화된 인터페이스를 사용하였다. 이때, 접속자의 익명성을 강화하기 위하여 기기 내 모든 데이터 초기화를 위한 PIN 코드, 메시지 자동 삭제 등과 같은 기능을 추가하였다.

연방수사국은 powershell을 통해 인크로챗에 접속한 사용자의 위치와 정보를 추적하기 위하여 원격 접속 시스템에 운영체제 명령 실행(OS Command Execution) 공격을 수행하여 온라인 수색(EI)을 진행하였다.

장비 간섭(EI) 분석을 위한 실험 환경은 다음과 같다. 본 실험에는 칼리 리눅스(kali linux) 내 파워쉘 엠파이어(powershell empire)와 파워스플로이트(powersploit) 공격 프레임워크가 사용되었다. 관리자 시스템에서 사용자 시스템으로 원격 cmdlet을 실행하여 파일을 복사하였고, 바이너리 명령어를 통하여 powershell session에 연결하였다. profile 스크립트에 공격 코드를 삽입하기 위하여 레지스트리 데이터를 powershell.exe -NonInteractive -WindowStyle Hidden -ExecutionPolicy bypass -File "C:\windows\ system32\evil.ps1"와 같이 설정하였다.

해당 사건에서 사용된 수색 프레임워크는 다음과 같다. 이벤트 필터의 쿼리 조건에 해당하는 이벤트가 발생하면 연방수사국에 이벤트가 전달되고, 인크로챗 사용자가 전달받은 이벤트를 인지하면 powershell이 실행되면서 profile 스크립트가 로딩되어 profile.ps1에 삽입된 공격 코드가 동작한다. 이때, powershell 콘솔에서 수행한 공격 행위에 대한 직접적인 흔적은 남지 않으나, 의심스러운 powershell 스크립트의 흔적에 대해 해당 po

wershell prefetch 파일의 생성 시간과 마지막 실행 시간의 간격을 통하여 공격 시간을 추측할 수 있다. 특히 스크립트 파일 내에서 삽입된 공격 코드를 탐색하는 profile.ps1 파일은 생성 후 대부분 수정되지 않기 때문에 공격 시간을 유추하기가 쉽고, 메모리에만 데이터를 저장하는 악성코드에 대해 대응이 불가하다.

Operation Venetic 사건에서 사용된 온라인 수색 기술을 통하여 압수한 정보는 <Table 2>와 같다. 장비 간섭을 통해 CPU 사용 시간, 접속자의 가상환경, 악성 NPM 패키지, 스크립트 파일의 저장 위치, 장치 식별에 사용되는 호스트 이름, 활성화된 운영체제의 접속자 이름을 수집하였다.

〈Table 2〉 티로 수집된 정보

Section	Collected Data
1	CPU Usage time
2	Host name
3	Location where the equipment is stored
4	Malicious NPM package
5	Name of the active operating system accessor
6	Virtual environment

정리하자면, 상기 온라인 수색 제도를 사용한 수사사례들은 압수수색 영장의 범위가 넓어서 다크 웹 내의 모든 접속자의 기기를 획일적으로 추적할 수 있다는 점에서 사법관할권의 문제가 발생할 수 있으며, 나아가 제삼자의 기본권 침해 위험도 배제할 수 없다[20]. 수색의 과정에서 부가적인 정보수집의 명목으로 피수색인의 개인정보 노출 우려가 있기 때문이다. 제한범위의 광범위성으로 인해 수집한 정보를 제한 없이 복제, 전송, 추출할 수 있기에 수색의 범위를 명확하게 특정해야 하나, 아직 명확하게 특정 지은 수사사례가 없다는 맹점이 있다.

기술적 수단을 활용한 온라인 수색의 경우, 증거 확보를 위한 수색에 그치는 것이 아니라, 함정수사와 같은 수단으로 악용될 수 있다. 처분의 확장성을 통해 범죄자에게 범죄의 기회를 새롭게 제공하는 실정인 것이다.

종래 온라인 수색 제도의 난독화된 실행코드 추출, 메모리 휘발성, 무결성, 민감 데이터 식별 불가 등의 기술적 한계 및 기본권 침해를 해결하기 위해 본 논문에서는 물리 메모리 데이터 분석을 통한 익명 네트워크 기반의 블록체인 다크 웹 범죄 수사방안을 제안한다.

3. 온라인 수색 기법 개선 방안

본 장에서는 물리 메모리와 가상 메모리를 결합한 데이터 분석 기반의 블록체인 사용자 행위 추적 프레임워크를 제시하고, 제시한 온라인 수색 기법을 평가해 보고자 한다.

3.1 온라인 수색 기법 개선 방안 제시

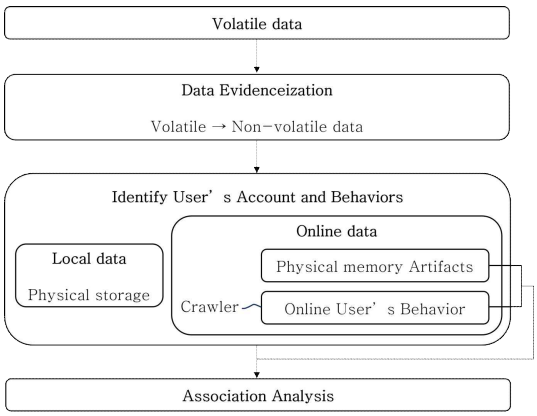
제안하는 수사방안의 물리 메모리 구조도는 (Figure 2)와 같다. 해당 구조도는 제안하는 블록체인 기반 포렌식 기법의 합의에 해당한다. 로컬 아티팩트만으로는 사용자 행위 추적을 위한 정보수집이 제한되어 물리 메모리를 이용하여 웹 서비스 접속 및 로그인 이력 등 로컬에서 저장되지 않는 정보를 수집하였다. 휘발성 데이터를 증거화하여 익명 네트워크 접속자 계정 및 행위 식별을 통해 온라인 데이터를 수집하고, 타임라인을 분석하여 사용자의 활동과 로컬 아티팩트와의 연결성을 예측한다. 이때, 수집 대상은 로컬 데이터, 온라인 데이터와 휘발성 데이터로 설정하였다.

로컬 데이터는 물리 저장소에 저장된 데이터 및 익명 네트워크 설치 이력 등을 수집하였고, 휘발성 데이터를 비휘발성 데이터로 전환하여 데이터를 증거화하였다.

온라인 데이터는 물리 메모리 아티팩트를 활용하거나, 온라인상의 사용자 행위를 수집하여 채증한다. 전자는 사이트 로그인 및 접속 이력과 계정 인증 정보 식별을 통해 접속자의 계정을 식별하고, 후자는 보안 메신저 ID, 작성 게시글, 파일 공유 행위 등을 크롤러를 통해 수집하는데[17], 이로

써 상시로 변동되는 도메인에 대한 접속자의 안티-포렌식(anti-forensic) 행위를 방지할 수 있으며, 민감 데이터 식별이 가능하다.

상기 데이터를 대상으로 익명 네트워크 사용 시점 전후 로컬 시스템의 사용자 활동 분석 및 로컬 아티팩트와의 연관성 분석을 통하여 수사 대상자를 식별하였다.



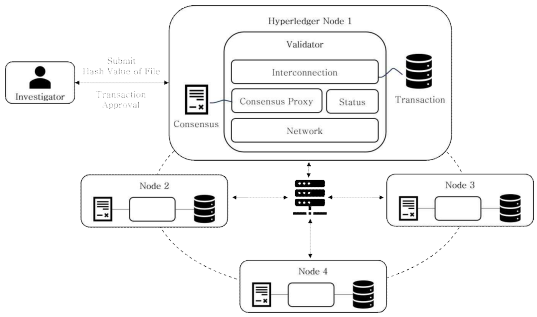
(Figure 2) 제안하는 온라인 수색법의 물리 메모리 분석 구조도

본 논문에서 제안하는 블록체인 기반 사용자 행위 추적 프레임워크는 (Figure 3)과 같이 네트워크 계층, 데이터 계층, 애플리케이션 계층, 트랜잭션 계층 및 합의 계층으로 분류된다. 수사 과정에서 조사자는 하이퍼레저 프레임워크를 통해 증거의 무결성을 검증하고, 장치를 식별하고, 자료를 쉽게 갱신할 수 있다. 블록체인을 구성하는 프로세스의 기능은 다음과 같다.

네트워크 계층은 허가된 사용자 간 사설 P2P 네트워크를 설정한다. 이때 각 노드는 다른 노드와의 상호작용을 위해 동일하게 간주하였다. 네트워크 계층은 블록체인 네트워크 트랜잭션의 유효성을 보장하기 위하여 비잔틴 장애 허용 기반 합의 알고리즘(Practical Byzantine Fault Tolerance, PBFT)을 사용하여 합의에 참여하는 모든 노드를 캡슐화한다. 노드 간 PBFT 합의 프로토콜을 공유함으로써 내결함성을 유지하며, 무결성을 보장한다.

트랜잭션 계층은 증거의 유효성을 검사하며, 신뢰성을 보장한다. 트랜잭션 데이터 블록에는 이전 블록의 해시 인덱스 값이 포함되는데, 이러한 데이터 노드는 이전 블록의 해시값, 랜덤으로 설정된 숫자, 타임스탬프, 머클트리(Merkle-tree)[18]에 따른 해시 루트로 구성되어 노드를 확인한다. 트랜잭션 블록이 생성되면 네트워크 계층에 연결되고, PBFT가 생성된다.

애플리케이션 계층은 합의 승인, 파일의 해시값을 전송하는 기능 등을 수행한다. 조사자와 하이퍼레저 프레임워크는 8008 TCP 포트를 통해 이루어진다.



(Figure 3) 블록체인 기반 사용자 행위 추적 프레임워크

본 논문에서 제안하는 온라인 수색 방안과 종래 방식을 비교한 결과는 <Table 3>과 같다. 제안 방안은 물리 메모리를 사용함으로써 제한적인 정보 수집 범위 문제를 해결한다. 물리 메모리 기반의 로컬 및 온라인 데이터를 수집하여 민감 데이터를 식별하고, 사용자의 안티-포렌식 행위를 방지하며, 블록체인 기반의 행위 추적 기법으로 내결함성 및 무결성을 보장한다.

〈Table 3〉 NIT, EI와 제안 방안의 비교 분석

	NIT	EI
Vulnerability Utilized	Buffer overflow, Memory corruption	O S Command execution
Online Search Process	1. Create Session ID 2. Code execution 3. Data Collection	
Limitation	- Easy to guess attack time - Unable to collect artifact - Unable to collect information when blocking applications - Unable to respond malware stores data only in memory	

	Proposed idea
Online Search Process	Gather information using physical memory · Local Data - Data stored in physical storage - History of installing anonymous network · Online Data - Proof of volatile data
Feature	- Ensure fault tolerance and integrity(security) - Prevention of anti-forensics acts - Sensitive data identifiable - Troubleshooting limited information gathering scope

3.2 제안한 수사 기법에 대한 평가

평가는 국내 이용자가 많은 익명 네트워크 커뮤니티 10개의 물리 메모리 잔존율과 공격이 있는 환경에서의 합의 성공률을 지표로 설정하여 제안하는 온라인 수색 방안의 실효성과 보안성을 측정하였다. 사용자의 행위 추적을 위한 데이터의 수집 방법은 <Table 4>와 같다.

〈Table 4〉 제안하는 온라인 수색법의 데이터 수집 방안

Section		Collected Data	
Local Artifact	Lokinet	C:\ProgramData	· Address of the Exit node · Crash dump files · Node Database · Router Uptime log · Setting files
		C:\Program Files	ID Signed to the Bootstrap node
	In need of Set-up	· Cached files · Login password · Number of visits, Title of web services, URL accessed by Tor network	
	Not Required to be Set-up	· Guard node List · Tor network Usage time · URL hosting the server and web services	
Memory Artifact		User's Login history	
		User's Connection history	
		File Sharing behavior	
		Posting behavior	

3.2.1 물리 메모리 잔존율

물리 메모리 잔존율을 위한 사용자 행위 추적은 로컬 아티팩트와 물리 메모리 분석을 통하여 진행하였으며, 전자의 경우 lokinet[19]을 사용하여 수집하거나, 추가 설정의 필요 여부에 따라 수집 목록을 세 가지로 분류하였다. lokinet을 통해 ProgramData 파일에서 lokinet 설정 파일, PAGE_READWRITE 에러 시 생성되는 덤프 파일, 노드 데이터베이스, 라우터 가동 시간 로그, 엑시트 노드의 주소값을 수집하였고, Program Files 파일에서 부트스트랩 노드에 서명된 ID를 수집하였다. 별도의 설정이 불필요한 가드 노드 리스트, 서버와 웹 서비스 호스팅을 하는 URL(Uniform Resource Locator), 토르 네트워크 사용 시간은 Tor 폴더(로컬 아티팩트) 내 state, torrc 파일에서 수집하였

고, 별도의 설정이 필요한 로그인 암호, 캐시 파일, 토르 네트워크로 접속한 URL, 방문 횟수, 웹 서비스 제목은 profile.default 폴더 내 cache, places.sqlite(moz_places), logins.json & key4.db 파일에서 추출하였다. 이때, 캐시된 파일로 다크 웹 내 저장된 멀티미디어 파일과 토르 브라우저를 통해 접근한 웹 서비스를 유추할 수 있다.

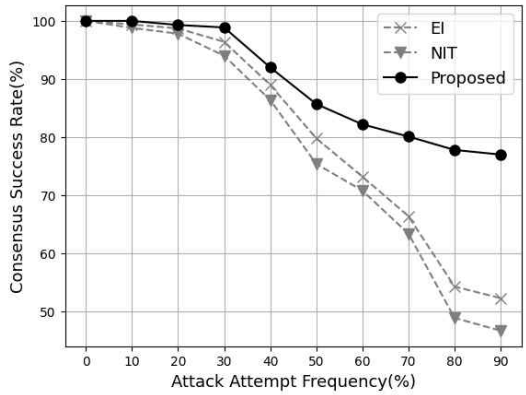
후자의 경우 물리 메모리에 hiberfil.sys, pagefile.sys, swapfile.sys 가상 메모리를 결합하여 익명 네트워크 사이트 10개에 대한 사용자의 로그인 및 접속 이력, 게시글 작성 및 파일 공유 행위를 유추하였다. XOR로 암호화된 MBR(Master Boot Record) 정보를 복호화한 후 헥스 에디터(Hex Editor, HxD) 2.5를 사용하여 디코딩하였다. 로그인 이력은 그림 3과 같이 'log=', 'login=', 'req_username=', 'username='의 형태로 웹 사이트마다 다른 흔적을 보인다. 접속 이력은 토르 네트워크 내 웹 서비스 요청에 "250 OK"로 응답하는 로그들을 선별하였고, SOCK5 프로토콜 구조를 통하여 접속자가 사용한 웹 서비스와 사용 시간을 식별하였다. 메모리 아티팩트 분석을 통해 사용자 행위와 시간 값, 작성 게시글 내용 등을 통하여 게시글 작성 행위를 파악하였다. 파일 공유 사이트 URL 정규 표현식을 통하여 물리 메모리 내 파일 공유 아티팩트를 수집해 사용자 간의 파일 공유 행위를 유추하였다. 이로써 난독화가 해제된 실행코드를 추출할 수 있으며, 암호화하기 이전 및 복호화 이후의 데이터를 수집할 수 있다.

3.2.2 보안성

제안하는 수사방안의 보안성 측정을 위하여 faulty 노드의 합의 성공률(consensus success rate)을 평가 지표로 설정하였다. 합의 성공률은 전체 합의를 시도한 횟수 중 합의에 성공한 로컬 노드의 수를 의미한다. Faulty 노드의 투표 영향력(voting power)이 합의의 성공과 신뢰도를 결정하는데, 본 연구에서는 합의 실패(consensus failure)에 영향을 미치는 faulty 노드가 전체 노드의 절반 이상일 경우로 가정하고 실험을 진행하였다. 외부의 공격자가 공격을 시도하여 증거 수집을 교란시킨다고 할 때, 합의 성공률은 수식 (1)과 같이 표현할 수 있다.

$$Consensus\ success\ rate(\%) = \frac{voting\ power\ of\ faulty\ node}{total\ nodes} \quad (1)$$

실험은 10개의 노드가 500개의 블록을 생성하는 실험을 500번 진행한 뒤 공격 시도를 0%부터 90%까지 늘리며 이들의 평균값을 산출하여 진행하였다. (Figure 4)는 공격이 있는 환경에서의 NIT, EI와 제안 방법의 합의 성공률을 나타낸 그래프이다.



(Figure 4) Consensus Success Rate based on Attack Rate

x축을 공격 시도의 빈도, y축을 합의 성공률이라고 설정할 때, 세 모델 모두 공격 시도의 비율이 증가할수록 합의 성공률은 감소하는 반비례 양상을 보인다. 공격 빈도가 90%일 때, NIT와 EI의 합의 성공률은 각각 46.7%, 52.3%이고 제안 방법의 합의 성공률은 77.2%이다. 제안 방법은 공격이 존재하는 환경에서 500개의 합의를 생성하고자 할 때, 386개의 블록 합의에 성공할 수 있다.

4. 결론

본 논문에서는 물리 메모리와 가상 메모리를 결

합한 데이터 분석 기반의 블록체인 사용자 행위 추적 방안을 제안하고, 수사로서의 정합성을 평가하였다. 종래 온라인 수색 기법은 메모리의 휘발성으로 프로그램이 종료되면 아티팩트를 수집할 수 없고, 무결성이 침해되며, 메모리에만 데이터를 저장하는 악성코드에 대응할 수 없고, 민감 데이터 식별이 어렵다는 기술적 한계와 기본권 침해의 문제가 존재한다. 제안하는 기법을 통하여 종래 파일 시스템 기반 포렌식 분석 기법의 기술적 한계인 민감 데이터 식별 및 사용자 행위 추적 문제를 해결하였고, 공격이 있는 상황에서도 내결함성을 유지하였다. 이에, 기본권 침해를 최소화하는 방향으로 물리 메모리 데이터 분석을 통한 익명 네트워크 사용자 행위 추적 기반의 블록체인 범죄 수사방식의 도입이 필요하다.

이에, 본 연구에서는 이러한 기술적 기법의 실현 전제 조건으로서 다음 세 가지 측면에서 온라인 수색의 국내 도입방안에 관한 기술·법적 제안을 해보고자 한다.

첫째, 온라인 수색 법적 근거가 마련되어야 한다. 온라인 수색은 비공개 처분으로, 형사소송법상 공개처분인 압수수색 제도에서 포섭하기에는 한계가 있으므로, 국가기관에 의한 온라인 수색이 헌법상 침해하는 기본권에 대한 새로운 검토가 필요하다. 수사기관과 정보기관이 국가안보와 범죄 및 테러의 예방과 수사에서 모두 사용 가능하며, 감시의 느낌을 최소화할 수 있도록 온라인 수색에서 '수색'이라는 용어를 (다른 용어로) 수정할 필요성이 있다.

두 번째, 추가 영장 집행 승인 절차의 도입이다. 법률에서 허용하는 제한적 조치로 온라인 수색을 운용하기 위해서는 기본권 제한에 헌법상 원칙을 따라야 한다. 목적의 정당성, 과잉금지원칙의 준수, 수단의 적합성 등을 만족시킬 때만 기본권 제한이 정당화될 수 있다. 그렇다면, 기존의 온라인 수색 집행 승인 절차에 관련성이 있는 증거만 선별해서 압수하기 위한 추가 승인 절차를 거쳐야 한다.

마지막으로, 사건 특징에 따른 개별적 온라인 수색 코드 개발 및 집행이다. 로그인된 사용자가 대상 시스템에서 발생한 이벤트인지 아닌지를 파악하고, 원격으로 대상을 식별하기 위하여 각각의 사건에 따른 코드가 개발되어야 한다. 온라인 수색 코드 설치 이전에 컴퓨터에 내장된 데이터와 설치 이후에 생성된 데이터를 비교하여 수집된 모든 데이터로부터 수사기관에서 필요로 하는, 특히 관련성 있는 데이터만 선별하는 절차도 추가되어야 할 것이다.

온라인 수색은 대상 범위가 넓어 범죄사실의 대상성만을 기준으로 수색 범위를 정확히 특정하기 어려울 수 있다. 그런데, 수색 범위가 특정되지 않는 것은 일반 영장에 해당하여 영장주의 본질상 허용될 수 없다. 이는 아쉽게 디지털 증거 압수수색의 본질적 딜레마이기도 하다. 향후 온라인 수색 기법 국내 도입에 관한 법 제도적 논의에 더해, 본질적 한계를 해결하기 위한 기술적 수단의 절차 활용 및 통제 방안과 더불어, 프로세스가 메모리 할당을 해제했을 시 데이터를 획득할 방안에 관한 융합적 연구를 진행해보고자 한다.

참고문헌

[1] 이상진, 디지털 포렌식 개론, 이룬, 2015.

[2] Gesetz uber das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Lander in kriminalpolizeilichen Angelegenheiten, 1 B.K.A.G. § 49, 2022.

[3] Strafprozeßordnung, 8 S.t.P.O. § 100b, 2022.

[4] Federal Rules of Criminal Procedure, 41 F.R.C.P § 6, 2023.

[5] 김학경, "미국의 온라인수색 제도에 관한 연구: 연방형사소송규칙 제41장 개정내용 중심으로", 시큐리티연구, 2022.

[6] American Civil Liberties Union, Challenging Government Hacking in Criminal Cases, pp. 38-42, 2017.

[7] UK Legislation, Investigatory Powers Act(I.P.A), 2023.

[8] 김학경, "영국 수사권한법에 규정된 온라인 수색 법제에 관한 소고", 형사법의 신동향,

2022.
[9] UK Government, Investigatory Powers Act – Codes of Practice(E.I.C.P), 2023.
[10] The MITRE Corporation. CVE(Buffer Overflow). https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0633, 2023.
[11] The MITRE Corporation. CVE(Memory Corruption). https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0634, 2023.
[12] MIT, Twisted server, http://twisted.org/. GitHub Repository : https://github.com/twisted/twisted, 2023.
[13] Jindrapetrik. JPEXS-decompiler. GitHub Repository :https://github.com/jindrapetrik/jpexs-decompiler/releases, 2023.
[14] The Haxe Foundation, Haxe tool kit, http://haxe.org, 2023.
[15] Sujoy Chakraborty, Mark Fowler, “Vector Quantizer with Fuzzy Equivalence Relations clustering”, IEEE International Symposium on Signal Processing and Information Technology(ISSPIT), 2020.
[16] Python. difflib. https://docs.python.org/3/library/difflib.html/. GitHub Repository : https://github.com/python/cpython/blob/3.11/Lib/difflib.py, 2023.
[17] Nguyen Hong Ngoc, Alvin Chan, Huynh Thi Thanh Binh, Yew Soon Ong. “Anti-Forensic Deepfake Personas and How To Spot Them”, IEEE International Joint Conference on Neural Networks(IJCNN), 2022.
[18] L. Ahmad, S. Khanji, F. Iqbal, and F. Kamoun, “Blockchain-based chain of custody: Towards real-time tamper-proof evidence management”,. 15th Int. Conf. Availability, Rel. Secur, 2020.
[19] Lokinet. https://lokinet.org, 2023.
[20] 김하영, “익명통신 범죄 온라인수색 도입방안”, 성균관대학교 과학수사학과 석사논문, 2022.

〔저자소개〕

한 채 림 (Chae-Rim Han)
2020년 03월 ~ 현재 성신여자대학교 학사과정

email : 20200969@sungshin.ac.kr

김 학 경 (Hak-kyong Kim)
1999년 3월 경찰대학 법학과 법학사
2004년 7월 영국 University of Leicester 경찰학(위기관리) 석사
2011년 5월 영국 University of Portsmouth 경찰학(위기관리) 박사
2012년 3월 계명대학교 경찰행정학과 교수
2015년 4월 ~ 현재 성신여자대학교 융합보안공학과 교수

email : pocol@sungshin.ac.kr