정 보 보 호 학 회 지
제 32 권 제6호, 2022. 12

안티포렌식 기술 동향 및 디지털 포렌식 대응 방안

김 지 언*, 정 병 찬*, 윤 우 성*, 박 정 흠**, 이 상 진***

요 약

디지털 포렌식 기술이 발달하면서 그에 대항하는 안티포렌식 기술 역시 고도화되고 있다. 보안 메신저 사용, 클라우드 환경의 발달, 익명 네트워크의 등장은 안티포렌식 기술의 일종으로, 디지털 포렌식 조사 시 시간과 비용을 증가시키며, 데이터 수집 및 분석 과정에서도 어려움을 겪게 한다. 본 논문에서는 최신 안티포렌식 기술과 이에 대응하기 위한 디지털 포렌식 기술의 현황을 소개한다. 특히, 최근에 디지털 포렌식 활동을 어렵게 하는 대표적인 요소인 '보안 메신저 서비스', '클라우드 스토리지 서비스', 그리고 '익명 네트워크 기반 서비스'를 위주로 기술한다.

Ⅰ. 서 론

컴퓨터 기술의 발전으로 로컬 디바이스에 저장하는 데이터의 양이 점점 줄고, 익명성과 보안성 강화로 사용자 추적이 어려워졌다. 이에 따라 기술을 악용한 관련 범죄가 증가하였다. 과거에는 로컬 디바이스에 저장된 데이터를 삭제, 은닉, 또는 조작하는 방식으로 안티포렌식 행위가 이루어져왔다[1]. 한편, 최근에는 안티포렌식 기술이 점점 발전한 형태로 로컬 디바이스에 데이터를 거의 저장하지 않거나 또는 저장하더라도 암호화되어 있는 경우가 많아졌다. 이러한 안티포렌식 기술은 디지털 포렌식 조사 시 분석 시간이 증가하고 데이터 수집에 어려움을 야기시킨다[2].

2020년 영국에서는 보안 메신저 앱을 통해 마약 거래, 자금 강탈 및 세탁 등의 범죄 사건이 발생한 바 있다. 사용자가 데이터를 원격으로 삭제할 수 있는 '킬 코드' 기능을 지원하는 앱으로, 영국 국가범죄청(NCA)는 앱을 해킹하는데 성공하였다[3].

로컬 저장소에서 클라우드 저장소로 저장 공간이 옮겨감에 따라 클라우드 스토리지 서비스를 이용한 범죄도 증가하였다. 12개월 간 클라우드 사용 기업의 40%가 클라우드 기반 데이터 침해를 경험한 바 있다[4]. 또한, MEGA, Google Drive와 같은 클라우드 서비스를 통해서 불법 영상을 공유하고 유포한 사건이 있다. 클라우드 링크에 접속하여 파일을 다운로드한 뒤 거래가 종료되는 방식으로 진행되며, 구매자는 판매자에게 가상화폐로 대가를 지불한다[5].

국내에서는 익명 네트워크를 이용하여 접속할 수 있는 다크웹에서 마약 유통이 지속적으로 증가하고 있으며, 대부분 익명 네트워크를 통해 유통이 이루어지는 것으로 파악된다. 익명 네트워크를 통해 다크웹에 접속하고, 보안 메신저를 이용하여 전달하는 일정을 방법을 결정하는 방식으로 마약 유통이 이루어진다[6]. 또한, 익명 네트워크를 통한 개인정보 데이터의 대규모 유출 사건도 지속적으로 발생한다[7].

다양한 서비스에서 프라이버시를 보호한다는 이유로 보안을 강화하고 있다. 사용자가 의도하든 아니든 안티포렌식 기술이 적용되고 있으며, 이는 디지털 포렌식 수사를 어렵게 한다. 따라서 이러한 안티포렌식 기술에 대응하기 위한 디지털 포렌식 조사와 분석 방법에 대한 연구가 필요하다.

본 고의 구성은 다음과 같다. 2절에서는 안티포렌식과 관련한 배경지식을 소개한다. 3절에서는 안티포렌식 기술에 대응하는 상용도구의 수집 및 분석 현황에 대해 기술한다. 4절에서는 이러한 기술에 대응하는 분석 연구 동향에 대해 살펴본다. 이를 바탕으로 5절에서는 안티포렌식 기술 대응을 위한 향후 연구개발 방향을 제시하며 결론으로 마무리한다.

이 논문은 과학기술정보통신부·경찰청이 공동 지원한 '폴리스랩2.0 사업(www.kipot.or.kr)'의 지원을 받아 수행된 연구결과입니다.
[과제명: 안티-포렌식 기술 대응을 위한 데이터 획득 및 분석 기술 연구 / 과제번호: 210121M07]
* 고려대학교 정보보호대학원 정보보호학과 (박사수료, kijie@korea.ac.kr, naaya@korea.ac.kr, yunws@korea.ac.kr)
** 고려대학교 정보보호대학원 정보보호학과 (조교수, jungheumpark@korea.ac.kr)
*** 고려대학교 정보보호대학원 정보보호학과 (정교수, sangjin@korea.ac.kr)

Ⅱ. 배경지식

2.1. 보안 메신저

보안 메신저는 현대 사회에서 매우 중요한 커뮤니케이션 수단으로 활용되고 있다. 일반적인 대화를 나누는 기능뿐만 아니라 파일 송·수신, 커뮤니티(오픈 채팅 - 카카오톡, 텔레그램 - 채널 등), 뉴스, 금융, 쇼핑, 방송 등 개인 생활과 밀접한 기능들을 제공하고 있다.

보안 메신저는 개인의 생활과 밀접한 기능들을 제공하고 있어 각종 사건·사건 사고 발생 시 중요한 단서로 사용되고 있으며 보안 메신저 내 데이터를 수집·분석하는 것은 선택이 아니라 필수가 되고 있다.

최근 국내·외 메신저 감청 사건을 이유로 많은 사용자가 개인 정보 보호를 강화한 메신저들을 많이 찾고 있으며 각 메신저 서비스 자체적으로도 보안을 강화하고 있다. 이렇게 강화된 보안 기능은 개인의 정보를 보호하는 순작용도 하게 되지만 강화된 보안 기능으로 인해 메신저 서비스 내 데이터를 획득하기가 어려워져 각종 범죄의 온상이 되고 있다[8].

또한, 한 사람이 하나의 디바이스를 사용하며 디바이스 중심의 데이터 저장이 일반적이었지만 최근에는 일과 삶의 균형(Work-Life Balance), COVID19 등 원격 근무 환경으로의 변화가 가속화되어 한 사람이 여러 개의 디바이스를 사용하는 경우가 많아지면서 계정 중심의 클라우드를 기반 데이터 저장으로 전환되고 있다. 이에 맞춰 디지털 포렌식 분야에서도 디바이스 중심으로 로컬 디바이스에 남아있는 데이터를 중점으로 수집하는 연구뿐만 아니라[9], 하나의 계정으로 클라우드에 동기화되는 데이터를 수집하는 연구도 많이 수행되고 있다.

2.2. 클라우드 스토리지

클라우드 스토리지 서비스는 사용자들이 클라우드 서버에 파일을 저장하고 언제든지 데이터에 접근하고 공유할 수 있게 도와준다. 과거에 비해 클라우드 서비스에서 제공하는 기능이 다양해졌으며, 실시간으로 다른 사용자와 공유할 수 있다.

범죄자들은 해외에 서버를 두고 있는 클라우드 스토리지 서비스들을 이용하여 위법 데이터를 유통할 때 사용하기도 한다. MEGA와 같은 클라우드 스토리지 서비스는 계정이 없이도 다운로드 링크를 공유할 수 있다. 그런데 클라우드 서버에 저장된 데이터는 여러 디바이스와 사용자가 연결되어 있을 수 있어 언제든지 데이터가 생성, 수정, 삭제될 수 있다[10].

데이터가 원격지 서버에 저장됨에 따라 디지털 포렌식 조사 시 국가 공조, 재판관할권, 서비스 제공업체의 협조 등으로 인해 데이터 수집에 어려움이 생겨났다[11]. 수집할 수 있는 클라우드 기반 자원의 종류와 양도 증가하였다. 이에 대응하여 디지털 포렌식 조사 체계에 맞게 원격지 데이터를 수집하는 것이 중요하다. 또한, 모든 클라우드 데이터를 다운로드 받아 분석하는 것보다 데이터 선별을 통해 수집하고 분석하는 것이 효과적일 것이다.

2.3. 익명 네트워크

인터넷을 통해 일반적으로 접속할 수 있는 웹 페이지에 접속하는 경우, 이는 익명성을 보장하지 않는다. 인터넷 사용자들이 포털 사이트를 통해 검색하거나, 커뮤니티에 접속하여 글을 읽는다거나, 쇼핑몰에서 물건을 구입할 때, 이용하는 웹 사이트에 트래커가 달려있다면, 트래커에 의해 사용자의 행위가 수집될 수 있다. 트래커는 사용자가 어떤 행위를 했는지 수집하고 맞춤형 광고를 제공하거나 해당 데이터를 재가공하여 판매할 수도 있다.

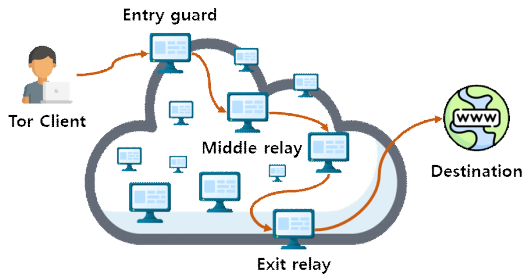
〔표 1〕 익명 네트워크 종류 및 특징

종류	분석 지원 아티팩트
Tor	- 어니언 라우팅(Onion routing)을 사용하여 트래픽을 캡슐화 - 입구/중간/출구 노드의 과정을 거쳐서 통신하고 각 통신 과정이 암호화 되어 추적 불가
Lokinet	- 블록체인 기반으로 구축되어 분산 해시 테이블(DHT) 사용 - 각 서비스 노드가 네트워크에서 라우터 역할 수행
Freenet	- 비계층 노드로 공유되는 비정형 p2p 네트워크로 설계 - Tor와 유사하게 입구/중간/출구 노드 사이를 왕래
I2P	- 서로에게 가명으로 안전하게 메시지를 보내는 다크넷 방식 - I2P 라우터라고 불리는 레이어를 실행하여 Tor와 다르게 여러 개의 패킷 혹은 메시지 전송 가능
GNUnet	- Mesh Network 기반으로 구축되어 분산 해시 테이블(DHT)를 사용 - DNS를 대신해 GNS라는 독자적 체계 사용

학교, 정부, 인터넷 서비스 공급자 등 네트워크 관리자는 HTTPS 연결로 인해 사용자가 정확히 어떤 행위를 하는지는 알 수 없지만, 어느 웹 사이트에 접근하는지는 알 수 있다.

익명 네트워크는 인터넷을 사용할 때 웹 사이트들의 트래킹을 피하고 네트워크 관리자로부터 익명성을 보장하기 위해 사용된다. 익명 네트워크에는 Tor, Lokinet, I2P, Freenet, GNUnet 등 여러 종류가 각기 다른 방식으로 익명성을 확보하고 있지만, 현재 사용자 수가 가장 많은 익명 네트워크는 Tor이다[12].

Tor 네트워크는 여러 노드를 거치면서 겹겹이 암호화하여 통신하는 어니언 라우팅(Onion routing)을 사용하여 트래픽을 캡슐화한다. Tor 네트워크를 통해 웹 페이지에 접속하면 한 번에 해당 웹 페이지로 통신하지 않고, 입구 노드, 중간 노드, 출구 노드를 거쳐서 통신한다[13]. 여러 노드를 거쳐서 통신하게 되는 과정에서 각 과정이 암호화되어 있어 역추적하는 것이 이론적으로 불가능하다. [그림 1]은 Tor 네트워크의 동작 방식을 나타낸다.



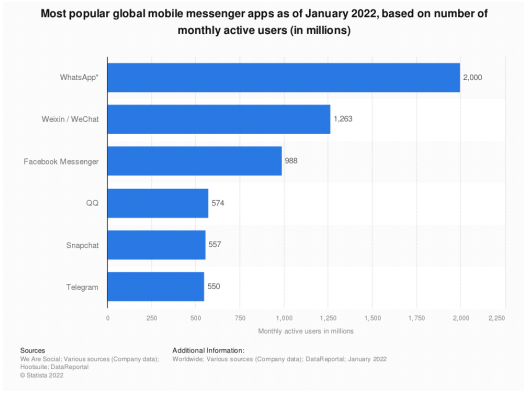
〔그림 1〕 Tor 네트워크 동작 방식

Ⅲ. 안티포렌식 대응 기술 현황

본 절에서는 보안 메신저, 클라우드 스토리지, 익명 네트워크로 각각 나누어 안티포렌식 기술에 대응하는 디지털 포렌식 도구들의 수집 현황을 기술한다. 또한, 상용도구들의 특징과 장단점을 비교하고 분석하여 설명한다.

3.1. 보안 메신저 서비스 현황

보안 메신저는 범죄 사건·사고에서 핵심적인 단서로 사용될 수 있어서 많은 상용도구가 이를 지원하고 있다. [그림 2]는 세계에서 가장 많이 사용되고 있는 메신저 순위[14]를 나타낸다.



〔그림 2〕 세계 모바일 메신저 점유율(2022.01)

보안 메신저에 대한 상용도구 지원 현황은 [표 2]와 같다. 여러 상용도구에서 많은 보안 메신저에 대한 수집·분석을 지원하고 있지만, 메신저 서비스는 빠른 업데이트 주기, 신규 서비스의 등장 등의 영향으로 즉각적인 대응이 어려운 상황이 발생하기도 한다.

〔표 2〕 모바일 메신저 수집 지원 현황

구분	AXIOM (v5.3.0)		Oxygen Forensic Detectives (v13)		MD-RED (v3.7.40)		Cellebrite Physical Analyzer (v7.48.1.3)	
	Android	iOS	Android	iOS	Android	iOS	Android	iOS
WhatsApp	○	○	○	○	○	○	○	○
WeChat	○	○	○	△	○	○	-	○
Telegram	△	○	○	○	○	○	○	○
Kakaotalk	○	○	△	○	○	○	○	○
LINE	○	○	○	○	○	○	○	○

△: 일부 아티팩트(계정, 첨부파일, 대화 내역)는 지원하지 않음

3.2. 클라우드 스토리지 서비스 현황

[표 3]은 클라우드 스토리지에 대한 서비스별 수집 관련 지원 현황을 나타낸 표이다. 여러 상용도구에서 다양한 종류의 클라우드 스토리지 서비스에 대한 메타

〔표 3〕 클라우드 스토리지 서비스별 점유율과 수집 지원 현황

클라우드 서비스명	Oxygen 지원 여부	AXIOM 지원 여부	Cellebrite 지원 여부
Google Drive	O	O	O
Dropbox	O	O	O
OneDrive	O	O	O
MEGA	O	O	O
Box	O	O	O

데이터 및 파일 수집을 지원하고 있지만, 도구마다 수집하는 메타데이터와 데이터가 다르다.

[표 4]에서 볼 수 있듯이 Google Drive로 대상으로 하였을 때, 서비스마다 수집 가능한 범위가 조금씩 다른 것을 알 수 있다. 분석 대상 클라우드 서비스와 상용도구에 따라 수집되는 데이터 범위가 다르고, 메타데이터 표현 방법에도 조금씩 차이가 있다. 이처럼 현재 원격지 데이터 수집 시 완전하게 데이터를 수집하는데는 한계가 있으며, 도구마다 서로 다른 결과를 도출하기도 한다.

〔표 4〕 Google Drive에 대한 상용 도구 수집 현황

구분 (버전)	Oxygen (4.0.0.1367)	AXIOM (5.10.0.30634)	Cellebrite (7.49.0.28)
API 방법	Internal API	Open API	Internal API
내 파일 (파일/폴더)	O/X	O/O	O/O
공유 파일	X	X	X
이메일 공유	X	O	O
링크 공유	X	O	O
휴지통 파일	O	X	O
휴지통에서 삭제 파일	X	X	X
기타	폴더 정보 표시하지 않음	휴지통 파일 표시하지 않음	휴지통 파일 표시하지 않음

3.3. 익명 네트워크 서비스 현황

익명 네트워크 분석을 지원하는 상용도구는 많지 않다. [표 5]는 익명 네트워크 분석을 지원하는 상용도구를 정리한 표이다. MAGNET AXIOM은 Tor Chat과 Tor URLs 분석을 지원한다. Tor URLs는 시스템 파일이나 미할당 영역에서 다크웹 주소(.onion)를 식별하여 분석하는 방식이다.

〔표 5〕 익명 네트워크 분석을 지원하는 상용도구

종류	상용도구	분석 지원 아티팩트
Tor	MAGNET AXIOM	- Tor Chat: Local Date/Time, Sender, Receiver, Message - Tor URLs: URL, Site Name, Date/Time-UTC, Date/Time-Local
	Elcomsoft	- Tor Browser Password Breaker

Ⅳ. 안티포렌식 대응 기술 연구 동향

본 절에서는 안티포렌식 기술 대응을 위한 최신 동향에 대해 살펴본다.

4.1. 보안 메신저에 대한 연구

최근 보안 메신저에 대한 연구는 데이터 저장 위치에 따라 두 가지로 나누어지고 있다. 클라이언트 디바이스에 데이터를 저장하는 메신저에 대한 연구와 계정 기반으로 클라우드 내에 데이터를 저장하는 메신저에 대한 연구로 나누어진다.

클라이언트 디바이스 내에 데이터를 저장하는 메신저는 주로 저장된 데이터에 대한 암호화·복호화, 직렬화·역직렬화, 삭제된 메시지에 대한 복구 등과 같이 클라이언트 디바이스에 저장된 데이터의 수집·분석 방법에 대한 연구가 주로 이루어지고 있다.

J. Choi 외 3명[15]은 Windows OS에서 동작하는 국내 메신저인 카카오톡, 네이트온과 해외 메신저인 QQ 메신저에 대하여 연구를 수행하였다. 소스코드 정적 분석을 통해 사용자 데이터를 저장하고 있는 데이터베이스를 복호화하는 방법론을 제시하였다.

G. Kim 외 5명[16]은 Android와 iOS에 설치된 Wicker와 Private Text Messaging 두 메신저 저장되는 정적·동적 분석을 통해 암호화된 데이터베이스를 복호화하는 알고리즘 파악하고 이를 통해 사용자 데이터를 수집하는 방법론을 제안하였다.

이처럼 많은 보안 메신저에 관한 연구는 조사 대상

디바이스에 남아있는 아티팩트를 수집·분석하는데 치우쳐 있다. 하지만, 최근에는 원격 근무 환경으로의 전환됨으로 인해 한 명의 사용자가 하나의 디바이스만 사용하지 않고 여러 디바이스를 사용하고 있다. 따라서, 많은 메신저 서비스들은 하나의 계정으로 여러 디바이스에 데이터가 동기화되는 방식으로 서비스를 제공하고 있으며, 사용자 크리덴셜 정보를 획득할 수 있으면 별도의 조사가 가능한 디바이스에서 사용자 데이터를 수집할 수 있다. 신수민 외 3명[17]은 Windows OS의 Wire 메신저에 대한 사용자 크리덴셜 정보 획득과 사용자 아티팩트에 대한 연구를 수행하였다. 사용자 크리덴셜 정보를 획득하여 다른 PC에 로그인할 수 있음을 확인하였지만 이를 통한 데이터 획득에 관한 내용은 다루지 않았다. 남기훈 외 3명[18]은 Android OS에서 OAuth 프로토콜을 이용한 클라우드 서버 내에 저장된 메신저 데이터를 수집하는 방법에 대한 연구를 수행하였다.

최근 많은 보안 메신저들이 클라이언트 디바이스에는 데이터를 남기지 않는 정책을 사용하고 있다. 따라서, 사용자 크리덴셜을 이용하여 클라우드 서버에 저장된 데이터 획득 방법에 대한 연구가 활발히 진행되고 있다.

4.2. 클라우드 스토리지에 대한 연구

클라우드 스토리지 서비스를 대상으로 한 연구는 활발히 진행되어 왔다. 수집 및 분석 방법은 크게 세 가지로 나뉘며, Open API를 활용한 데이터 수집, Internal API를 활용한 데이터 수집, 로컬 아티팩트 수집이 있다.

R. Vassil 외 2명[19]은 API를 활용한 클라우드 데이터 수집의 필요성을 강조하면서 클라우드 서버에 저장된 데이터를 획득하는 도구(kumodd)를 개발하였다. Google Drive, Microsoft OneDrive, Dropbox, Box를 대상으로 도구를 개발하였으며 서버에 저장된 파일, 이전 버전 등의 데이터를 수집할 수 있다.

한중수 외 5명[20]은 클라우드 스토리지에 저장된 파일들을 선별 수집하는 방법에 대한 연구를 수행하였다. OAuth 2.0 인증을 통해 서버로부터 사용자임을 확인 받고, Open API를 활용하여 데이터를 수집한 다음, 획득한 데이터를 기반으로 파일을 선별하여 수집하는 방안을 제시하였다.

J. Yang 과 J. Kim 외 2명[21]은 Open API 와 Internal API를 활용하여 클라우드 서버에 저장된 자원을 완전하게 수집할 수 있는 조사 체계를 제안하였다. 제안한 조사 체계를 바탕으로 도구를 개발하고, Microsoft OneDrive에 대해서 케이스 스터디를 진행하였다. 기존 상용도구와 비교하였을 때 제안한 조사 체계가 완전한 클라우드 자원 수집에 효과적임을 확인하였다.

Martini 외 1명[22]은 오픈 소스 기반 ownCloud를 대상으로 몇 가지 실험을 통해 클라이언트 중심 아티팩트와 서버 아티팩트가 어떻게 남는지 조사하였다. 대상 서비스를 사용함에 따라 동기화한 파일에 대한 정보, 캐시 파일, 서비스 관련 인증 정보, 브라우저 아티팩트 등 다양한 종류의 아티팩트가 남는 것을 확인하였다.

4.3. 익명 네트워크에 대한 연구

현재까지 익명 네트워크에 대한 연구는 사용자 수가 가장 많은 Tor 네트워크에 집중되어 있다. Tor 네트워크는 특정 브라우저(Tor, Brave)를 통해서만 사용할 수 있는데, 이러한 소프트웨어가 로컬 시스템에 남기는 흔적과 메모리에 올라가는 데이터를 분석하는 연구가 진행되어왔다.

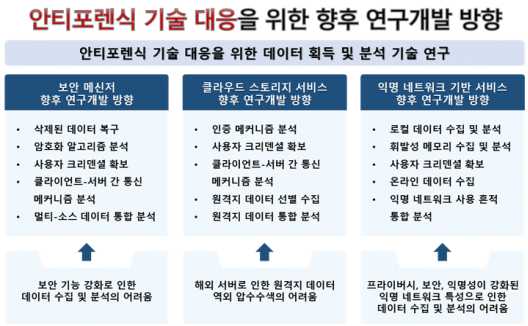
Tor 네트워크는 익명성을 보장하는 특성상 로컬 시스템에 웹 사이트 접속 기록이나 다운로드한 파일 목록 등 사용 이력에 대한 흔적을 거의 남기지 않는다. 하지만 Tor 네트워크를 통해 다크웹에 접속할 때. 메모리에서는 유의미한 사용 흔적을 찾을 수 있다.

A. Malak 외 1명[23]은 Tor 네트워크 사용 시 메모리에 어떤 아티팩트가 남고 로컬 시스템에 남아있는 실행 이력과 흔적을 통해 Tor 네트워크 분석 절차 서술하였고, M. Muir 외 3명[24]은 Tor 브라우저를 사용한 PC에 대해 디지털 포렌식 분석을 서술하였다.

M. J. C. Huang 외 3명[25]은 메모리를 통해 Tor 브라우저 사용 흔적을 찾고 다른 브라우저와 비교하여 서술하였고, M. R. Arshad 외 5명[26]은 윈도우 10과 안드로이드 10버전에 대한 Tor 브라우저 포렌식 분석 방법을 서술하였다.

Ⅴ. 향후 연구개발 방향

본 절에서는 [그림 3]과 같이 안티포렌식 기술 대응을 위한 향후 연구 방향에 대해 논의한다.



〔그림 3〕 안티포렌식 기술 대응을 위한 향후 연구개발 방향

5.1. 보안 메신저 향후 연구개발 방향

5.1.1. 삭제된 데이터 복구

많은 보안 메신저 서비스는 SQLite, LevelDB 등과 같은 데이터베이스를 이용하여 사용자 데이터를 저장하고 있다. 삭제된 데이터에 대한 복구를 위해서는 각 메신저가 데이터를 관리하는 메커니즘을 분석해야 한다. 정적·동적 분석을 통하여 데이터를 삭제하는 원리를 파악하고 삭제된 데이터에 대한 복구를 시도해야 한다.

5.1.2. 암호화 알고리즘 분석

보안 메신저 서비스는 자체적으로 사용자 데이터를 암호화하여 저장한다. 사용자 데이터가 저장된 데이터베이스 파일 자체에도 암호화 기법을 적용할 뿐만 아니라 데이터베이스의 레코드 단위에도 암호화 기법을 적용하고 있다. 암호화된 사용자 데이터를 복호화하기 위해서는 역공학을 통해 암호 알고리즘을 파악하고 이를 통해 사용자 데이터를 복호화할 수 있다.

5.1.3. 사용자 크리덴셜 확보

최근 클라이언트 디바이스에는 데이터를 남기지 않는 보안 메신저들이 많이 출시되고 있다. 디지털 포렌식 조사 과정 중 사용자 데이터를 확보하기 위해서는 사용자 크리덴셜 정보를 이용하여 클라우드 서버 내 저장된 데이터를 가져오는 것은 필수적이다.

따라서, 자동 로그인 기능, 로그인 상태 유지를 위한 세션 정보 등과 같은 사용자 크리덴셜을 확보하여 사용자 데이터에 접근·수집해야 한다.

5.1.4. 클라이언트-서버 간 통신 메커니즘 분석

보안 메신저 서비스는 클라이언트와 서버 간의 통신을 통하여 사용자들 간의 대화를 주고받는다. 다수의 보안 메신저는 디바이스 간 동기화를 위해 클라우드 서버 내에 데이터를 저장하고 있다. 이때 클라이언트에서는 클라우드 서버에 데이터를 요청한다. 데이터를 요청하는 방법으로 서비스 자체적으로 개발한 SDK(Software Development Kit)를 제공하기도 하지만 서비스에서 내부적으로 구현한 방식으로 동작하기도 한다. 따라서, 클라우드 서버 내에 존재하는 사용자 데이터를 가지고 오기 위해서 보안 메신저 서비스에서 제공하는 통신 메커니즘을 분석해야 한다.

5.1.5. 멀티-소스 데이터 통합 분석

원격 근무 환경이 발달하면서 한 명의 사용자가 하나 이상의 디바이스와 보안 메신저 서비스를 사용하고 있다. 또한, 보안 메신저 서비스는 사용자의 사생활과 밀접한 데이터가 저장되어 있어 각종 사건·사고를 해결할 수 있는 중요한 키 역할을 한다. 따라서, 한 명의 사용자를 조사하기 위해서는 다양한 소스에서 분산되어 저장되는 사용자 데이터를 통합하여 분석하는 것이 필요하다.

5.2. 클라우드 스토리지 향후 연구개발 방향

5.2.1. 인증 메커니즘 분석

클라우드 자원에 접근하기 위해서는 클라우드 서버로부터 사용자 인증이 필수적이다. 일반적으로 Open API의 경우, OAuth 2.0 인증 방법을 통해 서버로부터 토큰을 교환받는 방식으로 사용자를 인증받을 수 있다. Internal API의 경우, Selenium 또는 Playwright과 같은 웹 브라우저 자동화 프레임워크를 활용할 수 있으며, 사용자의 아이디와 비밀번호를 자동으로 입력하여 사용자 인증을 받을 수 있다. 클라우드 스토리지 서비스는 API(Open API, Internal API)의 종류와 대상 서비스에 따라 사용자임을 인증받는 방법이 달라지기 때문에 인증 메커니즘을 분석할 필요가 있다.

5.2.2. 로그인 크리덴셜 확보

클라우드 서버에 사용자 데이터를 요청하기 위해서는 쿠키나 토큰 등과 같은 로그인 크리덴셜 확보가 필수적이다. 앞서 인증 메커니즘 분석에 이어 인증에 필요한 로그인 크리덴셜을 확보하여야 한다. API와 대상 서비스에 따라 필요한 로그인 크리덴셜이 다르기 때문에 로그인 크리덴셜에 대한 분석이 요구된다.

5.2.3. 클라이언트-서버 통신 메커니즘 분석

클라이언트에서 클라우드 서버에 데이터를 요청할 때 데이터를 주고받는 방식은 클라우드 스토리지 서비스와 API별로 다르다. Open API가 존재하는 경우, 서비스 제공업체에서 공개하기 때문에 비교적 쉽게 분석할 수 있다. Internal API의 경우, 클라이언트가 클라우드 서버에 어떻게 요청하여 어떤 응답을 받는지 분석하여야 한다. 응답받는 형식은 GZIP, JSON 등의 포맷이 대표적이며, 클라우드 스토리지 서비스들은 각기 다른 통신 메커니즘을 가지고 있으므로 다양한 서비스에 대한 분석을 통해 향후 연구를 진행하여야 한다.

5.2.4. 원격지 데이터 선별 수집

클라우드 스토리지에는 방대한 양의 사용자 데이터가 저장되어 있다. 나날이 그 양이 증가하고 있기 때문에 디지털 포렌식 조사 시 모든 데이터를 다운로드 받는 것은 비효율적이다. 따라서, API를 호출하여 획득한 메타데이터 기반으로 파일을 선별하거나, 검색 API를 호출하여 파일을 선별하는 등의 방법을 통해 원격지 데이터를 선별하여 수집하는 방안이 필요하다.

5.2.5. 원격지 데이터 통합 분석

클라우드 스토리지 서비스는 다양한 종류의 메타데이터를 저장한다. 파일 소유자, 클라우드 서버에 생성된 날짜, 서버상에서 수정한 날짜 등의 메타데이터뿐만 아니라 OCR 텍스트, 파일의 이전 버전, 썸네일과 같은 메타데이터도 저장한다. 서비스에 따라 어떤 사용자와 파일을 공유했고, 공유한 파일을 누가 언제 수정했는지 기록하기도 한다. 따라서, 파일의 변경 이력을 추적하거나 사용자의 클라우드 서비스 사용 이력, 파일 간의 관계 등을 분석하기 위해 데이터를 통합하여 분석하는 것이 필요하다.

5.3. 익명 네트워크 향후 연구개발 방향

5.3.1. 로컬 데이터 수집 및 분석

익명 네트워크를 사용하기 위해서는 익명 네트워크를 활성화하기 위한 특정 소프트웨어(Tor, Lokinet, Brave 등)를 설치해야 한다. 로컬 시스템에 익명 네트워크 전용 소프트웨어를 설치하고 실행하면 해당 소프트웨어에 대한 버전 정보, 설치 정보, 실행 정보를 수집할 수 있다. 또한, 운영체제에서 일시적으로 메모리의 용량이 부족해지는 순간에 하드 디스크의 일정한 영역을 가상 메모리 공간으로 설정하는 경우, 휘발성 메모리 일부가 로컬 시스템에 파일 형태로 저장되기도 한다. 이 파일에는 익명 네트워크를 통해 다크웹에 접속할 때 사용하는 인터넷 프로토콜의 데이터나 다크웹 주소들이 남을 수 있다. 보안성과 익명성이 강화된 익명 네트워크의 특성상 로컬 시스템에 익명 네트워크에 대한 구체적이고 자세한 사용 흔적은 남아있지 않다. 하지만, 익명 네트워크 소프트웨어의 대략적인 정보를 파악할 수 있으므로 로컬 시스템의 데이터를 수집하고 분석해야 한다.

5.3.2. 휘발성 메모리 수집 및 분석

휘발성 메모리에 대한 수집 및 분석은 로컬 시스템 데이터보다 사용자의 행위를 특정하기 쉽고 로컬 시스템 데이터에서 수집할 수 없던 사용자 인증 정보 또는 방문 기록을 획득할 수 있다. 로컬 환경에 저장되지 않는 익명 네트워크 서비스에 대한 아티팩트를 수집할 수 있으므로 휘발성 메모리의 수집 및 분석은 익명 네트워크를 분석하면서 필수적이다. 익명 네트워크를 사용하는 동안 물리 메모리에는 방문 기록, 사용자 인증 정보 등과 같은 정보가 저장된다. 하지만 휘발성 메모리의 특성상 익명 네트워크 프로세스를 사용 중일 때는 물리 메모리에서 많은 정보를 수집할 수 있으나, 익명 네트워크를 종료하여 프로세스가 사라진 후에는 시간이 지날수록 정보가 유실된다. 따라서, 메모리를 얼마나 신속하게 수집할 수 있는지가 중요하다.

5.3.3. 다크웹 로그인 크리덴셜 확보

다크웹 로그인 크리덴셜 확보는 익명 네트워크 내 사용자의 활동을 파악하는 데에 있어서 중요하다. 익명 네트워크를 통해 접속하는 다크웹에는 로그인이 필요 없는 게시글을 열람할 수 있는 블로그 형식도 있지만, 로그인하여 인증 절차를 거치면 불법 서비스를 이용할 수 있는 웹 페이지도 있다. 이러한 웹 페이지에 로그인하는 경우, 사용자가 쓴 글, 댓글 등 사용자의 다양한 익명 네트워크 내 활동을 파악할 수 있다. 다크웹 로그인 크리덴셜은 사용자 본인으로부터도 확보할 수 있지만, 물리 메모리에서도 확보할 수 있다. 웹 페이지에 로그인할 때, 물리 메모리에 특정 패턴을 남기게 되는데, 이를 통해서 사용자의 크리덴셜을 확보할 수 있다. 사용자의 아이디와 비밀번호를 동시에 획득할 수 있는 때도 있고, 아이디나 패스워드 둘 중 하나만 남는 때도 있다.

5.3.4. 온라인 데이터 수집

다크웹에 서비스되는 악의적인 콘텐츠의 특성상 기존에 운영되던 다크웹 서비스가 중단되거나, 새로운 형태로 다시 운영되는 경우가 빈번하며, 온라인상의 사용자 흔적은 언제든 변조되거나 없어질 가능성이 있다. 따라서, 수집한 로컬 데이터와 물리 메모리 데이터로부터 익명 네트워크를 통한 다크웹 접속 기록을 확보하였다면, 다크웹 상에 기록된 사용자 흔적을 수집해야 한다. 다크웹 페이지에 대한 온라인상의 데이터를 수집함으로써 다크웹 페이지가 운영 중단되거나, 사용자 본인의 글을 삭제 및 변조, 계정을 삭제하는 등의 안티포렌식 행위에 대응할 수 있다.

5.3.5. 익명 네트워크 사용 흔적 통합 분석

익명 네트워크 사용 흔적을 파악하기 위해서는 세 영역의 아티팩트를 통합하여 분석해야 한다. 먼저, 익명 네트워크의 설치 및 사용 기록은 로컬 아티팩트 분석을 통해 확인할 수 있으며, 사용자가 익명 네트워크를 통해 어떠한 행위를 하였는지는 물리 메모리에 남아있는 정보를 통해 알아낼 수 있다. 마지막으로, 익명 네트워크를 사용하며 온라인에 남긴 흔적은 온라인상의 데이터 수집을 통해 파악할 수 있다. 따라서, 익명 네트워크에 대한 사용 흔적을 파악하기 위해서는 로컬 저장소, 물리 메모리, 온라인 데이터, 세 영역을 통합하여 분석하여야 익명 네트워크 사용 흔적을 재구성할 수 있다.

Ⅵ. 결 론

본 논문에서는 안티포렌식 기술에 대한 개념을 설명하고, 보안 메신저, 클라우드 스토리지, 익명 네트워크 기술 현황을 분석하였다. 또한, 안티포렌식 기술에 대응하기 위하여 디지털 포렌식 관점의 아티팩트 수집 및 분석 연구 동향을 살펴보고, 데이터 수집 한계를 설명하였다.

익명성과 보안성이 강화되는 인터넷 기술의 발전에 따라 사용자 데이터를 수집하는 방안과 사용자 행위를 분석하는 방안에 관한 연구가 수행될 필요가 있다.

참 고 문 헌

[1] 이석희, 박보라, 이상진, 홍석희, “안티 포렌식 기술과 대응 방향”, *한국정보보호학회논문지*, 18(1), 2008.

[2] 윤지수, 이경렬, “안티 포렌식 신종기법에 대한 형사법적 대응방안”, *한국형사정책학회*, 32(4), 65-99, 2021.

[3] ZDNET Korea, “영국 경찰, 보안 메신저 해킹...범죄자 수백명 체포”, 2020.07.06., URL:https://zdnet.co.kr/view/?no=20200706162004, Accessed: 2022.11.26.

[4] 아이티데일리, “[이슈조명] 해킹으로 이틀 만에 1억 원 피해...클라우드 보안 대책은?”, 2022.05.02., URL: http://www.itdaily.kr/news/articleView.html?idxno=207832, Accessed: 2022.11.27.

[5] 국민일보, “[n번방 1년, 남은 질문들②] 초고속 n차 유포 불붙이는 ‘클라우드’, 2021.05.11., URL:http://news.kmib.co.kr/article/view.asp?arcid=0015830882&code=61121111&sid1=soc&stg=vw_rel, Accessed: 2022.11.27.

[6] 서울신문, “마수 뻗는 다크웹… 마약 빠진 2030”, 2022.07.26.,URL: https://www.seoul.co.kr/news/newsView.php?id=20220727006027, Accessed: 2022.11.27.

[7] cctv뉴스, “다크웹에 중국인 10억 명 개인정보 유출”, 2022.07.05.,URL: https://www.cctvnews.co.kr/news/articleView.html?idxno=232857, Accessed: 2022.11.27.

[8] 보안뉴스, “조주빈의 박사방, 갓갓의 n번방... 텔레그램, 디지털 성범죄 ‘온상지’된 이유는”, 2020.03.25., URL: http://m.boannews.com/html/detail.html?idx=87177, Accessed: 2022.11.30.

[9] K. Rathi, U. Karabiyik, T. Aderibigbe, H. Chi, “Forensic analysis of encrypted instant messaging applications on Android,” 2*018 6th International Symposium on Digital Forensic and Security (ISDFS)*, 1-6, 2018.

[10] 정현지, 이상진, “클라우드 컴퓨팅 환경에서의 디지털 포렌식 동향 및 전망”, *정보보호학회지*, 22(7), 7-13, 2012.

[11] 이규민, 이영숙, “클라우드 환경에 적합한 디지털 포렌식 수사 모델”, *융합보안논문지*, 17(3), 15-20, 2017.

[12] Welcome to Tor Metrics, “Tor Metrics: Users Stats”, URL: https://metrics.torproject.org/user-stats-relay-country.html, Accessed: 2022.11.30.

[13] R. Dingledine, N. Mathewson, P. Syverson, “Tor: The second-generation onion router.”, *Naval Research Lab Washington DC*. 2004

[14] Statista. Most popular global mobile messaging apps 2022. https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/. 2022.

[15] J. Choi, J. Yu, S. Hyun, H. Kim, “Digital forensic analysis of encrypted database files in instant messaging applications on Windows operating systems: Case study with KakaoTalk, NateOn and QQ messenger,” *Digital Investigation*, 28, S50-S59, 2019.

[16] G. Kim, S. Kim, M. Park, Y. Park, I. Lee, J. Kim, “Forensic analysis of instant messaging apps: Decrypting Wickr and private text messaging data,” *Forensic Science International: Digital Investigation*, 37, 301138. 2021.

[17] 신수민, 김소람, 윤병철, 김종성. Windows 에서의 Wire 크리덴셜 획득 및 아티팩트 분석. *정보보호학회논문지*, 31(1), 61-71. 2021.

[18] 남기훈, 공성현, 석병진, 이창훈. 안드로이드 환경의 OAuth 프로토콜을 이용한 원격지 데이터 수집 방법 연구. *정보보호학회논문지*, 28(1), 111-122. 2018.

[19] R. Vassil, B. A. Felipe, I. Ahmed, “Forensic Acquisition of Cloud Drives,” *Cryptography and Security*, Jan 2016.

[20] 한중수, 이승용, 오정훈, 김준수, 정혜진, 황현욱, “클라우드 스토리지 서비스에 대한 메타데이터 기반 파일선별 수집 방법 및 구현”, *디지털포렌식연구*, 14(3), 305-315, 2020.

[21] J. Yang, J. Kim, J. Bang, S. Lee, J. Park, “CATCH: Cloud Data Acquisition through Comprehensive and Hybrid Approaches,” *Forensic Science International: Digital Investigation*, 43, Sep 2022.

[22] B. Martini, K. R. Choo, “Cloud storage forensics: ownCloud as a case study,” *Digital Investigation*, 10(4), 287-299, Dec 2013.

[23] M.Alfosail, P. Norris, “Tor forensics: Proposed workflow for client memory artefacts” *Computers & Security*, 106, 102311, 2021.

[24] M. Muir, P. Leimich, W. J. Buchanan, “A forensic audit of the tor browser bundle” *Forensic Science International: Digital Investigation*, 29, 118-128. 2019.

[25] M. J. C. Huang, Y. L. Wan, C. P. Chiang, S. J. Wang, “Tor browser forensics in exploring invisible evidence,” *2018 IEEE International Conference on Systems*, Man, and Cybernetics (SMC), pp. 3909-3914, Oct 2018.

[26] M. R. Arshad, M. Hussain, H. Tahir, S. Qadir, F. I. A. Memon, Y. Javed, “Forensic analysis of tor browser on windows 10 and android 10 operating systems,” *IEEE Access*, 9, 141273-141294. 2021

〈저자소개〉

김 지 언 (Jieon Kim)
2018년 8월 : University of Pennsylvania Criminology 석사
2021년 2월~현재 : 고려대학교 정보보호대학원 박사수료
<관심분야> 클라우드포렌식, IoT포렌식, 데이터 분석

정 병 찬 (Byeongchan Jeong)
2019년 2월 : 고려대학교 정보보호대학원 공학석사
2021년 2월~현재 : 고려대학교 정보보호대학원 박사수료
<관심분야> 디지털포렌식, 모바일포렌식, 침해사고

윤 우 성 (Woosung Yun)
2020년 2월 : 고려대학교 정보보호대학원 공학석사
2022년 2월~현재 : 고려대학교 정보보호대학원 박사수료
<관심분야> 디지털포렌식, IoT포렌식, 안티포렌식

박 정 흠 (Jungheum Park)
2014년 2월 : 고려대학교 정보보호대학원 공학박사
2015년 1월~2019년 2월 : 미국 국립표준기술연구원(NIST) 방문연구원
2021년 9월~현재 : 고려대학교 정보보호대학원 조교수
<관심 분야> 디지털포렌식, 사이버범죄대응

이 상 진 (Sangjin Lee)
종신회원
1989년 10월~1999년 2월 : ETRI 선임 연구원
1999년 3월~2001년 8월 : 고려대학교 자연과학대학 조교수
2001년 9월~현재 : 고려대학교 정보보호대학원 교수
2008년 3월~현재 : 고려대학교 디지털포렌식연구센터
<관심분야> 디지털포렌식, 심층암호, 해시암호