JDCS
디지털콘텐츠학회논문지
Journal of Digital Contents Society
Vol. 21, No. 4, pp. 781-791, Apr. 2020

Check for updates

메모리 포렌식 관점에서의 모바일 브라우저 사생활 보호 모드 분석

박 진 성[1] · 서 승 희[2] · 이 창 훈[3*]
[1]서울과학기술대학교 컴퓨터공학과 석사과정
[2]서울과학기술대학교 컴퓨터공학과 박사과정
[3]서울과학기술대학교 컴퓨터공학과 교수

Analysis of mobile browser privacy mode from memory forensic

Jinseong Park[1] · Seunghee Seo[2] · Changhoon Lee[3*]

[1]Master's Course, Department of Computer Science and Engineering, Seoul National University of Science and Technology, Seoul 01811, Korea
[2]Ph.D. Course, Department of Computer Science and Engineering, Seoul National University of Science and Technology, Seoul 01811, Korea
[3]Professor, Department of Computer Science and Engineering, Seoul National University of Science and Technology, Seoul 01811, Korea

[요 약]

웹 브라우저에서 행해지는 행동과 관련된 데이터들을 저장하지 않는 기능을 사생활 보호 모드라고 하며, 대다수 웹 브라우저에서 지원하는 기능이다. 해당 기능은 사용자의 개인 정보 보호를 목적으로 제공되나, 웹 활동 데이터를 저장하지 않아 웹 브라우저 상의 사용자 행위 추적에 대한 안티포렌식 방안으로 사용할 수 있다. 그러나 모바일 웹 브라우저의 사생활 보호 모드에 대한 포렌식 관점으로 분석한 기존 연구가 전무하다. 따라서 본 논문에서는 모바일 웹 브라우저 4종을 대상으로 모바일 웹 브라우저의 사생활 보호 모드에서 메모리 포렌식을 시도하여 사용자 행위를 유추할 수 있는 데이터를 획득하였다. 실험을 통해 검색 엔진에 따른 검색 사이트의 URL을 분석하여 검색어 및 방문 사이트를 찾기 위한 키워드를 추출하였다. 또한, 파일 다운로드 여부를 확인하고, 저장된 경로를 추출하였다. 본 연구를 통해 분석된 웹 브라우저의 사용 흔적은 디지털 포렌식 수사에 활용되어 사용자의 행위 파악에 기여할 수 있다.

[Abstract]

The function that allows not to store data of actions taken in web browsers is called privacy mode, and is supported by most web browsers. This function is provided to protect user's privacy, and since it does not store web activity it can be used as an anti-forensics method to protect from tracking users behavior in web browsers. However, there are no existing researches analyzed from a forensics perspective on the privacy mode of mobile web browsers. Thus, in this paper, four mobile web browsers were selected to conduct memory forensics of the privacy mode to obtain data that can determine user's behavior. The experiment was conducted by analyzing the URL of the searched sites according to the search engine and extracting keywords to find searched terms and visited sites. In addition, it was analyzed whether the file was downloaded or not, and if it was, we were able to extract path to the file. The web browser traces analyzed in this study can be used in digital forensics to help identify user behavior.

색인어 : 웹 브라우저 사생활 보호 모드, 모바일 웹 브라우저 포렌식, 모바일 메모리 포렌식, 모바일 포렌식
Key word : Web Browser Private Mode, Mobile Web Browser Forensics, Mobile Memory Forensics, Mobile Forensic

http://dx.doi.org/10.9728/dcs.2020.21.4.781

Received 04 March 2020; **Revised** 15 April 2020
Accepted 25 April 2020

***Corresponding Author; Changhoon Lee**

Tel: +82-2-970-6712
E-mail: chlee@seoultech.ac.kr

Ⅰ. 서 론

정보 획득의 창구라고 볼 수 있는 브라우저는 PC 및 모바일 기기에 설치되어 인터넷을 이용할 수 있게 돕고 있으며, 사용자의 인터넷상에서의 활동에 대한 많은 정보를 저장한다. 특히 모바일 웹 브라우저의 경우, 한국인터넷진흥원에서 조사한 결과에 따르면 대부분의 사람들이 인터넷을 이용하고 있으며, 인터넷 접속 방법은 모바일 웹 브라우저를 이용한 접속이 대다수인 것으로 나타나 그 중요성을 짐작할 수 있다.[1] 이러한 웹 브라우저는 검색 단어 기록, 방문한 사이트 기록, 인터넷 이용 시에 사용자에게 제공하기 위한 이미지 및 사용자가 다운로드한 파일 등의 자료를 저장하고 있다. 브라우저의 방문 기록, 쿠키 저장소 등을 확인하면 찾아볼 수 있는 이러한 자료는 디지털 포렌식 수사 과정에서 주요한 직접 증거 혹은 정황증거로써 사용할 수 있으므로 디지털 포렌식 관점에서 중요한 아티팩트로 활용될 수 있다. 그러나 이러한 자료는 쉽게 취득할 수 있으므로, 개인 정보 유출에 대한 우려가 생길 수 있다. 이러한 우려를 해결하기 위해 브라우저의 제조사는 웹 브라우저에서 사생활 보호 모드를 제공하고 있다. 크롬 브라우저의 Incognito 모드, 파이어폭스 브라우저의 Private browsing 모드, 엣지 브라우저의 InPrivate 모드 등이 있으며, 사용자의 방문 기록, 검색 기록 등 사용자 기기에 남은 흔적을 지워 개인 정보를 보호한다. 이러한 기능은 사용자의 개인 정보를 보호할 수 있는 순기능을 하기 위해 제공되지만, 피의자가 자신의 행적을 숨기기 위해 안티포렌식(Anti-Forensic) 측면에서 활용하는 역기능을 하기도 한다.

피의자는 자신의 범죄 행위를 위해 인터넷을 통해 정보를 수집한다. 또한, 사이버 범죄 같은 일부 범죄는 인터넷을 통해서 범죄 행위가 발생하기도 한다. 디지털 포렌식 수사관은 이러한 범죄 행위 혹은 범죄 행위를 위한 사전 준비과정을 밝히기 위해, 일반적으로 웹 브라우저의 검색 기록, 방문 기록, 다운로드 기록 및 캐시 파일 등을 조사하여 추적한다. 따라서 이러한 웹 아티팩트들은 범죄 행위에 대한 증거로 사용될 수 있으므로 매우 중요한 정보로 분류할 수 있다. 그러나 웹 브라우저의 사생활 보호 모드를 활성화하는 경우, 일반적으로 발생하는 웹 활동 흔적이 발생하지 않기 때문에 수사관이 범죄 행위를 입증하기 어렵게 한다. 실제로 2018년에 발생한 일명 '드루킹' 사건에서도 추후 포렌식 조사를 대비하여 크롬 브라우저의 사생활 보호 모드를 활성화하여 사용할 것을 강조한 매뉴얼이 발견되기도 하였다[2]. 따라서 디지털 포렌식 수사관의 관점에서 사생활 보호 모드를 활성화한 브라우저에서의 행위를 추적할 수 있어야 피의자의 범죄 행위를 입증할 수 있다.

그러나 모바일 환경에서의 웹 브라우저 사생활 보호 모드에 관한 연구는 전무하다. 따라서 본 논문에서는 모바일 웹 브라우저의 사생활 보호 모드에 메모리 포렌식을 적용하였으며, 사용자 행위를 유추할 수 있는 데이터를 획득하였다. 통계 사이트 Statcounter[3]가 제공한 정보에 따르면 안드로이드 운영체제는 국내 모바일 기기의 운영체제의 점유율의 75%를 상회한다. 따라서 실험 환경은 최신 안드로이드 운영체제인 Android 9.0에서 연구를 수행하였다. 또한, 대상 모바일 웹 브라우저는 안드로이드 운영체제에서 구동하는 애플리케이션의 사용률이 높은 Chrome, Samsung Internet, Whale, Firefox의 4개의 모바일 웹 브라우저를 선정하였다. 실험을 위해 실험 대상 모바일 웹 브라우저의 사생활 보호 기능을 실행한 후, 영어 및 한국어로 검색하였으며, 웹 사이트를 방문하고, 파일을 다운로드하는 등의 웹 활동을 수행한 후, fridump 도구를 사용하여 메모리를 덤프하였다. 추출한 덤프 파일을 분석하여 검색 엔진에 따른 검색 사이트의 URL을 추출하여 검색어 및 방문 사이트를 찾기 위한 키워드를 추출하였다. 또한, 방문한 웹 사이트에서의 다운로드 가능한 파일이 존재하는 경우, 파일 이름을 키워드로 검색하여 파일 다운로드 여부를 확인하였고, 저장된 경로를 추출하였다. 실험 내용을 바탕으로 모바일 웹 브라우저의 사생활 보호 모드를 분석하기 위한 메모리 포렌식 절차를 제시하였다. 그 결과, 모든 대상 모바일 웹 브라우저에 대하여 검색 키워드, 방문한 웹 페이지 내역, 다운로드 파일의 경로를 추출할 수 있었다. 이렇게 추출한 웹 아티팩트는 디지털 포렌식 수사에 직접 증거 또는 간접 증거로 활용할 수 있을 것으로 기대된다.

본 논문은 2장에서 모바일 메모리 포렌식, 모바일 웹 브라우저 분석, 웹 브라우저 사생활 보호 모드 분석으로 나누어 관련 연구들을 정리하고, 3장에서 웹 브라우저의 사생활 보호 모드에서 데이터 획득 및 분석 시나리오를, 4장에서 실험 환경 및 실험 결과를 제시한다. 마지막으로 5장에서는 결론과 함께 향후 연구 계획을 기술하며 본 논문을 마치고자 한다.

Ⅱ. 관련 연구

디지털 포렌식 관점에서의 웹 브라우저 분석에 관련된 연구는 여러 차례 진행된 바 있다. 모바일 환경에서 행해진 기존 연구들을 살펴보면 모바일 메모리 포렌식을 통해 데이터를 추출하기 위한 시도가 여러 차례 존재한다. 그러나 일부 애플리케이션에 관한 연구만 진행되었기 때문에, 웹 브라우저 애플리케이션에 적용한 연구는 존재하지 않았다. 이외에도 PC 환경에서의 웹 브라우저의 사생활 보호 모드는 많은 정보가 저장되지 않아 범죄 행위 은닉에 사용될 수 있어 연구되어왔다.

2-1 모바일 메모리 포렌식

모든 프로그램은 실행되기 위해서 RAM에 적재된다. RAM은 휘발성 메모리이기 때문에 PC에 전원이 종료되는 경우, RAM에 적재되었던 데이터는 모두 휘발된다. 그러나 PC의 전원이 종료되기 이전에 RAM을 포렌식 수사관이 획득할 수 있는 경우, 하드 디스크에 기록되지 않은 정보를 획득할 수 있다. 웹 브라우저 또한 프로그램이므로 사생활 보호 모드를 활성화하더라도 프로그램이 실행되기 위해서 RAM에 브라우저 프로그램의 코드 및 관련 데이터가 적재되어야 한다. 따라서 용의자

가 사생활 보호 모드를 활성화한 웹 브라우저를 사용하더라도, 신속하게 사용된 PC의 RAM 메모리를 확보하여 데이터를 수집하면 RAM에 적재된 데이터를 분석하여 웹 브라우저에서의 활동 기록을 추출할 수 있다.

Thing 외 2명[4]은 다양한 시나리오를 예상한 후, 메모리 포렌식을 이용하여 모바일 기기를 실시간으로 분석하는 자동 시스템을 제안하였다. 해당 연구에서는 시나리오별로 메모리 덤프 간격을 다르게 하였다. Google Talk 메신저를 통해 모바일 기기와 PC에서 송·수신한 메시지를 추출한 후, 메모리 덤프 파일을 분석하여 송·수신한 메시지를 취득하는 연구를 진행하였다. 연구를 통해 발신 메시지의 취득률은 100%, 수신 메시지는 시나리오별로 75.6%에서 100%까지 다양한 분포를 보였다.

이외에도 모바일 환경에서 메모리 포렌식을 진행한 연구가 존재한다. Zhou Fan 외 3명[5]은 중국에서 가장 많이 사용하는 메신저인 Wechat 메신저를 대상으로 Wechat 애플리케이션이 사용하는 메모리 영역을 덤프하여, 저장된 메시지뿐만 아니라 이미 삭제된 메시지, 암호화된 메시지마저 평문 형태로 추출할 수 있음을 보였다.

2-2 모바일 웹 브라우저 포렌식

최신 모바일 기기는 기술의 발전에 따라 성능이 매우 증가하였으며, 데스크톱 PC보다 모바일 기기의 성능이 더 높은 경우가 많아지고 있다. 그 결과, 모바일 기기는 점차 데스크톱 PC를 대체하기 시작하였다. 또한, 모바일 기기는 휴대가 간편하므로 접근성이 용이하다. 이러한 이유로 모바일 기기의 사용률이 증가하였고, 따라서 모바일 웹 브라우저를 대상으로 포렌식적으로 웹 아티팩트를 분석한 연구가 존재한다.

Emrah Sariboz외 1명[6]은 안드로이드 환경에서 Chrome, Samsung, Firefox, Opera, Web Explorer의 5개의 웹 브라우저에서 15개의 웹 사이트를 대상으로 웹 스토리지를 분석하여 웹 사이트의 방문 기록을 추출하였다. 그러나 해당 연구는 사생활 보호 모드를 고려하지 않았으며, 사용자가 웹 활동을 은닉하기 위해 파일을 삭제하는 경우에 대한 해당 방법은 정보 획득에 어려움이 있다.

2-3 웹 브라우저 사생활 보호 모드 포렌식

웹 브라우저의 사생활 보호 모드를 활성화한 경우, 데이터를 취득하기 위한 많은 연구가 진행되었다. Said Huwida 외 3명[7]은 Google Chrome, Mozilla Firefox, Internet Explorer 브라우저에서 사생활 보호 모드의 효용성을 검사하고, 사생활 보호 모드를 활성화한 경우, 포렌식 아티팩트를 추출하는 방법을 연구하였다. 그 결과 pagefile.sys 파일에서 일부 잔존 흔적을 발견하였으며, 포렌식 도구로 RAM을 조사하여 사생활 보호 모드에서 사용한 웹 아티팩트를 복원할 수 있음을 보였다.

Alam Shumaila 외 2명[8]은 Microsoft 사의 Edge 브라우저의 경우, 시크릿 브라우징 프로세스가 종료된 이후에는 데이터가 삭제되지만, 다른 데이터로 덮어쓰게 되기 이전에는 디스크에 데이터가 남아있어 적절한 포렌식 도구를 이용하여 데이터를 분석할 경우 사용자의 행적을 Web Cache 파일 및 pagefile.sys 파일, Master File Table (MFT) 및 비할당영역에서 데이터를 취득하여 추적할 수 있음을 보였다.

Rebecca Nelson 외 2명[9]은 Google Chrome, Mozilla Firefox, Tor 브라우저에 대하여 사생활 보호 모드를 활성화하지 않은 브라우저와 사생활 보호 모드를 활성화한 이후의 브라우저에서 추출할 수 있는 포렌식적 아티팩트를 비교 조사하였으며, Firefox 브라우저 및 Firefox 브라우저를 기반으로 제작된 Tor 브라우저의 확장 도구를 설치하여 사용한 경우, 일부 확장 도구에 한하여 복구 가능함을 보였다.

본 장에서는 기존 연구를 모바일 메모리 포렌식, 모바일 웹 브라우저 포렌식, 웹 브라우저 사생활 보호 모드 포렌식의 세 가지 관점에서 살펴보았다. 그러나 모바일 환경에서 웹 브라우저의 사생활 보호 모드를 활성화한 경우에 관한 연구는 전무하였다. 또한, PC 환경의 웹 브라우저의 사생활 보호 모드 포렌식 연구에서 시도된 일부 분석기법은 파일 시스템 구조의 차이, 안드로이드 환경에서의 메모리 관리 기법의 차이 등으로 인하여 모바일 환경 분석에 적합하지 않다. 이외에도 모바일 환경에서 포렌식적 증거 획득을 위해 사용된 연구가 존재하나, 모바일 웹 브라우저를 대상으로 하고 있지 않았다. 따라서 본 연구는 안드로이드 환경에서 적용 가능한 분석 관점 중 메모리 포렌식을 이용하여 웹 아티팩트 추출 절차를 제시하였으며, 제시된 웹 아티팩트 추출 절차대로 실험하였다. 또한, 취득한 데이터를 분석하여 디지털 포렌식 아티팩트를 추출하여 브라우저별로 결과를 비교하였다.

Ⅲ. 모바일 웹 브라우저 메모리 포렌식 절차

PC 환경과 동일하게 모바일 환경에서도 프로그램이 실행되기 위해서는 메인 메모리에 적재되어야 한다. 따라서 용의자가 모바일 기기에서 웹 브라우저의 사생활 보호 모드를 활성화하여 사용하더라도 모바일 기기의 전원이 종료되기 이전에 포렌식 수사관이 수집 절차에 따라[10] 신속하게 데이터를 추출한 경우, 사생활 보호 모드가 활성화된 웹 브라우저의 활동 기록을 추출할 수 있다. 그러나 메인 메모리의 경우, 휘발성 데이터이기 때문에, 모바일 기기의 전원이 종료된 후 입수된다면 메모리 포렌식 기법을 이용한 분석이 불가능하다.

메모리 포렌식을 이용하는 경우, 분석 절차는 다음과 같다. 먼저 분석 대상 모바일 기기의 메모리를 덤프한다. 이후, 덤프한 데이터에서 검색어를 추출한다. 검색 페이지는 검색 엔진에 따라 특정 키워드를 URL 상에 포함하게 된다. 국내 대부분의 웹 브라우저는 Google 검색 엔진, Naver 검색 엔진, Bing 검색 엔진을 주로 사용하며, 세 개의 웹 브라우저 모두 URL에 공통으로 search라는 키워드를 포함한다. Google 및 Bing 검색 엔진

은 ‘search?’ 키워드 다음에 ‘q=’이라는 키워드가 한 번 더 사용되었으며, ‘q=’키워드 다음에 검색어가 등장하였다. Naver 검색 엔진은 search라는 키워드 뒤에 ‘query=‘라는 키워드가 한 번 더 사용되었으며, ’query=’ 키워드 다음에 검색어가 나왔다. 따라서 메모리 덤프 파일에서 search라는 키워드를 바탕으로 검색을 진행하여, 검색어를 추출할 수 있다.

다음으로 방문한 웹 사이트를 추출한다. 대부분의 웹 사이트는 접속 시, ‘http://’ 혹은 ‘https://’라는 단어로 시작하게 된다. 따라서 키워드 검색을 통해 일차적으로 접속한 사이트를 추출할 수 있다. 그러나 일부 사이트의 경우, 해당 키워드가 남지 않는 경우가 존재한다. 따라서, 앞선 과정에서 추출한 접속 사이트에서 키워드를 추출한 후, 추출한 키워드를 바탕으로 이차적으로 검색하는 과정이 반드시 필요하다. 해당 과정을 반복하여 접속한 웹 사이트의 기록을 추출할 수 있다.

웹 브라우저에서 파일을 다운로드하는 경우, 파일은 웹 브라우저에서 지정된 기본 경로에 저장되게 된다. 따라서 각 웹 브라우저의 파일 저장 경로를 키워드로 덤프 파일을 검색하면 찾을 수 있다. 또는, 일부 사이트의 경우, 웹 페이지에 다운로드 가능한 파일이 존재하며, 이는 또 하나의 검색 키워드가 될 수 있다. 파일 이름을 키워드로 하여 덤프 파일을 다시 검색하면, 다운로드한 파일의 디렉토리를 확인할 수 있다. [그림 1]는 제시한 과정을 절차도로 나타내었다.

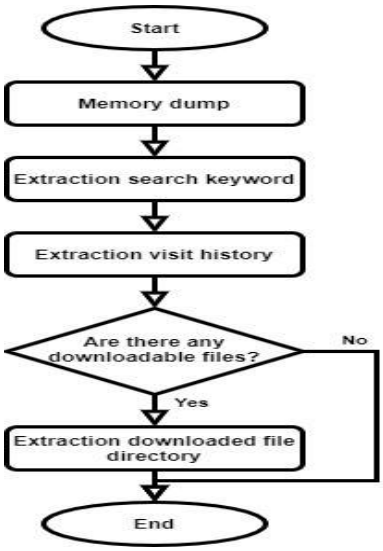

그림 1. 모바일 웹 브라우저 분석 절차도
Fig. 1. Mobile Web Browser Analysis Flow Chart

Ⅳ. 실험 및 결과 분석

본 장에서는 이전 장에서 제시한 프로세스를 바탕으로 실험을 수행하여 사생활 보호 모드를 활성화한 웹 브라우저의 활동 기록을 추출한 후 결과를 정리한다.

4-1 실험 환경 및 설정

실험에 사용된 기기는 Galaxy A7 (2018) (SM-A750N)을 사용하였으며, 실험 대상 웹 브라우저의 애플리케이션의 정보는 [표 1]과 같다.

표 1. 실험 대상 웹 브라우저 애플리케이션
Table 1. Target Web browser application

Web Browser	Application Version	Privacy Protect Service	Default Search Engine
Chrome Browser	79.0.3945.93	Incognito mode	Google
Samsung Internet Browser	10.2.00.53	Secret mode	Google
Whale Browser	1.1.8.2	Secret Window	Naver
Firefox Browser	68.3.0	Private browsing mode	Google

실험은 다음 방법으로 진행하였다. 모바일 기기에서 각 실험 대상 웹 브라우저의 사생활 보호 모드를 활성화한 후, 범죄와 관련된 단어를 검색하였다. 본 연구에서는 모든 웹 브라우저에서 공통적으로 한글로 ‘마약’이라는 단어와 영어로 ‘drug’라는 단어를 검색하였으며, 검색 사이트 중 일부 페이지를 방문 및 파일을 다운로드하는 등의 웹 활동 기록을 남긴다. 그 후 이전 장에서 제시한 방법을 통해 포렌식 아티팩트의 추출 가능성을 확인한다.

본 실험에서는 Frida 라는 오픈 소스로 공개된 동적 바이너리 조사 도구를 이용하였다. Frida는 Python을 기반으로 동작한다. Frida API로 만들어진 도구는 frida-tools 라는 Python 패키지를 통해 설치 가능하다. frida-tools로 설치되는 도구 중, 메모리 덤핑 기능을 제공하는 fridump를 이용하여 대상 기기의 메모리를 덤프하였다. fridump는 Windows나 Linux, Mac OS까지 지원하기 때문에 Linux를 기반으로 하는 안드로이드뿐만 아니라 Mac OS를 기반으로 하는 iOS 또한 분석 가능하다는 장점이 있다.

본 실험에서 Frida는 12.6.23 버전을 사용하였으며, fridump를 사용하기 위해 설치가 필요한 frida-tools는 4.1.0 버전을 설치하였다. Frida를 사용하기 위해 대상 기기에서 데이터를 전송하기 위한 Frida server를 실행하여야 하며, Frida server는 12.8.5 버전을 사용하였다[표 2].

표 2. Frida 실험 환경
Table 2. Frida Experimental Environment

Tool	Version
Frida	12.6.23
Frida-tools	4.1.0
Frida-server	12.8.5

Frida는 대상 기기에 서버를 설치하고, PC 환경에 설치된 Frida는 클라이언트로 동작하여, PC에서 명령어를 전송하면 대상 기기에 설치된 서버에서 동작하여, 그 결과를 다시 PC에서 보여주는 구조를 이룬다[그림 2]. 대상 기기에 Frida-server 바이너리 파일을 전송한 후, 백그라운드로 실행시키는 간단한 과정을 거치면 Frida의 기능을 이용할 수 있다.

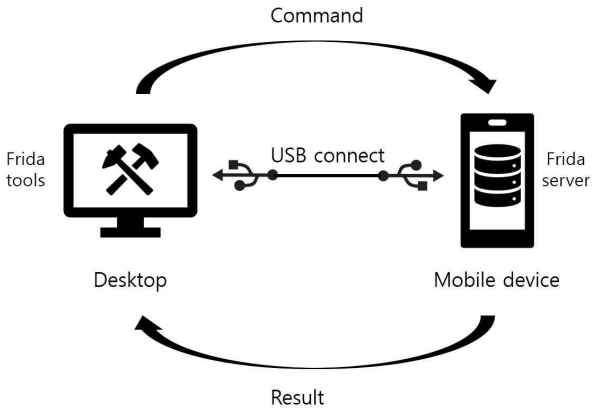

그림 2. Frida 환경 설정
Fig. 2. Frida Setting

4-2 브라우저별 메모리 포렌식 분석 실험

RAM에 저장되는 데이터는 휘발성 데이터이므로 용의자가 웹 브라우저의 사생활 보호 모드를 활성화하여 사용한 후, 전원이 종료되기 이전에 포렌식 수사관이 모바일 기기를 입수하였음을 전제로 한다. 또한, 해당 실험에서 디바이스의 루팅이 반드시 전제되지는 않는다. 그러나 Frida server를 실행시킨 계정의 권한에 따라 읽기가 가능한 데이터만 추출하기 때문에, 루팅이 되지 않은 경우에 비해 루팅이 된 경우에 더 많은 데이터를 추출할 수 있다. Android 모바일 기기의 메인 메모리를 분석하기 위해 메인 메모리를 덤프하는 작업이 선행되어야 한다.

1) Chrome 브라우저

Google에서 제공하는 chrome 브라우저의 private browsing에 관한 문서[11]에서 Incognito mode를 활성화하면 기록 정보, 쿠키 및 사이트 데이터, 양식에 입력한 정보, 웹 사이트에 제공한 권한 정보 등이 기록되지 않는다고 명시되어 있다. 위와 같은 정보를 바탕으로 사용자가 chrome 브라우저의 Incognito mode를 활성화한 후, 실험 환경에서 언급한 바와 같이 웹 활동을 하였다고 가정한 후, fridump를 이용하여 메모리를 덤프한 후, 피의자의 웹 활동 기록과 관련된 웹 아티팩트를 추출할 수 있는지 확인하였다.

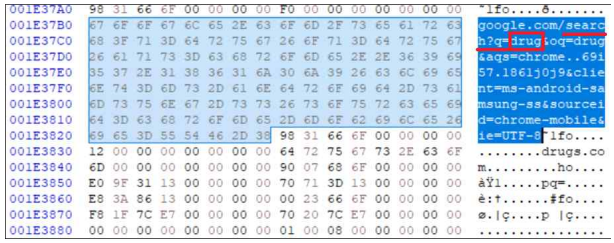

그림 3. Chrome 브라우저 검색어 (drug) 확인
Fig. 3. Chrome browser search term (drug)

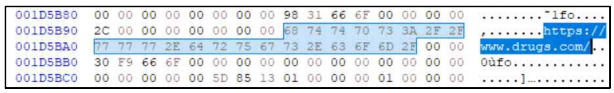

그림 4. Chrome 브라우저 방문 사이트 URL 확인
Fig. 4. Chrome browser visit history URL

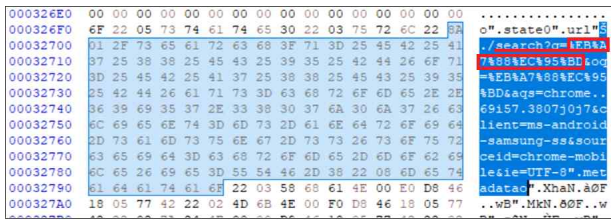

그림 5. Chrome 브라우저 한글 검색어 (마약) 확인
Fig. 5. Chrome browser Korean search term (drug)

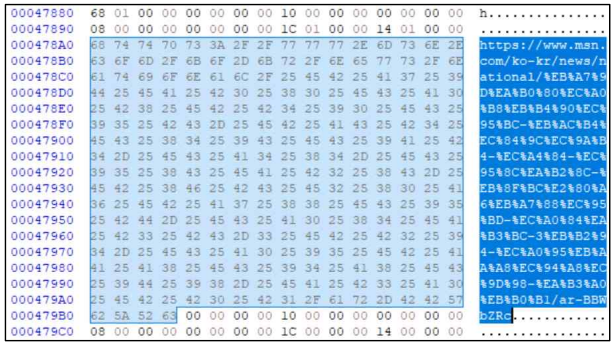

그림 6. Chrome 브라우저 방문 사이트 (한글 포함) 확인
Fig. 6. Chrome browser visit site (including Korean)

실험 결과, Chrome 브라우저에서 검색한 영어 단어 'drug'와 한글 단어 '마약'을 덤프 파일에서 확인할 수 있었으며[그림 3, 5], 접속한 사이트 목록 또한 영어로만 이루어진 URL[그림 4], 한글이 포함된 URL[그림 6]도 덤프 파일에서 확인할 수 있었다. 단, 한글이 포함된 경우, 퍼센트 인코딩이 되어있었다.

또한, 파일을 다운로드한 후, 파일을 삭제하여 흔적을 삭제하더라도 [그림 7]과 같이 방문한 웹 사이트의 주소를 파악할 수 있으며, 해당 사이트에 게시된 파일을 확인할 수 있었다. 또한 [그림 8]과 같이 다운로드한 흔적을 찾을 수 있었으며, 앞서 방문한 웹 사이트에서 게시된 파일명과 다운로드된 파일명을 비교하여 다운로드 여부를 확인할 수 있다.

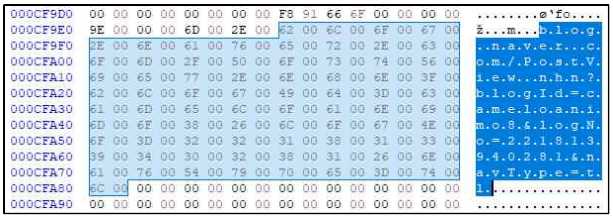

그림 7. Chrome 브라우저 다운로드 웹 페이지 주소 확인
Fig. 7. Chrome browser download webpage address

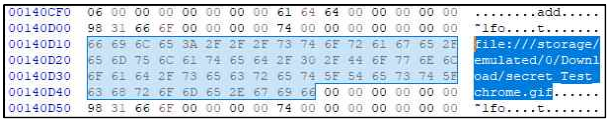

그림 8. Chrome 브라우저 다운로드 경로 및 파일 이름 확인
Fig. 8. Chrome browser download path and file name

2) Samsung Internet 브라우저

Samsung에서 제공하는 Samsung Internet 브라우저의 secret mode에 관한 문서[12]에서 Secret mode를 이용하면 브라우징 기록, 쿠키, 비밀번호 및 자동완성 데이터 등이 기록되지 않는다고 명시되어 있다. 위와 같은 정보를 바탕으로 피의자가 Samsung Internet 브라우저의 Secret mode를 활성화한 후, 실험 환경에서 언급한 바와 같이 웹 활동을 하였다고 가정한 다음, 메모리를 덤프하여 분석한 결과는 다음과 같다.

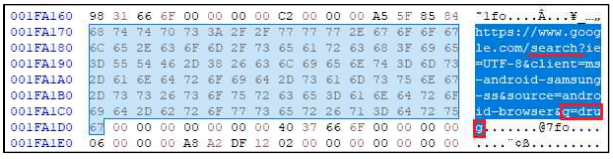

그림 9. Samsung Internet 브라우저 검색어 (drug) 확인
Fig. 9. Samsung Internet browser search term (drug)

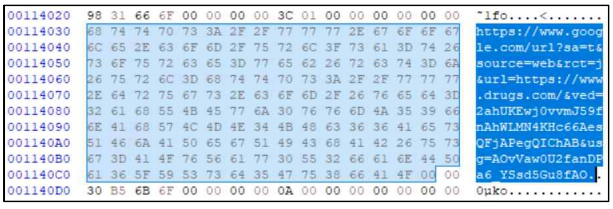

그림 10. Samsung Internet 브라우저 방문 사이트 URL 확인
Fig. 10. Samsung Internet browser visit history URL

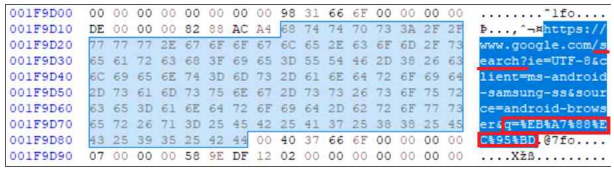

그림 11. Samsung Internet 브라우저 한글 검색어 (마약) 확인
Fig. 11. Samsung Internet browser Korean search term (drug)

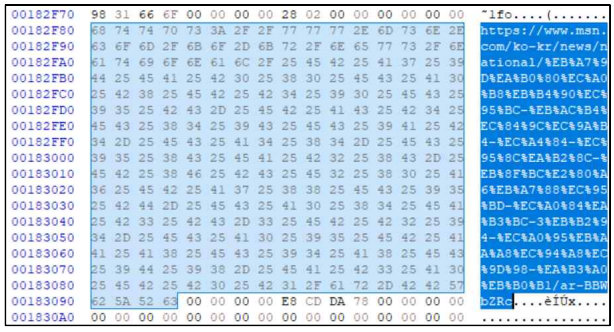

그림 12. Samsung Internet 브라우저 방문 사이트 (한글 포함) 확인
Fig. 12. Samsung Internet browser visit site (including Korean)

실험 결과, Samsung Internet 브라우저에서 검색한 영어 단어 'drug'와 한글 단어 '마약'을 덤프 파일에서 확인할 수 있었으며 [그림 9, 11], 접속한 사이트 목록 또한 영어로만 이루어진 URL[그림 10], 한글이 포함된 URL[그림 12]도 덤프 파일에서 확인할 수 있었다. 또한, Chrome 브라우저와 마찬가지로 한글이 포함되는 경우, 퍼센트 인코딩이 되어있었다.

Samsung Internet 브라우저는 타 브라우저와는 달리 파일을 다운로드할 때, [그림 13]에서 볼 수 있듯이 시크릿 모드에서 다운로드가 되는 것이 아니라, 일반 모드를 통해서 파일이 다운로드된다. 따라서 브라우저의 다운로드 페이지로 접근하면 다운로드했던 기록을 확인할 수 있다. 그러나 피의자가 자신의 웹 활동 기록을 은닉하기 위해 다운로드 기록을 삭제하는 경우에 메모리 포렌식을 이용하여 다운로드 페이지[그림 14] 및 다운로드 파일의 저장 디렉토리[그림 15]를 검출할 수 있다.

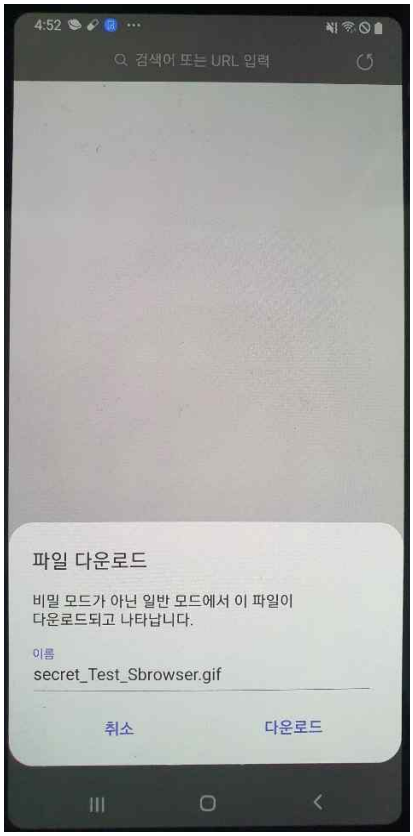

그림 13. Samsung Internet 브라우저 다운로드 화면
Fig. 13. Samsung Internet browser download screen

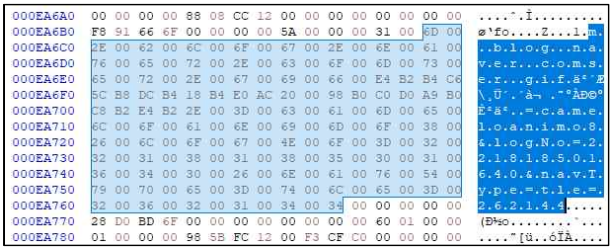

그림 14. Samsung Internet 브라우저 다운로드 웹 페이지 주소 확인
Fig. 14. Samsung Internet browser download webpage address

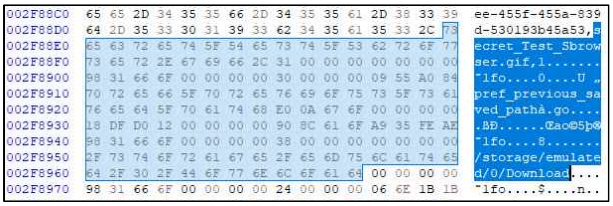

그림 15. Samsung Internet 브라우저 다운로드 경로 및 파일 이름 확인
Fig. 15. Samsung Internet browser download path and file name

3) Whale 브라우저

Naver에서 제공하는 Whale 브라우저의 시크릿 창에 관한 문서[13]에서는 해당 기능을 이용하면 방문 기록, 쿠키, 자동완성 및 임시파일은 기록되지 않으나, 북마크, 아이디 및 패스워드와 같은 계정 정보, 다운로드 목록은 유지된다고 명시되어 있다. 위와 같은 정보를 바탕으로 피의자가 Whale 브라우저의 시크릿 창을 이용하여 실험 환경에서 언급한 바와 같이 웹 활동을 하였다고 가정한 다음, 메모리를 덤프하여 분석한 결과는 다음과 같다.

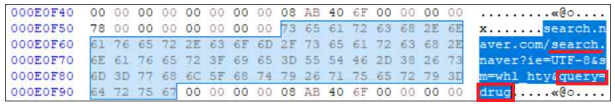

그림 16. Whale 브라우저 검색어 (drug) 확인
Fig. 16. Whale browser search term (drug)

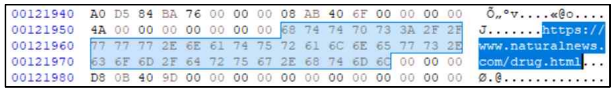

그림 17. Whale 브라우저 방문 사이트 URL 확인
Fig. 17. Whale browser visit history URL

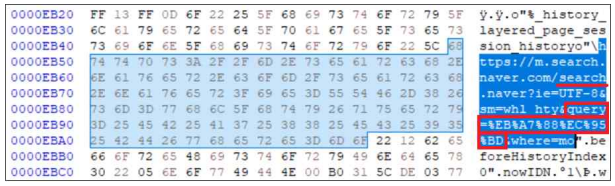

그림 18. Whale 브라우저 한글 검색어 (마약) 확인
Fig. 18. Whale browser Korean search term (drug)

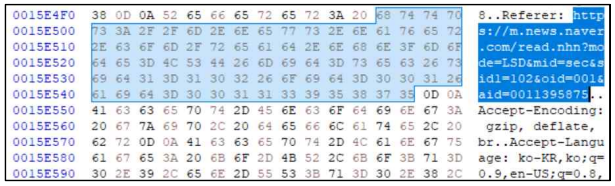

그림 19. Whale 브라우저 방문 사이트 (한글 포함) 확인
Fig. 19. Whale browser visit site (including Korean)

실험 결과, Whale 브라우저도 검색 단어[그림 16, 18]와 방문 사이트의 URL[그림 17, 19]을 덤프 파일에서 확인할 수 있었으며, 한글의 경우 퍼센트 인코딩이 되어있었다.

앞서 언급한 것과 같이 Whale 브라우저는 다운로드 기록을 유지한다고 명시하고 있다. 그러나 Samsung Internet 브라우저와는 다르게 일반 모드로 전환 후, 다운로드를 실행하지 않고 시크릿 창인 상태로 다운로드를 진행한다. 시크릿 창에서 다운로드를 진행하는 경우, 일반 모드의 다운로드 기록에서는 나타

나지 않고, 시크릿 모드의 다운로드 기록에서만 나타나게 된다. 따라서 프로세스가 종료되는 경우 다운로드 기록은 사라지게 된다. 그러나 메모리 포렌식을 이용하여 추출한 방문 페이지 목록에서 [그림 20]과 같이 다운로드 페이지를 확인하고, [그림 21]과 같이 다운로드한 파일의 경로를 확인할 수 있었다.

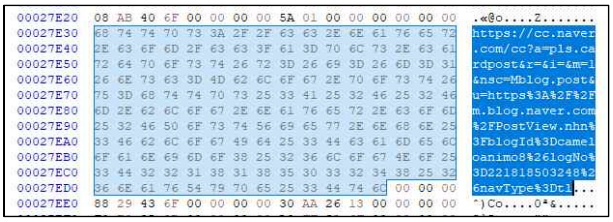

그림 20. Whale 브라우저 다운로드 웹 페이지 주소 확인
Fig. 20. Whale browser download webpage address

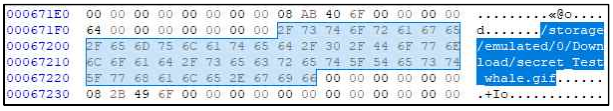

그림 21. Whale 브라우저 다운로드 경로 및 파일 이름 확인
Fig. 21. Whale browser download path and file name

4) Firefox 브라우저

Mozilla Firefox 브라우저의 private browsing에 관한 문서[14]에서 Private browsing mode를 이용하면 방문 히스토리, 폼 및 검색 항목, 다운로드 목록, 쿠키, 임시 보관 파일 등이 기록되지 않는다고 명시되어 있다. 위와 같은 정보를 바탕으로 피의자가 Firefox 브라우저의 Private browsing mode를 활성화한 후, 실험 환경에서 언급한 바와 같이 웹 활동을 하였다고 가정한 다음, 메모리를 덤프하여 분석한 결과는 다음과 같다.

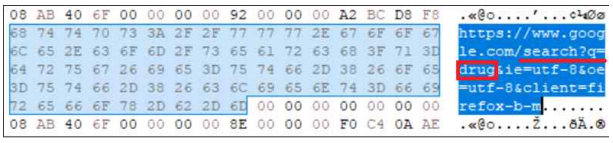

그림 22. Firefox 브라우저 검색어 (drug) 확인
Fig. 22. Firefox browser search term (drug)

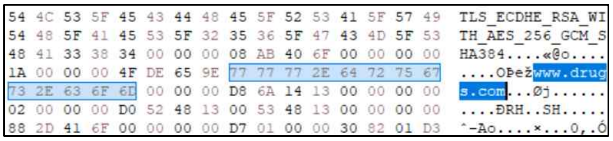

그림 23. Firefox 브라우저 방문 사이트 URL 확인
Fig. 23. Firefox browser visit history URL

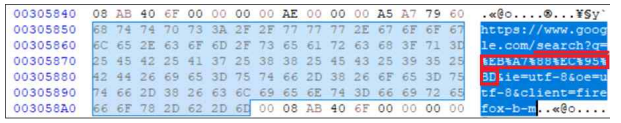

그림 24. Firefox 브라우저 한글 검색어 (마약) 확인
Fig. 24. Firefox browser Korean search term (drug)

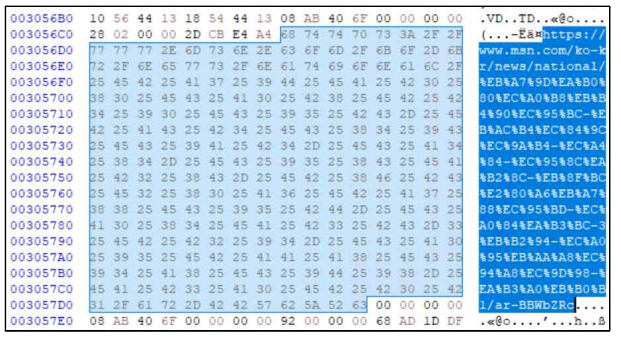

그림 25. Firefox 브라우저 방문 사이트 (한글 포함) 확인
Fig. 25. Firefox browser visit site (including Korean)

실험 결과, Firefox 브라우저도 타 브라우저와 같이 검색 단어[그림 22, 24] 및 방문 사이트 URL[그림 23, 25]를 확인할 수 있었으며, 한글은 퍼센트 인코딩이 되어있었다.

Firefox 브라우저의 다운로드 기록은 저장되지 않는다고 private browsing에 관한 문서에서 언급하고 있으며, 실제로 private browsing을 종료하는 경우, 다운로드 기록은 삭제되게 된다. 따라서 메모리 포렌식을 이용하여 메모리를 덤프한 후, 덤프 파일을 조사하였다. 그 결과, [그림 26]과 같이 다운로드한 웹 페이지의 주소를 확인할 수 있었으며, [그림 27]과 같이 다운로드한 파일의 디렉토리를 확인할 수 있었다.

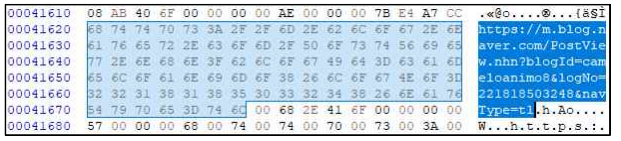

그림 26. Firefox 브라우저 다운로드 웹 페이지 주소 확인
Fig. 26. Firefox browser download webpage address

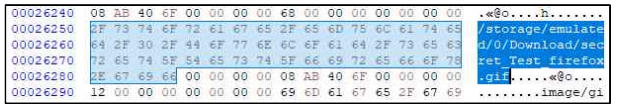

그림 27. Firefox 브라우저 다운로드 경로 및 파일 이름 확인
Fig. 27. Firefox browser download path and file name

4-3 결과 정리

모바일 웹 브라우저 제조사가 명시한 사생활 보호 모드에서 데이터의 저장 여부는 [표 3]과 같으며, 본 논문에서 수행한 실

험 결과를 정리하면 [표 4]과 같다. 실험 결과, 본 논문에서 제시한 절차대로 실험을 진행한 경우 메모리 포렌식을 통하여 모든 실험 대상 모바일 웹 브라우저의 사생활 보호 모드를 활성화하더라도 웹 아티팩트를 추출할 수 있음을 확인하였다.

표 3. 브라우저 제조사에서 제공하는 모바일 웹 브라우저 사생활 보호 모드 데이터 저장 여부
Table 3. Whether to save the mobile web browser privacy mode data provided by the browser manufacturer

Browser	Save Data	Non Save Data
Chrome	Bookmarks, Download file	Browsing history Cookies, Site Data, Information entered in Forms, Permissions
Samsung Browser	Bookmarks and Save pages (Only see secret mode), Download list, Download files	Browsing history, Cookies, Passwords, Auto-fill data
Whale	Bookmarks, ID/PW, Download list	Browsing history, Cookies, Auto-fill data, Cache file
Firefox	Bookmarks, New password, Download file	Browsing history, Information entered in Forms, Download list, Cookies, Cache file

표 4. 실험 결과
Table 4. Experimental Result

Experimental content	Browser	Detected	Content
Extraction Search Word (Using ‘search’ keyword)	Chrome	O	Search word can be found after ‘search?q’ keyword
	Samsung Browser	O	Search word can be found after ‘search?q’ keyword
	Whale	O	Search words can be found at the following 'query=' URL containing search keywords
	Firefox	O	Search word can be found after ‘search?q’ keyword
Extraction Visit Web site (Using ‘http://’, ‘https://’ keywords)	Chrome	O	Website address can be found
	Samsung Browser	O	Website address can be found
	Whale	O	Website address can be found
	Firefox	O	Website address can be found
Detected file download traces	Chrome	O	Download file directory checkable
	Samsung Browser	O	You can view the history on the download page, Download file directory checkable
	Whale	O	Download file directory checkable
	Firefox	O	Download file directory checkable

또한, 본 논문에서 제시된 방법은 사생활 보호 모드가 아닌 일반 모드에서도 사용이 가능하다. 일반 모드와 사생활 보호 모드에서 실행한 내용을 메모리 덤프 파일에서 추출했을 때의 차이점을 발견할 수 없었다. 실제로 Samsung Internet 브라우저의 경우, 다운로드가 일반 모드에서 진행되었지만, 메모리 포렌식을 진행한 결과, 타 브라우저와 마찬가지로 다운로드 여부 및 경로를 확인할 수 있었다.

Ⅴ. 결 론

본 논문은 범죄 행위가 의심되는 피의자의 모바일 기기를 전원이 종료되지 않은 상태로 압수된 상태로 디지털 포렌식 수사가 진행되었음을 가정하였다. 해당 시나리오를 바탕으로 피의자가 모바일 웹 브라우저의 사생활 보호 모드를 활성화하여 정보를 수집한 경우에도 메모리 포렌식을 이용하여 웹 아티팩트를 추출할 수 있었다.

실험을 수행한 결과, 모든 실험 대상 웹 브라우저가 사생활 보호 모드를 활성화하더라도 메모리 포렌식을 통하여 검색 흔적을 찾을 수 있었으며, 이를 바탕으로 웹 페이지의 방문 기록을 추출하였으며, 다운로드한 파일이 있을 경우, 파일을 저장한 경로 및 다운로드한 파일명을 추출할 수 있었다.

이렇게 추출한 웹 아티팩트를 바탕으로 디지털 포렌식 수사관은 피의자의 범죄 행위의 입증을 위한 증거로 사용할 수 있을 것이다. 비록 추출한 웹 아티팩트가 직접 증거로 사용될 수 없고, 정황증거로만 사용할 수 있을 수 있지만, 범죄 행위에 대한 추론을 가능하게 하는 역할을 할 수 있으므로 그 중요성을 짐작할 수 있다.

하지만 메모리 포렌식은 메모리가 휘발성이라는 문제점으로 인하여 모바일 기기를 전원이 종료되지 않은 상태로 압수되어야 한다는 한계점이 존재한다. 따라서 디지털 포렌식 수사관은 본 논문에서 제시한 메모리 포렌식을 이용한 웹 아티팩트 추출 방법뿐만 아니라 안드로이드 환경에서 적용할 수 있는 다른 방법인 비할당영역의 분석을 통해 웹 아티팩트를 찾는 연구가 수행되어야 할 것이다. 또한, 제시된 모바일 웹 브라우저 메모리 포렌식 프로세스 이후에 찾은 파일 경로를 이용하여 비할당영역 분석을 수행한다면 삭제된 파일의 복구 또한 수월하게 진행할 수 있을 것으로 기대된다. 따라서 향후 연구를 통하여 모바일 웹 브라우저의 비할당영역 분석을 진행하고자 한다.

감사의 글

이 연구는 서울과학기술대학교 교내연구비의 지원으로 수행되었습니다.

참고문헌

[1] 2018 Internet Usage Survey Summary Report. Korea Internet & Security Agency, KR, 2018.

[2] G. Y. Yu, (2018, April), [Monthly Central]"Druking"Chief"...Argette 'Sanchae' Core 30 People", Korea Joongang Daily [Online]. Available: https://news.joins.com/article/22551130

[3] Statcounter GlobalStats, Mobile & Tablet Browser Market Share Republic Of Korea. [Internet]. Available: https://gs.statcounter.com/browser-market-share/mobile-tablet/south-korea/#monthly-201812-201912.

[4] THING, Vrizlynn LL; NG, Kian-Yong; CHANG, Ee-Chien. "Live memory forensics of mobile phones." *digital investigation*, 7, S74-S82, 2010.

[5] F. Zhou, Y. Yang, Z. Ding, and G. Sun, "Dump and analysis of android volatile memory on wechat." *IEEE International Conference on Communications (ICC)*. p. 7151-7156, 2015.

[6] E. Sariboz and C. Varol, "Acquisition of Browser Artifacts from Android Devices." *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*. Vol. 7.2, p. 175-182. 2018.

[7] H. Said, N. Al Mutawa, I. Al Awadhi, and M. Guimaraes, "Forensic analysis of private browsing artifacts." *IEEE 2011 International Conference on Innovations in Information Technology*, p. 197-202. April 2011.

[8] S. Alam, M. A. Aziz, and W. Iqbal, "Forensic Analysis of Edge Browser In-Private Mode." *International Journal of Computer Science and Information Security*. Vol. 14.9, p. 256. 2016.

[9] R. Nelson, A. Shukla, and C. Smith, "Web Browser Forensics in Google Chrome, Mozilla Firefox, and the Tor Browser Bundle." *Springer, Digital Forensic Education*. p. 219-241. 2020.

[10] S.H. Seo, J.S. Park, Y. Kim and C.H. Lee, "Research on data collection for Android devices in the digital forensic aspect" *OSIA Standards & Technology Review*, Vol. 31.2, p.12-17. 2018.

[11] Google Chorme Help, How private browsing works in Chrome, [Internet]. Available: https://support.google.com/chrome/answer/7440301

[12] Samsung Newsroom, Samsung Internet 4.0 and Cross App Boost Functionality for Galaxy Devices with Android 6.0 Marshmallow Update https://news.samsung.com/global/samsung-internet-4-0-and-cross-app-boost-functionality-for-galaxy-devices-with-android-6-0-marshmallow-update

[13] Whale help, Secret Window, [Internet]. Available: https://help.whale.naver.com/desktop/features/secretwindow/

[14] Support mozilla, Private browsing mode, [Internet]. Available: https://support.mozilla.org/ko/kb/private-browsing-use-firefox-without-history

박진성(Jinseong Park)

2019년 : 서울과학기술대학교 대학원 컴퓨터공학과 (공학석사)

2019년～현　재: 서울과학기술대학교 컴퓨터공학과 석사과정
※관심분야 : 정보보호, 디지털 포렌식, 모바일 포렌식, 암호학 등

서승희(Seunghee Seo)

2019년 : 서울과학기술대학교 대학원 컴퓨터공학과 (공학석사)
2020년 : 서울과학기술대학교 대학원 컴퓨터공학과 (공학박사)

2020년～현　재: 서울과학기술대학교 컴퓨터공학과 박사과정
※관심분야 : 정보 보안, 메모리 포렌식, 모바일 포렌식 등

이창훈(Changhoon Lee)

2001년 : 한양대학교 자연과학부 수학전공 학사
2003년 : 고려대학교 정보보호대학원 석사
2008년 : 고려대학교 정보경영전문대학원 정보보호전공 박사

2008년～2008년: 고려대학교 정보보호연구원 연구교수
2009년～2012년: 한신대학교 컴퓨터공학부 조교수
2012년～2015년: 서울과학기술대학교 컴퓨터공학과 조교수
2015년～2020년: 서울과학기술대학교 컴퓨터공학과 부교수
2020년～현　재: 서울과학기술대학교 컴퓨터공학과 교수
※관심분야 : 정보보호, 사이버 보안, CTI, IoT보안, 디지털 포렌식, 암호학 등