Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.31, NO.3, Jun. 2021 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2021.31.3.353

협업 툴의 사용자 행위별 아티팩트 분석 연구 - 운영환경에 따른 differential forensic 개념을 이용하여*

김 영 훈,[1†] 권 태 경[2‡]
[1,2]연세대학교 정보대학원 정보보호 연구실 (대학원생, 교수)

On Artifact Analysis for User Behaviors in Collaboration Tools - Using differential forensics for distinct operating environments*

Young-hoon Kim,[1†] Tae-kyoung Kwon[2‡]
[1,2]Information Security LAB, GSI, Yonsei University (Graduate student, Professor)

요 약

언택트(Untact) 시대로의 급속한 변화 속에서 협업 툴(Collaboration Tool)은 비대면 업무를 위한 디지털 솔루션으로써 그 활용도와 가치가 증대되고 있다. 협업 툴은 다양한 기능을 지원하는 한편, 그 편의성에 비례하여 정보 유출, 보안사고 등 디지털 범죄 및 사고우려 또한 내재되어 있어 디지털 포렌식 관점에서의 연구가 필요하다. 본 연구에서는 세계적으로 점유율이 가장 높은 협업 툴 Microsoft Teams에 대한 윈도우즈 및 안드로이드 포렌식 연구를 통해 주요 사용자 행위를 정의하고 각 행위들을 수행한 뒤 의미 있는 아티팩트가 존재하는지 확인하였다. 이후 각 운영환경에서 획득 가능한 아티팩트를 비교·분석하고 여기에서의 차이점을 바탕으로 한 차분 포렌식(differential forensic)을 통해 협업 툴 분석기법 및 수사 시나리오 등 활용 방안을 제시하였다.

ABSTRACT

As the Untact era is rapidly changing, collaboration tools are increasing their utilization and value as digital technologies for non-face-to-face work. While instant messenger-based collaboration tools support a variety of functions, crime and accident concerns are also increasing in proportion to their convenience, such as information leakage and security incidents. Meanwhile, the digital forensics perspective on collaborative tools is not enough, so forensics research is needed. This study analyzes significant artifacts in the two operating environments through Windows and Android forensics research on Microsoft Teams, the collaboration tool with the highest share in the world. Also, based on differences in artifacts and data attributes according to the operating environment, by applying 'differential forensic', we proved that the usefulness of evidence can be improved by presenting a complementary analysis method and timeline configuration through information linkage.

Keywords: Digital Forensics, Differential forensic, Collaboration Tool, Microsoft Teams

Received(01. 08. 2021), Modified(04. 08. 2021), Accepted(04. 08. 2021)

* 본 연구는 2021년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(NRF-2019R1A2C1088802).

† 주저자, goodsmile@yonsei.ac.kr
‡ 교신저자, taekyoung@yonsei.ac.kr(Corresponding author)

I. 서 론

현대 사회는 디지털 워크로 빠르게 변모 중인 가운데 코로나19 이후 언택트(Untact) 문화가 확산됨에 따라 비대면 업무도 증가하고 있다. 이에 원활한 비대면 업무를 위한 각종 디지털 솔루션 수요가 높아지고 있으며, 그중에서 협업 툴(Collaboration Tool)이 그러한 니즈를 충족시키고 있다. 협업 툴은 Instant Messenger(IM)을 기반으로 하며 텍스트 외에도 음성 및 화상회의, 이메일, 파일 공유, 프로젝트 관리 등의 다양한 기능을 바탕으로 비대면 업무를 위한 유용한 도구로 자리매김하고 있다.

한편, 협업 툴의 기반인 인스턴트 메신저는 '텔레그램 n번방 사건'과 같이 디지털 범죄의 수단으로 악용되는 경우도 적지 않다. 이 같은 관점에서 볼 때 협업 툴 또한 경우 업무공간에서 이루어지며 쉽고 빠르게 정보를 교류할 수 있다는 장점과 동시에 기밀정보 및 자료 유출 등 범죄수단으로 악용되거나 보안사고를 유발할 가능성 또한 적지 않아 디지털 포렌식 관점의 연구가 필요하다. 또한, 대부분의 플랫폼 타입 애플리케이션의 경우 데스크톱과 모바일 환경 모두를 지원하는데 각 운영환경에서 생성되는 아티팩트의 종류 및 내용에도 차이가 존재할 수 있으며, 이 차이점을 포렌식 분석 전략으로 활용한다는 점에 기인한 차분 포렌식(differential forensic) 개념에 기반한 아티팩트 분석 및 활용방안 제시를 통해 여러 운영환경에서의 아티팩트를 종합적으로 비교·분석하고 활용한다면 디지털 증거의 다양성과 활용성을 높임으로써 궁극적으로 디지털 범죄 수사의 효율성을 제고하는데 기여할 수 있을 것으로 기대한다.

특히, 협업 툴은 시공간적 제약을 최소화한 업무 효율 향상에 그 목적이 있으므로 데스크톱 외에도 스마트폰 등 포터블 디바이스를 이용하여 다양한 운영환경에서 대상 애플리케이션을 이용할 수 밖에 없을 것이다. 따라서 본 연구에서는 분석 대상 애플리케이션이 윈도우즈 및 안드로이드 운영환경 모두에서 사용되는 것으로 가정한다.

본 논문에서 분석하는 프로그램은 그 대상 선정기준에 있어 범용성을 우선 고려하여, 다양한 종류의 협업 툴 중에서 현재 전 세계 시장점유율 1, 2위를 다투고 있는 협업 툴 애플리케이션인 Microsoft Teams를 선정하였다. 2장에서는 윈도우즈 및 안드로이드에서의 인스턴트 메신저 포렌식에 대한 기존 연구와 더불어 기존 연구의 한계점을 바탕으로 본 연구와의 차이점에 대하여 언급한다. 3장에서는 실험을 위한 실험 설계 및 구체적인 실험 방법을 설명하고 4장에서는 협업 툴의 포렌식 분석 결과를 정리하는데 각 운영체제에서 획득한 아티팩트와 함께 이에 관한 비교 분석 및 활용방안을 제시한다. 마지막으로 5장을 통해 본 논문의 결론을 맺는다.

II. 관련 연구 및 정의

2.1 기존 연구

협업 툴은 Instant Messenger(IM)을 기반으로 하며 이와 관련한 디지털 포렌식 연구는 다양하다. Aditya Mahajan, Thakur 등은 안드로이드 버전별 WhatsApp에 대한 포렌식 데이터 분석을 수행하여 다양한 아티팩트 획득이 가능함을 보였고[1][2] Yoon 등은 국내에서 점유율이 가장 높은 KakaoTalk 메신저에 대해 흔적파일의 디렉터리를 찾아 접근권한을 분석하고 데이터베이스 파일 구조분석을 통해 메시지 획득이 가능함을 보였다.[3] Yang 등은 윈도우즈 운영체제에서 세계적으로 사용되는 IM인 Facebook과 Skype를 대상으로 사용자 행위별 아티팩트를 발견할 수 있음을 증명하였고[4] 국내에서도 Seo 등은 안드로이드 환경에서 국내 랜덤 채팅 애플리케이션을 대상으로 사용자 행위 관점의 아티팩트를 분석한 결과 채팅 메시지 송수신 시간 및 내용, 송수신자, 계정 생성 시간 등을 확인한 연구를 선보였다.[5] 협업 툴에 대한 포렌식 분야 연구는 Shin 등이 Slack을 대상으로 모바일 및 PC 환경에서의 아티팩트를 분석한 것이 유일하며[6] Ababneh, A 등은 다양한 운영환경에서의 IM 아티팩트 분석을 목표로 안드로이드의 Nand flash memory와 윈도우즈의 RAM 메모리로부터 아티팩트를 획득 가능함을 증명하였다.[7] 안드로이드 포렌식의 다양한 데이터 추출 및 분석 기술을 다룬 연구도 수행되었는데, Scrivens, N 등은 안드로이드의 stroage의 구조 및 위치를 분석하고 storage에서의 데이터 추출 방법을 Logical Image / Physical Image로 구분하여 소개하였고 특히 Chip-Off, JTAG 등 기존의 기술 외 ADB, Custom Recovery 등을 이용하여 데이터의 무결성을 보장하고 화면 잠금으로 인해 데이터 추출이 제한되는 상황에서도 이를 우회할 수 있는 유용한 최신 기술을 언급하고 이를 이용한 실제 실험을 통해 데이터

를 추출하고 아티팩트를 분석한 결과를 발표하였다.[8]

2.2 기존 연구의 한계점

앞서 언급한 바와 같이 IM과 관련한 수많은 연구가 존재하지만 기존 연구들은 본 연구와 비교하여 몇 가지 한계점 및 차이점이 존재한다. [7]에서는 윈도우 및 안드로이드에서의 IM 아티팩트를 분석하고자 하였으나 윈도우의 경우 RAM 메모리를 덤프하여 메모리 포렌식을 수행하였는데 이러한 활성시스템 포렌식은 범죄자의 데스크탑 전원이 On 상태에 있어야 한다는 한정적인 상황에만 가능한 접근법으로 현실적이지 못하다는 한계점이 존재한다. 그러한 관점에서 본 연구는 분석대상 장비의 활성여부라는 제약요인을 해소하고자 윈도우즈 시스템의 디스크 이미징을 통한 포렌식에 한정하여 연구를 수행하였다. 또한, 다양한 IM 포렌식 대한 연구가 이루어졌으나 협업 툴에 대한 포렌식 연구의 경우 본 연구에서 분석하는 Microsoft Teams에 대해서는 포렌식 연구가 전무하며, 일부 협업 툴에 관한 1건의 연구만 존재하는 등 매우 미진한 실정이다. 이외에도 IM에 대한 기존 포렌식 연구는 대부분 단일 환경에서의 아티팩트 분석을 다루고 있으며 윈도우즈 및 안드로이드 양 환경에서의 분석결과를 비교하고 이를 종합하여 상호보완적으로 활용함으로써 증거의 다양성과 활용성을 높이려는 시도는 없었다. 이처럼 다양한 연구가 진행되었으나 최근 활용도가 높아지는 협업 툴에 대한 포렌식 연구는 미약하고, 윈도우즈 및 안드로이드 등 다양한 운영환경에서 포렌식 아티팩트를 분석하고 결과를 종합적으로 활용하기 위한 시도가 부족하여 본 연구의 필요성이 제기된다.

2.3 정의 : 차분 포렌식

포렌식 관련 연구 중 차분 포렌식의 개념을 다룬 연구가 Garfinkel 등에 의해 수행되었는데 여기에서는 최초 이미지와 최종 이미지 간의 변화된 부분에 초점을 맞추어 그 차이점을 분석하여 검증해야 할 정보의 양을 줄이고 중요 단서를 위한 노력을 집중할 수 있음을 보이고 있다.[9]

본 연구에서 다루고자 하는 차분 포렌식의 개념은 디지털 증거 간의 차이점에 기인하여 포렌식 분석을 위한 전략을 도출하는 것으로 정의할 수 있다. 보다 구체적인 개념을 설명하면 본 연구의 분석 대상인 플랫폼 기반 애플리케이션은 여러 운영환경에서 동시에 구동되는데 이 경우 사용자의 특정 행위에 대한 아티팩트는 운영환경에 따라 파일 및 데이터 형식, 내용(contents) 등 어떠한 차이점, 즉 차분 특성(differential feature)이 존재할 수 있고 이를 수사에 효과적으로 활용할 수 있는 방안을 마련하는 것이다. 여기에서 차분 특성의 범주는 특정할 수 없으나 포렌식 분석에 유의미하게 활용될 수 있는 성질을 지닌 것이라면 무엇이든 포함될 수 있다. 따라서 차분 포렌식을 위해서는 우선적으로 차분 특성를 도출해야 하며 해당 특성이 갖는 이점 및 특징에 따라 활용방안을 마련하는 과정이 필요하다.

III. 실험 방법

본 연구의 분석은 대표적인 협업 툴 애플리케이션인 Microsoft Teams를 선정하였으며 실험 대상 OS(operating system)는 사용자 점유율이 높은 윈도우즈 및 안드로이드로 선정하였다. 연구의 핵심 아이디어는 먼저, 각 운영환경에서 생성되는 분석대상 애플리케이션의 사용자 행위별 아티팩트를 획득하는 것이며, 다음으로 양 운영환경의 획득결과를 비교하여 차분 특성을 도출하고, 이를 바탕으로 수사효율을 높일 수 있는 이점 및 활용방안을 마련함으로써 차분 포렌식을 입증하는 것이다. 이를 위해 분석 가치가 높을 것으로 판단되는 주요 사용자 행위(Table 1)를 선별하고 이를 25개의 데이터 세트로 구성하였다. 이 사용자 행위를 기반으로 행위별 아티팩트 분석 실험을 위한 가상의 시나리오를 작성하였다. 그리고 각 행위 단계별 세밀한 분석을 목적으로 디스크 이미징을 위한 가상머신 기반 OS 구비, 커스텀 리커버리를 이용한 안드로이드 루팅, 포렌식 분석도구 등 실험환경을 조성하였다. 이후에는 실제 실험을 위해 시나리오에 기반하여 행위를 수행하고, 각 행위별로 데이터를 추출하여 목록화하였으며 최종적으로 추출된 데이터를 분석하여 아티팩트를 획득하였다. 평가에서는 데스크톱 및 모바일 각각의 환경에서의 획득률을 분석하는데 여기서 획득률이란 25개의 사용자 행위 테스트 데이터 세트 중 아티팩트를 통해 확인한 테스트 데이터 비율을 말한다. 각 운영환경에서의 획득률과 양 운영환경에서의 종합 획득률을 비교하고, 추가적인 활용방안을 제안하는 순으로 실험을 설계하였다. 앞서 설명한 실험 절차를 단계별 도

Table 1. List of major user behavior

Classification of behaviors		Details
1	Install	• download & installation
2	Connect / Create account	• login • account : name, e-mail, Country • profiles : nickname, profile-image
3	Message	• sending / receiving • create channel, invite members
4	File	• upload / sending • download / receiving
5	Call	• individual call / group meeting
6	Disconnect	• log-out
7	Uninstall	• uninstallation

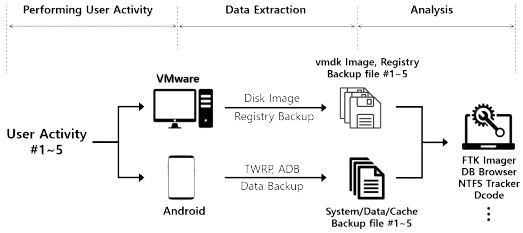


Fig. 1. Process of Artifacts Analysis

식화하면 Fig.1.과 같다.

운영체제 및 테스트 디바이스는 윈도우즈의 경우 Windows 10 Pro가 설치된 VMware 가상머신에서 실험을 하였고, 안드로이드는 Android version 8.0 오레오가 설치된 SAMSUNG Galaxy S8(SM-G950N)을 테스트 디바이스로 사용하였다. 또한, 행위별 데이터 변화를 분석하기 위하여 각 행위 단계별 디스크 이미징 및 데이터 추출(백업)을 진행하였는데 이러한 실험을 위해 윈도우즈에서는 테스트용 VMware workstation을 사용하였고, 안드로이드에서는 ADB(Android Debug Bridge), 커스텀 리커버리 TWRP[1)][10], Odin3[2)][11] 등의 소프트웨어를 이용하였다.

1) TWRP : (Team Win Recovery Project)는 안드로이드 기반 기기 오픈 소스 소프트웨어 커스텀 복구 이미지, 주로 안드로이드 장치 루팅시 활용

2) Odin3 : Samsung 내부에서 개발하고 사용하는 유틸리티 소프트웨어로써 사용자 정의 복구 펌웨어 이미지를 Samsung Android 장치로 플래시하는데 사용

IV. 실험 결과

4.1 윈도우즈 아티팩트

윈도우즈 운영체제에서 Teams 애플리케이션은 C:\Users\%USERPROFILE%\AppData\Roaming\Microsoft\Teams 경로에 설치되어 대부분의 데이터가 암호화되지 않은 형태로 저장된다. 포렌식 관점에서 유의미한 데이터는 애플리케이션 구동 및 사용자 행위에 따라 생성되는 log 및 cache 파일 등이 IndexedDB, Local Storage, Cache 디렉터리 등에 저장되어 있다.

Teams의 workspace 개념을 살펴보면 'Team'이 회사 등 조직을 의미하며 그 하위에 'Channel'이 워크스페이스 개념으로 구성되어 소통하는 방식이다. Team, Channel 정보 및 워크스페이스에서 이루어진 메시지 전송 관련 행위들에 대한 정보는 %USERPROFILE%\Microsoft\Teams\IndexedDB\https_teams.microsoft.com_0.indexddb.leveldb 디렉터리에 존재하는 [0-9]{6}.log에서 획득 가능한데 로그의 attribute 중 spaceThreadTopic, TeamAlias 항목에서 Team 명칭이 기록되고 threadProperties-topic에서 Channel 이름을 확인할 수 있다. 또한, Member(구성원) 및 Guest를 초대했을 경우 해당 참여자에 대한 사용자 정보도 확인 가능하였는데 UserType과 accountEnable 항목이 'Guest'인 부분의 로그에서 참여자의 이메일계정, 닉네임, 접속 시간 등의 정보를 확인할 수 있으며 Cache 디렉터리에서는 사용자 프로필 사진의 섬네일도 획득 가능하였다.

메시지 관련 데이터의 경우 messagetype, contenttype, content, displayname, composetime (originalarrivaltime), messageId 등 메시지 유형과 내용, 대화자 닉네임, 시간에 대한 Attribute 및 세부 정보가 포함되어 있다.(Fig. 2) 이 중 composetime은 UTC를 기준으로 기록되며 messageId는 동일한 시간정보를 Unix Time 포맷으로 저장하여 부여하게 된다. 앞서 확인한 정보들은 Cache 디렉터리의 data_#(0~3) Data block files에서도 획득 가능하였다.

파일 송수신 등 파일전송 관련 아티팩트는 %USERPROFILE%\Microsoft\Teams\IndexedDB\https_teams.microsoft.com_0.indexddb.

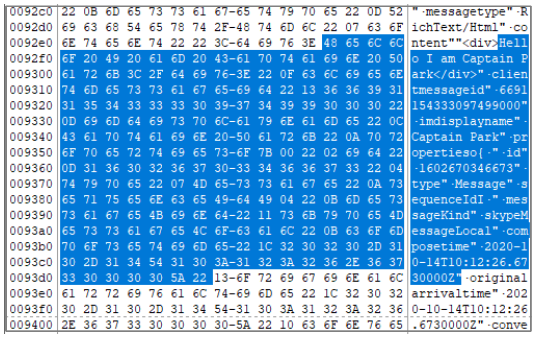


Fig. 2. Artifacts of Messaging Activities (Windows)

leveldb 디렉터리에 존재하는 [0-9]{6}.log에 포함되어 있으며 Attribute 중 'properties'가 'file'인 로그에서 ObjectURL(baseURL), type(파일 유형), title(파일 이름), composetime 등의 정보가 존재한다. 여기에서 ObjectURL의 경우 Team의 파일 공유를 위해 할당되는 SharePoint 개념으로 전송되는 파일이 저장된 서버의 URL이며 접속시 ID/password가 필요하고 파일 원본을 다운로드 할 수 있다.

이미지 파일을 전송하는 경우 Cache 디렉터리에 f_(0)(4)([0-9]|[a-z]){2}) 이름의 파일로 Thumbnail이 저장된다.(Fig. 3) 앞의 정보들은 %USERPROFILE%\Microsoft\Teams\Local Storage\leveldb 디렉터리의 [0-9]{6}.log에도 존재한다.

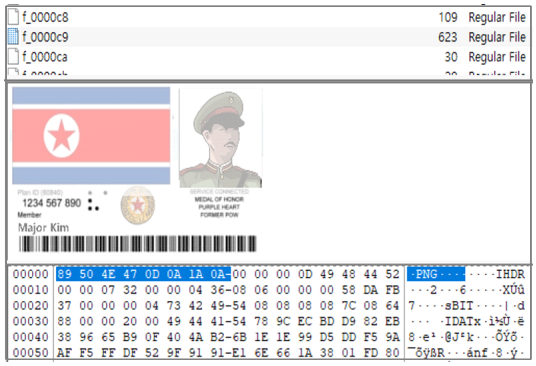


Fig. 3. Thumbnail of File transferred

4.2 안드로이드 아티팩트

일반적으로 안드로이드 운영체제에서 애플리케이션의 데이터는 '\data\data\패키지명' 경로 아래에 저장된다. 저장 방식은 크게 SQLite와 Preferenc em Local File으로 나뉘며 대부분 SQLite database를 사용한다. Teams 애플리케이션의 데이터는 'data\com.microsoft.teams' 경로에 저장되며 대부분의 데이터가 암호화되지 않은 형태로 저장되는데 사용자 행위 관련 데이터는 cache, databases, shared_prefs 디렉터리 '*.db' 및 '*.xml' 형식의 파일로부터 다양한 정보 획득이 가능하였다.

안드로이드 운영환경에서의 애플리케이션 설치 정보는 data\com.android.vending\databases 디렉터리의 localappstate.db 파일에서 얻을 수 있다.[12] 'appstate' 테이블의 package_name, first_downloads_ms, account(다운로드 계정), last_notified_version, install_request_timestamp_ms, title(app 이름) 등의 Attribute와 frosting.db 파일의 frosting_id 테이블에서 상세한 설치 정보 획득이 가능하다.

또한 data\com.microsoft.teams\files\shared_prefs 경로의 com.google.android.gms.appid.xml 파일에서도 설치와 관련한 데이터를 확인할 수 있다.

사용자 계정 및 프로필 설정과 관련한 정보는 com.microsoft.teams\shared_prefs 디렉터리의 'com.microsoft.teams_preferences.xml'에서 email, displayName, tenantId(팀 Id), region, name(실제 이름), PhoneNationalNumberMap (휴대전화 번호), mri 등의 정보를 알 수 있는데 여기서 'mri'는 tenant 에서의 사용자 UID(User Identifier)를 의미한다. com.microsoft.teams \databases 디렉터리 내 'SkypeTeams.db' 파일에서는 앞의 정보들을 포함하여 ImageUrl, profileImageString 등 프로필 이미지에 관한 데이터를 획득할 수 있다. com.microsoft.teams\cache \image_cache 하위 폴더에서는 사용자 프로필 사진의 cache 파일이 존재하는데 파일 확장자는 '*.cnt' 형식이지만 파일 시그니처 분석을 통해 이미지 파일임을 알 수 있었다.

Team 및 Channel 생성, 구성원 초대, 메시지 전송과 관련한 사용자 행위정보 대부분은 data\com.microsoft.teams\databases의 'SkypeTeams.db'에 존재한다. 여기서 중점적으로 확인할 테이블은 Message, MessagePropertyAttribute로 두 테이블에서 messageId, conversationId, content(Fig. 4), AttributeName & value 등 채팅

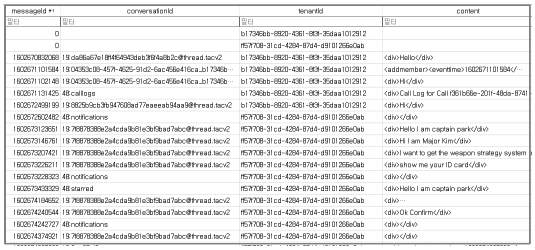


Fig. 4. Artifacts of Messaging Activities (Android)

이벤트 및 메시지 행위 관련 다양한 칼럼이 존재하고 유의미한 데이터 확보가 가능하다. 특히, mri, messageId, conversationId, tenantId 등 채널에서 이루어진 대화의 주체 및 메시지와 관련한 UID 정보를 활용하면 대부분의 대화내용을 타임라인에 따라 재구성 할 수 있다. Bookmark 테이블에는 채팅 도중 사용자가 특정 메시지를 저장하였음을 나타내는 정보가 존재한다.

개인 통화 및 그룹 통화(모임 기능)를 실행하면 'SkypeTeams.db' 파일의 MessagePropertyAttribute 테이블 내 attributeValue 값에서 callType이 'twoParty' 로 되어있는 경우 개인간 통화를 의미하며 CallConversationLiveState 테이블에 value 값을 참조시 group call에 대한 사용자 UID, 시간정보 등을 얻을 수 있다.(Fig. 5)

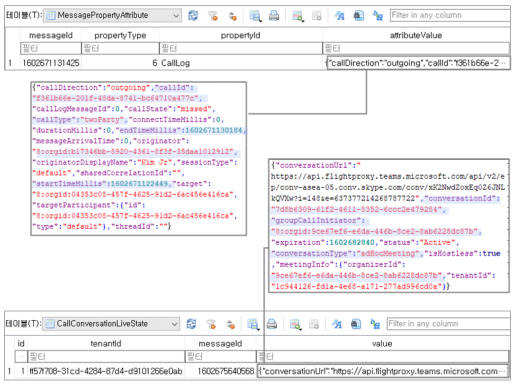


Fig. 5. Artifacts of 'Call' Activities(Android)

4.3 결과 분석 및 활용 방안

본 절에서는 4.2의 실험결과를 분석하여 도출한 두 가지 차분 특성을 바탕으로 디지털 증거의 다양성과 활용성을 높이기 위한 분석기법 및 활용방안을 제시한다.

4.3.1 운영환경별 아티팩트 획득률 비교 분석

먼저 4.2절의 실험결과를 바탕으로 각 운영환경에서의 아티팩트 획득률을 분석함으로써 아티팩트의 종류 및 내용 측면의 차이점을 첫 번째 차분 특성으로 도출하였다. 총 25개의 사용자 행위 테스트 데이터 세트로부터 획득된 아티팩트를 확인한 결과는 표 15와 같이 윈도우즈에서 18개의 아티팩트를 획득하여 72%의 획득률을 나타냈으며 안드로이드의 경우 21개의 아티팩트 획득으로 84%의 획득률을 보였다. 반면, 윈도우즈 및 안드로이드 아티팩트를 종합한 결과 23개, 92%의 획득률을 보였다. 이를 통해 양 운영환경의 아티팩트를 종합적으로 활용하는 것이 단일 운영환경에 비해 증거의 다양성을 높일 수 있다는 것을 알 수 있었다.

특히, 이 결과는 두 운영환경의 아티팩트를 종합

Table 2. Comparison of the Artifact acquisition rate on Windows and Android

Test data set of User Behaviors		Artifacts acquisition		
		Windows	Android	Win+And
[1] Install	① Application Download	X	○	○
	② Version information	○	○	○
	③ Installation	○	○	○
[2] Login / Account & Profile	④ Login – Time	○	○	○
	⑤ Login – Account	○	○	○
	⑥ Profile – Country	○	○	○
	⑦ Profile – Birthday	X	X	**X**
	⑧ Profile – Company name	○	○	○
	⑨ Profile – Nick name	○	○	○
	⑩ Profile – Real nane	○	○	○
	⑪ Profile – Phone number	X	○	○
	⑫ Profile – Email address	○	○	○
	⑬ Profile – Profile Image	○	○	○
[3] Chat (Message)	⑭ Workspace – Team info	○	○	○
	⑮ Workspace – Channel info	○	○	○
	⑯ Workspace – Add member	○	○	○
	⑰ Message – Text Chatting	○	○	○
	⑱ Message – Message bookmark	X	○	○
[4] File	⑲ File – Send	○	X	○
	⑳ File – Receive	X	○	○
	㉑ File - Save	○	○	○
[5] Call	㉒ Call	X	○	○
	㉓ Group Call (Meeting)	○	○	○
[6] Log out	㉔ Log out	X	X	**X**
[7] Uninstall	㉕ Application Uninstall	○	X	○
Total number of acquired data (Acquisition rate)		18 (72%)	21 (84%)	**23 (92%)**

하였을 때의 획득률이 단순히 윈도우즈와 안드로이드에서의 각 획득률 중에서 높은 획득률로 수렴하는 값이 아니라 기존 단일 운영환경에서의 높은 획득률 보다도 더욱 증가된 획득률을 새로이 갖게 된다는 점에 의의가 있다. 이는 두 운영환경에 존재하는 아티팩트의 종류 및 내용(데이터)에 차이로부터 기인하는 것으로 어느 한쪽에만 존재하는 아티팩트는 다른 운영환경에서 획득하지 못한 증거의 부족을 보완할 수 있도록 하거나 또는 추가적인 단서를 제공함으로써 수사에 도움을 줄 수 있다는 것을 의미한다. 이러한 차이점은 결과적으로 법증 확보에 필요한 더욱 다양한 정보들을 획득할 수 있도록 도울 수 있는데 예를 들어 윈도우즈 아티팩트에서는 주고 받은 메시지와 관련하여 단순히 대화시간 및 메시지 내용 등의 정보를 확인할 수 있지만 안드로이드의 데이터베이스 아티팩트에서는 특정 메시지를 저장해두는 bookmark 기능에 대한 흔적을 담고 있으므로 이를 통해 용의자가 저장해둔 중요 메시지를 확인하고 추가적인 법증을 수사하는데 활용될 수 있다.

이와 같은 결과는 다양한 운영환경을 동시에 지원하는 플랫폼 활용과 이에 대한 포렌식 분석의 중요성이 높아지고 있는 상황에서 운영환경으로부터 비롯되는 아티팩트의 차이점을 명확히 인식해야 함이 필수적일 뿐만 아니라, 이러한 차이점이 곧 차분 포렌식을 바탕으로 아티팩트가 갖는 특성정보(characteristics), 내용, 종류에 대한 다양성을 높일 수 있는 키포인트라는 점을 의미한다. 또한, 높아진 증거의 다양성은 곧 법증 확보와 재구성에 필요한 증거의 활용성을 높일 수 있게 된다. 이 같은 증거의 다양성 및 활용성 증대는 궁극적으로 디지털 증거의 신뢰성을 제고를 위한 근간이 될 수 있다는 점에서 가치가 있다.

4.3.2 활용방안 제시 : 분석 기법 및 수사활용 시나리오

본 항에서는 두 운영환경에서의 아티팩트를 종합적으로 활용하여 수사 효율을 높일 수 있는 방안으로써 협업 툴 분석기법 및 수사활용 시나리오를 제시한다. 먼저, 파일 형식 및 데이터 포맷에 기반한 아티팩트의 직관성을 두 번째 차분 특성으로 도출하였고, 여기에서 안드로이드 아티팩트의 직관성을 이용한 협업 툴 포렌식 분석기법을 고안하였다. 이때 직관성이란 가시성과 가독성을 포함하여 얼마나 명료한 분석이 가능한지에 관한 척도를 포함한다. 운영환경의 차이에 따라 윈도우즈 및 안드로이드에서 생성되는 아티팩트는 파일 형식 및 데이터 포맷 등에서 차이점이 존재하게 되는데 윈도우즈 아티팩트의 경우 데이터가 Hexadecimal로 기록되며 변환시에도 정형화되지 않은 구조를 지닌 Regular file로 생성되므로 직관적이지 않고 분석이 쉽지 않다. 하지만 안드로이드의 경우 데이터베이스 파일로 생성되어 각 속성별 테이블 및 컬럼으로 구분되어 기록되기 때문에 상당한 직관성을 제공하며 이를 바탕으로 데이터들이 어떠한 종류와 내용을 의미하는지 비교적 파악이 수월하다. 따라서 협업 툴에서의 아티팩트 분석을 위해서는 Fig. 6와 같이 우선적으로 안드로이드 운영환경에서의 데이터베이스 파일 기반 아티팩트 분석을 통해 각종 Attribute 명칭이나 사용자 식별자(User Identifier), 워크스페이스 및 메시지 객체에 대한 UID(Unique Identifier) 등 중요 값을 획득하고 그 데이터들을 윈도우즈 아티팩트 분석간 keyword로 활용하여 더욱 원활한 분석이 가능하다. 이는 안드로이드 아티팩트의 직관성을 활용하여 윈도우즈 아티팩트의 난독성을 해소함으로써 수사 효율을 높이는데 효과적일 것으로 판단된다.

다음으로 두 운영환경에서의 아티팩트를 비교분석하여 도출된 두 가지 차분 특성을 종합함으로써 상호보완적으로 활용할 수 있는 방안을 현실에서 발생 가능한 가상의 사건 시나리오로 작성하여 제시한다.

(사건 개요)

A 방산기업에서 기밀유출 사건이 발생하여 수사를 진행하던 중 관련 개발을 담당했던 박 대위가 유력한 용의자로 지목되어 사무실 압수수색 중이다. 한편, A 기업에서는 비대면 근무 확산에 따라 협업 툴 Teams를 도입하여 활용 중이었으나 박 대위의 PC 및 스마트폰에는 협업 툴 애플리케이션 및 관련 파일이 존재하지 않는다는 특이정황을 포착하여 포렌식 분석을 진행하려 한다.

(사건 분석)

① 윈도우즈에서만 획득 가능한 아티팩트 활용

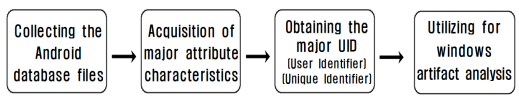


Fig. 6. An efficient collaboration tool analysis procedure utilizing the intuitiveness of Android artifacts

(애플리케이션 삭제 흔적) : 수사관은 박 대위의 PC를 조사하던 중 Teams 디렉터리에 존재하는 '.dead' 파일을 발견하였다. 이는 Teams 애플리케이션을 삭제 후에 남게 되는 흔적 파일로써 사용자가 애플리케이션을 사용하였으며 2020.10.14. 22:12에 의도적으로 삭제하였음을 확인하였다. 또한, 이를 바탕으로 스마트폰에서도 사용했을 가능성을 염두에 두고 안드로이드 포렌식 분석을 수행한 결과 localappstate.db 파일의 'appstate' 테이블에서 Unix Time 형식의 'install_request_timestamp_ms'를 발견, 한국 표준시인 UTC+9를 적용하여 변환한 결과 2020.10.14. 18:11의 설치시각 및 경로 등 설치 흔적을 확인할 수 있었다. (Fig. 7)

② 안드로이드에서만 획득 가능한 아티팩트 활용(프로필 정보) : '①'에서의 설치 흔적 확인을 통해 파일 복원을 수행하여 PC와 스마트폰 모두에서 대부분 파일을 복원하였다. 이후 윈도우즈에서 협업 툴 아티팩트를 분석하던 중 [0-9]{6}.log 파일로부터 계정ID 및 메일주소가 'militaryspy77@gmail.com'이고 실명 'Park Ho', 닉네임 'Captain Park' 등 사용자 계정 및 프로필 정보를 대부분 획득할 수 있었다.(Fig. 8)

하지만 윈도우즈 아티팩트 분석간 박 대위와 대화에 참여한 상대방 프로필 정보 확인을 위해 Attribute가 'guest'인 기록을 분석한 결과 상대방 계정이 'industrialspy99@gmail.com'라는 것 외에 별다른 정보를 획득하지 못하였는데 안드로이드 'SkypeTeams.db' 파일의 'User' 테이블로부터 앞서 획득한 이메일 주소를 매칭시켜 분석한 결과 Fig. 9과 같이 상대방

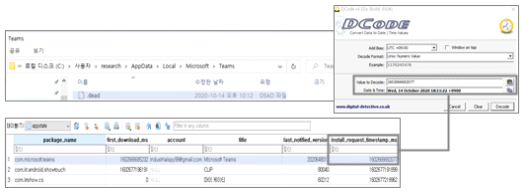
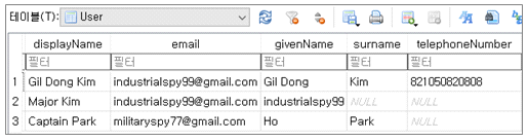


Fig. 7. Artifact of application deletion on Windows → Used for Android analysis

Fig. 8. Obtaining user account and profile information on Windows Artifacts



테이블(T): User

	displayName	email	givenName	surname	telephoneNumber
	필터	필터	필터	필터	필터
1	Gil Dong Kim	industrialspy99@gmail.com	Gil Dong	Kim	821050820808
2	Major Kim	industrialspy99@gmail.com	industrialspy99	NULL	NULL
3	Captain Park	militaryspy77@gmail.com	Ho	Park	NULL

Fig. 9. Complementing guest profile information that is restricted from obtaining in Windows with Android analysis

참여자는 displayName 컬럼이 'Major Kim'(닉네임), surname 및 givenName 컬럼이 'Kim Gil Dong'(실명), telephoeNumber(휴대전화 번호) 컬럼이 '821050820808'인 사용자로 실명 및 휴대전화 정보를 조회하여 방위산업스파이 용의자 중 한명임을 확인할 수 있었다.

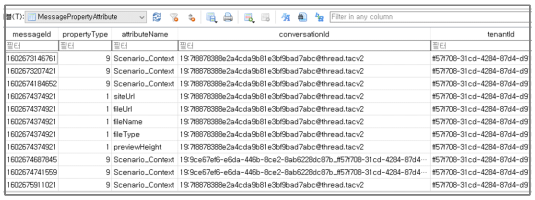
③ 윈도우즈와 안드로이드 아티팩트를 종합하여 범증 재구성(대화 및 파일 전송) : 안드로이드 'SkypeTeams.db' 데이터베이스 User 테이블에서 Fig. 10과 같이 사용자의 UID(User Identifier) 값을 저장하는 mri 컬럼으로부터 두 사용자 각각의 값을 획득하였다. 앞 8자리가 'ff57f708-'인 mri는 닉네임 'Major Kim'의 고유 식별자이고 '9ce67ef6-'인 값은 'Captain Park'의 고유 식별자임을 알 수 있다.

MesssagePropertyAttribute 테이블에서 tenantId 값이 'ff57f708-' 므로 대화가 이루어진 워크스페이스를 생성한 사용자는 'Major Kim'임을 알 수 있다. conversationId는 대화별로 부여되는 Unique Identifer로써 본 연구에서는 공개 채널에서의 대화와 개인간 대화로 구분하여 실험하였으므로 Fig. 11과 같이 2가지 값이 생성되었다. 개인간 대화의 conversationId는 두 사용자의 mri 값이 결합되는 형식으로 기록된다. 또한, propertyType 및 attributeName 컬럼을 통해 각 대화 내에서 일반 텍스트 기반의 대화 및 파일전송이 이루어졌음을 알 수 있다.

그리고 여기서 획득한 messageId는 사용자의 대화 및 파일전송 등 메시지 개체별로 부여되는 UID

mri	displayName
필터	필터
8:orgid:ff57f708-31cd-4284-87d4-d9101266e0ab	Major Kim
8:orgid:9ce67ef6-e6da-446b-8ce2-8ab6228dc87b	Captain Park

Fig. 10. Obtaining user identifier and nickname information from 'user' table



messageId	propertyType	attributeName	conversationId	tenantId
1602673146761	9	Scenario_Context	19:7f8878388e2a4cda9b81e3bf9bad7abc@thread.tacv2	ff57f708-31cd-4284-87d4-d9
1602673207421	9	Scenario_Context	19:7f8878388e2a4cda9b81e3bf9bad7abc@thread.tacv2	ff57f708-31cd-4284-87d4-d9
1602674184652	9	Scenario_Context	19:7f8878388e2a4cda9b81e3bf9bad7abc@thread.tacv2	ff57f708-31cd-4284-87d4-d9
1602674374921	1	siteUrl	19:7f8878388e2a4cda9b81e3bf9bad7abc@thread.tacv2	ff57f708-31cd-4284-87d4-d9
1602674374921	1	fileUrl	19:7f8878388e2a4cda9b81e3bf9bad7abc@thread.tacv2	ff57f708-31cd-4284-87d4-d9
1602674374921	1	fileName	19:7f8878388e2a4cda9b81e3bf9bad7abc@thread.tacv2	ff57f708-31cd-4284-87d4-d9
1602674374921	1	fileType	19:7f8878388e2a4cda9b81e3bf9bad7abc@thread.tacv2	ff57f708-31cd-4284-87d4-d9
1602674374921	1	previewHeight	19:7f8878388e2a4cda9b81e3bf9bad7abc@thread.tacv2	ff57f708-31cd-4284-87d4-d9
1602674687845	9	Scenario_Context	19:9ce67ef6-e6da-446b-8ce2-8ab6228dc87b_ff57f708-31cd-4284-87d4-	ff57f708-31cd-4284-87d4-d9
1602674741559	9	Scenario_Context	19:9ce67ef6-e6da-446b-8ce2-8ab6228dc87b_ff57f708-31cd-4284-87d4-	ff57f708-31cd-4284-87d4-d9
1602675911021	9	Scenario_Context	19:7f8878388e2a4cda9b81e3bf9bad7abc@thread.tacv2	ff57f708-31cd-4284-87d4-d9

Fig. 11. Obtaining UID values per chat space and message object

이며 이 값을 이용하여 'Message' 테이블에서 대화 내용이 기록된 'content' 테이블과 매칭시켜 대화 내용을 구성할 수 있다. messageId는 전송 시간을 바탕으로 Unix Time 포맷으로 기록되므로 표준시인 UTC 기준으로 변환하면 각 메시지의 전송 시각을 획득할 수 있다. 앞서 설명한 User, Message, MessagePropertyAttribute 테이블에서 획득 가능한 값들을 Fig. 12와 같이 매칭시키는 분석을 통해 어느 사용자(프로필 정보)가 어떠한 공간(워크스페이스 정보)에서 어떤 내용의 대화(혹은 파일전송)가 이루어졌는지 타임라인을 구성하여 범증을 재구성할 수 있게 된다.

V. 결 론

본 연구에서는 언택트 시대에 활용도가 급증하고 있는 협업 툴 Microsoft Teams를 대상으로 디지털 포렌식 관점에서 시나리오 기반의 사용자 행위에 따라 애플리케이션 사용시 생성 및 저장되는 데이터의 종류와 내용, 특성 등 유의미한 아티팩트를 분석하고자 하였다. 또한, 단순 아티팩트 분석에서 한 걸음 더 나아가 여러 운영환경을 지원하는 플랫폼 타입 애플리케이션이 갖게 되는 운영환경별 아티팩트 차이점에 기인하여 차분 포렌식 개념을 제안하고 윈도우즈 및 안드로이드에서의 아티팩트를 종합적으로 활용하는 것이 단일 운영환경에 국한된 아티팩트 분석에 비하여 증거의 다양성과 활용성을 높임으로써 더욱 효율적인 수사에 기여할 수 있음을 증명하였다.

본 연구 결과는 비대면 시대를 맞아 점차 증대되는 협업 툴 사용간 발생 가능한 디지털 범죄 및 사고 위협에 선제적으로 대응하고 실제 수사시 협업 툴 아티팩트 분석에 있어 효과적으로 활용 가능할 것으로 기대된다.

향후에는 보안기능 강화를 위해 애플리케이션 데이터를 암호화하는 협업 툴이 증가되고 있는데 이를 위한 분석기법 연구가 필요할 것이며, 다양한 협업 툴이 등장하는 가운데 국가별로 선호도가 높은 협업 툴 애플리케이션이 상이한데 국가별로 시장 점유율을 고려하여 분석 가치가 높은 협업 툴에 대한 선제적인 연구를 수행한다면 이와 관련한 디지털 수사에 기여할 수 있을 것이다.

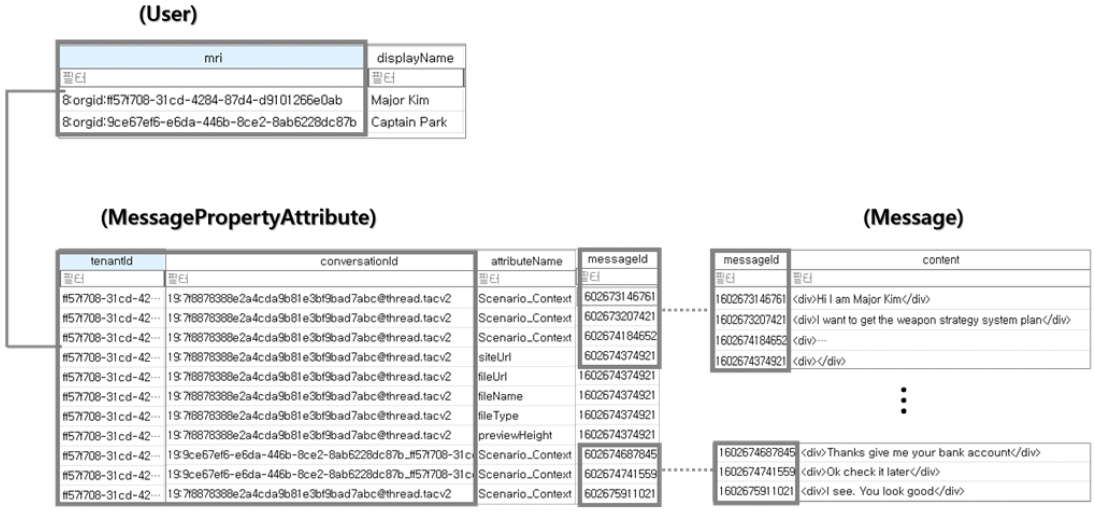


Fig. 12. Organize timeline by connecting key information acquired from user and message tables

References

[1] Mahajan, A. and Dahiya, M. S., & Sanghvi, H. P, "Forensic analysis of instant messenger applications on android devices," arXiv preprint arXiv, 1304.4915, Apr. 2013

[2] Thakur, N. S, "Forensic analysis of WhatsApp on Android smartphones," University of New Orleans Theses and Dissertations. 1706, Aug. 2013

[3] Jongcheol Yoon and Yongsuk Park, "Forensic Analysis of KakaoTalk Messenger on Android Environment," JKIICE, 20(1), pp. 72-80, Jan. 2016

[4] Yang, T. Y. and Dehghantanha, A. and Choo, K. K. R. and Muda, Z, "Windows instant messaging app forensics: Facebook and Skype as case studies," PloS one, 11(3), e0150300, Mar. 2016

[5] Seunghee Seo and Gihoon Nam and Yeog Kim and Changhoon Lee, "Artifacts Analysis of User s Behavior in Korea Random Chat Application." Journal of Digital Forensics, 12(3), pp. 1-7, Dec. 2018

[6] Shin, S. and Park, E. and Kim, S. and Kim, J, "Artifacts Analysis of Slack and Discord Messenger in Digital Forensic," Journal of Digital Contents Society(J. DCS), 21(4), 799-809, Apr. 2020

[7] Ababneh, A. and Awwad, M. A., and Al-Saleh, M. I, "IMO forensics in android and windows systems," 2017 8th International Conference on Information, Intelligence, Systems & Applications (IISA), pp. 1-6, IEEE, Aug. 2017

[8] Scrivens, N. and Lin, X, "Android digital forensics: data, extraction and analysis," Proceedings of the ACM Turing 50th Celebration Conference-China pp. 1-10, May. 2017

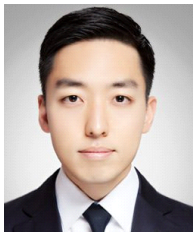
[9] Garfinkel, S. and Alex J. Nelson and Joel Young. "A general strategy for differential forensic analysis." Digital Investigation, pp. S50-S59, Aug. 2012

[10] TWRP, https://twrp.me/about/, Dec. 2020

[11] Odin. https://odindownload.com/, Dec. 2020

[12] Lee, J., Lee, Y., Jin, M., Kim, J., & Hong, J, "Analysis of application installation logs on Android systems," In Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing, pp. 2140-2145, Apr. 2019

〈저자소개〉



김 영 훈 (Young-hoon Kim) 학생회원
2009년 2월: 육군3사관학교 전산정보처리학과 졸업
2019년 3월~현재: 연세대학교 정보대학원 석사과정
〈관심분야〉 정보보호, 디지털포렌식 등

권 태 경 (Taekyoung Kwon) 종신회원
1992년 2월: 연세대학교 컴퓨터과학과 학사
1995년 2월: 연세대학교 컴퓨터과학과 석사
1999년 8월: 연세대학교 컴퓨터과학과 박사
1999년~2000년: U.C. Berkely Post-Doc
2001년~2013년 8월: 세종대학교 컴퓨터공학과 교수
2007년~2008년: Univ. Maryland at College Park 교환교수
2013년 9월~현재: 연세대학교 정보대학원 교수
〈관심분야〉 암호프로토콜, Usable Security, 소프트웨어/시스템보안, 기계학습과보안 등