https://doi.org/10.33778/kcsa.2023.23.3.037

# 메타버스 플랫폼 Roblox 포렌식을 통한 아티팩트 분석

최 이 슬*, 조 정 은**, 이 은 빈**, 김 학 경***, 김 성 민***

## 요 약

코로나19로 인한 비대면 환경 수요 증가와 블록체인, NFT 등 기술의 발전으로 메타버스의 성장이 가속화되고 있다. 그러나 다양한 메타버스 플랫폼의 등장으로 사용자가 증가함에 따라, 메타버스 내에서 랜섬웨어 공격, 저작권 침해, 성범죄 등 범죄 사례가 발생하고 있다. 이로 인해 메타버스 시스템 내에서 디지털 증거로 활용 가능한 아티팩트의 필요성이 높아지고 있다. 그러나 메타버스 솔루션에 대한 표준화된 포렌식 절차가 부재하며, 메타버스 포렌식을 위한 아티팩트에 대해서도 알려진 정보가 없다. 또한, 보안성 평가 및 포렌식 분석 뿐만 아니라 관련 제도나 가이드라인 역시 미비하여 포렌식에 어려움이 있다. 이에 본 논문은 대표적 메타버스 게임 솔루션인 Roblox에 대한 동적 분석을 통해 사용자의 행위 분석 및 타임라인 분석에 활용 가능한 아티팩트를 제시한다. 메모리 포렌식 및 로그 분석으로 파악한 아티팩트 간 연계를 통해 메타버스 범죄 시나리오에서의 활용 가능성을 제시하고, 현행 법률 및 규정에 대한 검토를 통해 제도적 미비점을 분석하여 개선 방안을 제언한다.

# Metaverse Artifact Analysis through the Roblox Platform Forensics

Yiseul Choi*, Jeongeun Cho**, Eunbeen Lee**, Hakkyong Kim***, Seongmin Kim***

## ABSTRACT

The growth of the metaverse has been accelerated by the increased demand for non-face-to-face interactions due to COVID-19 and advancements in technologies such as blockchain and NFTs. However, with the emergence of various metaverse platforms and the corresponding rise in users, criminal cases such as ransomware attacks, copyright infringements, and sexual offenses have occurred within the metaverse. Consequently, the need for artifacts that can be utilized as digital evidence within metaverse systems has increased. However, there is a lack of information about artifacts that can be used as digital evidence. Furthermore, metaverse security evaluation and forensic analysis are also insufficient, and the absence of attack scenarios and related guidelines makes forensics challenging. To address these issues, this paper presents artifacts that can be used for user behavior analysis and timeline analysis through dynamic analysis of Roblox, a representative metaverse gaming solution. Based on analyzing interrelationship between identified artifacts through memory forensics and log file analysis, this paper suggests the potential usability of artifacts in metaverse crime scenarios. Moreover, it proposes improvements by analyzing the current legal and regulatory aspects to address institutional deficiencies.

**Key words : Metaverse, Digital Forensics, Roblox, Forensic Artifacts**

접수일(2023년 08월 17일), 게재확정일(2023년 09월 10일)

* 성신여자대학교 융합보안공학과(주저자)
** 성신여자대학교 융합보안공학과(공동저자)
*** 성신여자대학교 융합보안공학과(공동교신저자)

# 1. 서 론

코로나19로 인한 비대면 환경 수요 증가 및 블록체인, NFT 등과 같은 메타버스 구현 기술의 발전에 따라 메타버스 기술의 성장이 가속화되고 있다. 현실 세계와 유사한 환경을 제한 없이 구현할 수 있는 특성으로 인해, 메타버스는 특정 분야에 한정되지 않고 게임을 비롯한 엔터테인먼트, 교육, 사업 등 다양한 분야에서 활용되고 있다. 이렇듯 메타버스는 사용 목적에 따라 많은 서비스를 제공하며, 다양한 플랫폼이 존재한다. 메타버스 플랫폼의 예로는 타인과 사회적 교류를 하는 커뮤니티가 주목적인 Ifland, ZEPETO, 게임이 주목적인 Roblox와 Minecraft, 그리고 경제적 이익 창출을 추구하는 Gather, Earth 2 등이 있다[1].

다양한 플랫폼의 등장으로 메타버스의 사용자가 급증하면서 메타버스 내에서 랜섬웨어 공격, 저작권 침해, 성범죄와 같은 범죄가 발생하고 있다[2, 3]. 실제 메타버스 플랫폼 중 하나인 ZEPETO에서 한 사용자가 다른 사용자로부터 성착취물을 요구당한 사례가 있다[2]. 메타버스를 사용하는 주 연령층에 미성년자가 포함된다는 점을 고려하면 범죄의 중대성이 크다. 또한, 메타버스 플랫폼을 업무 공간으로 활용하고자 하는 기업이 증가하면서, 메타버스가 업무 공간을 대체하게 될 시 산업기밀 유출과 같은 범죄 역시 발생할 수 있다. 실제로, 지멘스 메타버스 내에서 기업 정보 유출 사건이 발생한 사례가 최근 발생하였다[4]. 따라서, 이러한 범죄에 대한 효율적인 수사를 위해 메타버스 시스템 내에서 디지털 증거로 활용될 수 있는 아티팩트의 필요성이 높아지고 있다.

메타버스 플랫폼은 대부분 정보가 공개적인 오픈소스 기반이 아닌 상용 솔루션이기 때문에, API나 data format과 같은 자세한 정보들이 인터넷상에 공개되어 있지 않다. 또한 Microsoft Teams와 같이 난독화 기능을 제공하는 일부 솔루션들도 존재한다[5]. 이렇듯, 공개된 정보가 한정적이기 때문에 메타버스 솔루션을 분석하는 과정은 blackbox test 형태로 이루어질 수밖에 없다. 또한, 메타버스는 기술에 대한 보안성 평가 및 포렌식 관점에서의 충분한 분석이 이루어지지 않아 사용할 수 있는 아티팩트도 알려진 것이 충분하지 않다. 그뿐만 아니라, 사례 연구를 위한 공격 시나리오도 구체적으로 정립되어 있지 않으며, 관련 법적 제도나 가이드라인 역시 미비해 포렌식 절차가 정형화되어 있지 않다[6]. 지속해서 발생하는 메타버스 관련 범죄를 어떻게 처벌할 것인지에 대한 논쟁이 이루어지고 있지만, 관련 법령 및 제도를 수립하기 위해서는 메타버스 포렌식을 위한 아티팩트 분석 및 사례 연구가 필수적으로 선행되어야 한다.

이에 본 논문에서는 메타버스 플랫폼 중 하나인 Roblox에 대한 포렌식 관점에서의 아티팩트 수집을 위한 기술적 분석을 수행한다. 구체적으로, 메모리 포렌식과 로그 분석을 통해 사용자 식별 및 타임라인 추적에 활용할 수 있는 아티팩트를 찾아 제시하고자 한다. 특히, 아티팩트와 데이터 간의 연계에 대해 분석하고 해당 정보를 바탕으로 아티팩트 활용 시나리오를 사례 연구를 통해 제안한다. 끝으로, 메타버스 관련 현행 법률 및 제도에 대한 고찰을 통해 미비점을 분석하고 이에 따른 개선 방안을 제언한다.

# 2. 이론적 배경

## 2.1 메타버스 정의 및 활용 사례

메타버스는 현실 세계가 가상공간과 결합하여 사회 전반의 활동과 생활이 가상공간에서도 구현된다는 개념으로, 증강현실과 가상 세계가 서로 연결되어 공통으로 공유하는 공간을 통해 몰입형·실감형 체험을 제공한다[7]. 메타버스는 제공하는 서비스 및 플랫폼의 활용 목적에 따라 크게, 1) 사회관계 형성(SNS), 2) 디지털 자산 거래(Market), 3) 원격협업 지원(Assistant) 유형으로 분류할 수 있다. 각 서비스 모델 유형에 대한 대표적 상용 플랫폼들은 아래 < 표 1 >과 같다.

< 표 1 > 메타버스 유형에 따른 플랫폼

| 메타버스 유형 | 플랫폼 |
|---|---|
| 사회관계 형성(SNS) | Roblox, ZEPETO, Minecratf, Fortnite |
| 디지털 자산 거래(Market) | Decentraland, Earth2, Sandbox |
| 원격협업 지원(Assistant collaboration) | Mesh, Nvidia omniverse |

첫 번째, 사회관계 형성 유형은 오프라인 공연의

대체재로써 메타버스를 가장 적극적으로 활용하며 자신을 표현하는 아바타를 통해 현실 세계에서와 같은 만남과 소통 등이 가능해 새로운 사회관계를 형성할 수 있으며, 대표적인 플랫폼으로는 Roblox, ZEPETO 등이 있다. 두 번째, 디지털 자산 거래 유형은 메타버스 플랫폼 내에서 디지털 굿즈나 게임 아이템과 같은 가상 상품 및 가상 부동산 등의 거래를 통해 경제적 수익을 창출케 하며, 대표적인 플랫폼으로는 Sandbox, Decentraland 등이 있다. 마지막으로, 원격협업 지원 유형은 원격 의사소통 및 협업 공간 제공 등을 통해 원격 업무 환경에서의 업무 효율성을 증가시키며, 대표적인 플랫폼으로는 Mesh, Nvidia omniverse 등이 있다[8].

코로나19의 확산으로 인해 메타버스 기반 솔루션은 다양한 산업 분야에서 활용되고 있다. 구체적으로, 게임 분야에서는 Roblox와 같은 메타버스 플랫폼을 통해 캐주얼 게임부터 MMO RPG까지 다양한 게임이 출시되고 있으며, 교육 분야에서는 가상현실 체험과 같은 새로운 방식의 교육이 이루어지고 있다. 메타버스를 활용한 가상현실 교육은 실제로 체험하기 어려운 역사적인 사건이나 지리적인 지역의 체험이 가능하다. 정치 분야에서는 제46대 미국 대통령 선거와 제20대 대통령 선거운동에 메타버스가 활용된 사례[9, 10]가 있으며, 엔터테인먼트 분야에서는 가상 콘서트, 가상 전시회 등이 진행된다. 또한, 비즈니스 분야에서는 3D 모델링을 이용한 제품 설계 및 시뮬레이션 등이 이루어지고 있다.

## 2.2 디지털 포렌식 아티팩트

디지털 포렌식에서의 아티팩트란, 운영체제나 애플리케이션을 사용하면서 자동으로 생성되는 흔적을 의미한다[11]. 예를 들어 윈도우즈 운영체제 경우 프리패치, 점프목록, 이벤트 로그, 레지스트리 등이 아티팩트에 해당한다. 아티팩트 분석을 통해 응용프로그램의 마지막 실행 시각과 같은 실행 정보나 정보 유출 흔적을 파악할 수 있다. 나아가, 데이터 유출이나 악성코드 감염과 같은 침해사고의 효과적인 조사 및 분석을 할 수 있다. 수사적 관점에서 아티팩트는 디지털 환경에서 발생한 활동에 대한 증거로 사용될 수 있으며, 아티팩트 간의 연계 분석을 통해 사용자의 행위 분석 및 타임라인에 따른 사건 경과에 대한 상세 파악이 가능하다. 이와 같이 아티팩트는 디지털 포렌식 분야에서 필수 불가결하게 사용되는 개념이며 증거물로 활용 가능하므로 본 연구에서는 메타버스 포렌식을 위한 아티팩트 수집 및 분석을 진행하고자 한다.

## 2.3 메타버스 보안 및 포렌식 선행연구

메타버스 플랫폼의 활용 사례가 다변화되고 다양한 서비스가 등장함에 따라, 메타버스에서 발생할 수 있는 보안 이슈 및 범죄 시나리오에 관한 연구가 활발히 이루어지고 있다. Yuntao Wang 외 6명[12]은 메타버스 기술 개요, 보안 및 프라이버시 이슈에 대한 분석을 수행하였다. 동 연구에서는 새로운 분산 메타버스 아키텍처와 3원 세계 상호작용을 통한 주요 특성을 조사하고, 메타버스 상의 보안 및 프라이버시 위협에 대한 대응책을 제시하였다. Yang-Wai Chow 외 4명[13]은 시각화 기술과 관련한 메타버스의 사이버 위협 및 관련 연구를 조사하였다. 동 연구에서는 시각화 기술의 사용으로 인증 및 ID 문제, 개인정보보호 문제, 스토킹 등의 사회 문제, 몰입형 공격과 같은 물리적 위협이 야기될 수 있으며 XR 인증, AI 기반 보안 등의 연구가 이루어져야 함을 제시하였다.

김정화 외 2명[14]은 가상현실 공간에서 발생 가능한 성폭력 범죄 유형화를 통해 현행 법체계의 한계를 분석하고 유형별로 대안을 제시하였다. 동 연구는 현행법으로 규율 가능한 범죄 유형과 불가능한 범죄 유형으로 분류 후 관련 법안의 개정 방향과 판단 근거 등을 제시하였다. 남완우 외 1명[6]은 메타버스 내에서 발생하는 범죄를 성폭력 범죄, 신종폭력, 지식재산권 침해 및 사기 범죄, 자금 세탁으로 분류하였으며 경찰의 치안전략 및 범죄예방 활동 수립, 법제도 개선 등을 통한 법에 따른 제재의 필요성을 제시하였다.

앞서 언급한 선행 연구들은 메타버스 플랫폼 전반에 대한 보안성 분석에 그치는 수준이며, survey 논문의 특성상 실제 사용 메타버스 솔루션의 분석을 바탕으로 한 포렌식 방법론 및 아티팩트 도출을 위한 기술적 방안 및 수집 절차에 대한 연구가 부재하다.

메타버스 포렌식과 관련된 선행 연구로, Jaehyoung Park 외 4명[15]은 메타버스 환경에서 사용 가능한 몰입형 콘텐츠의 저작권 보호를 위한 포렌식 워터마크

를 제안하였다. 이러한 연구에서 제안된 포렌식 워터마크는 심층 신경망(DNN), 다중 히든 레이어로 구성되며 저작권자, 최초 구매자, 최종 구매자, 현재 사용자의 아이디, 콘텐츠 유통 경로 등의 정보를 포함한다.

박윤지 외 1명[16]은 메타버스 내 범죄 대응에 관한 연구 동향을 파악하고 메타버스 포렌식에서 고려해야 할 사항을 제시하였다. 동 연구에서는 VRChat 플랫폼과 Roblox 플랫폼의 저장매체 로그 및 메모리 분석을 수행하였다. 저장매체 로그 분석을 통해 VRChat 플랫폼 사용자의 계정정보 및 로그인 시각, 행위 결과를 확인하였으며 메모리 분석을 통해 Roblox 사용자의 아바타 이미지, 사용자 ID, PlacedID를 확인하였다.

기존 Roblox 메모리 포렌식을 수행한 선행 연구[16] 또한 메모리 포렌식 아티팩트 수집에만 초점이 맞추어져 있으며, 로그에 대한 분석은 충분히 이루어지지 않았다. 그뿐만 아니라 수집한 아티팩트의 활용 가능성을 제시하지 못하였다는 한계가 존재한다. 본 논문에서는 이러한 기존 연구의 한계를 극복하기 위해 메모리 포렌식 및 로그 분석을 이용하여 다양한 아티팩트 수집을 수행하고 시나리오를 통한 아티팩트 활용 가능성을 제시하고자 한다.

# 3. Roblox 아티팩트 수집 및 분석

## 3.1 연구 대상 및 연구 방법

메타버스 플랫폼에서 사용자의 행위 분석에 활용할 수 있는 아티팩트는 증거로써 수사에 도움이 될 수 있으므로 포렌식 아티팩트의 수집이 필수적이다. 대다수의 메타버스 플랫폼은 내재적인 특성상 인터넷상에서 활동이 이루어지기 때문에 관련 증거 역시 모두 디지털 증거의 형태로 남는다. 메모리 분석은 운영 중인 시스템의 상태를 기록하고 분석하여, 실행 중인 작업, 네트워크 활동, 최근 수행한 명령어와 같은 정보를 확인할 수 있으며, 디스크 암호키, 인젝션 코드, 캐시에 저장되지 않는 웹 브라우징 기록과 같은 디지털 포렌식 수사에 필요한 중요한 데이터를 확보할 수 있다[17]. 따라서 본 논문에서는 실제 메타버스 플랫폼 Roblox의 메모리 분석을 통해 수집 가능한 아티팩트가 무엇인지 확인하고, 이에 대한 활용 가능성을 구체적으로 파악하고자 한다.

Roblox는 메타버스 게임 플랫폼 중 하나로, 월간 사용자가 약 1억 5천만 명으로 많은 사람이 이용하며 실시간 소셜 플랫폼 서비스, 클라우드컴퓨팅 및 협업 인프라를 제공한다[18]. 해당 플랫폼을 통해, 자신만의 아바타를 만들어 사용자끼리 소통하고 자체 화폐인 '로벅스(Robux)'로 거래가 이루어진다. 또한, Roblox Studio를 통해 사용자가 직접 게임을 만들 수 있고 직접 제작한 게임을 다른 사용자와 함께 즐길 수 있다. 하지만 일부 사용자는 자체 제작한 게임의 배포가 가능하다는 탄력성을 악용해 악성코드를 심어 유포하기도 한다[19]. 높은 시장 점유율과 더불어, 잠재적으로 보안 위협 및 사이버 범죄 행위가 발생할 수 있다는 점에서 다양한 메타버스 플랫폼 중 Roblox를 분석 대상으로 선택하였다.

## 3.2 분석환경

아티팩트 수집 및 분석의 경우 Windows 11 Home 22H2 운영 체제가 설치된 LG gram 랩탑 환경(Intel i7-1065G7 CPU 및 16GB 메모리)에서 수행하였다. Roblox player를 통해 멀티 플레이어 모드로 게임을 실행하였으며, 사용자 행위 분석을 위해 텔레포트를 통한 맵 이동 등을 수행하였다. 이후 AccessData FTK Imager을 이용하여 메모리 덤프를 실시하였다. 생성된 메모리 덤프 파일의 데이터를 분석하기 위해 Hex Editor v.2.5를 이용하였고, Roblox 내 자체적으로 생성되는 로그의 경우 Notepad++ v8.4.5로 분석하였다.

## 3.3 메모리 아티팩트 분석

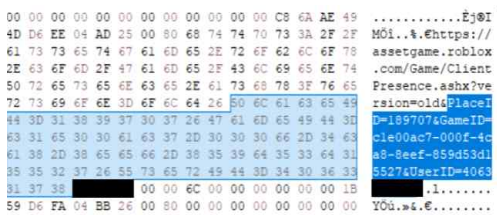
< 표 2 >는 Roblox 플랫폼의 게임을 실행한 후 메모리 덤프 파일과 생성된 로그 분석을 통해 수집한 아티팩트를 정리한 것이다. 먼저 Roblox의 메모리 덤프 파일을 통해 수집한 메모리 아티팩트는 크게 Local 사용자 정보, 타 사용자 정보 그리고 게임 정보로 구분할 수 있다.

Roblox의 경우 사용자별 UserID, 게임별 GameID, 장소별 PlaceID가 존재하며, 각각은 모두 고유한 식별번호이다. User의 정보로는 계정명과 UserID, 게임 정보로는 PlaceID, GameID, 접속 시간이 확인되었다.

< 표 2 > 메모리 덤프 파일과 로그의 아티팩트

| Artifacts | | 설명 | 활용 가능성 | 수집 방식 | |
|---|---|---|---|---|---|
| | | | | Memory dump file | File system log |
| Player Data | Name | 사용자 닉네임 | 용의자 특정 | V | V |
| | UserID | 사용자 고유번호 | | V | V |
| Other Player Data | Name | 사용자 닉네임 | | - | - |
| | UserID | 사용자 고유번호 | | V | - |
| | Number | 게임에 접속한 사용자 수 | 조사 대상 선정 | - | V |
| Game Data | PlaceID | 게임 내 장소 고유 번호 | 용의자 특정 알리바이 입증 | V | V |
| | GameID | 게임 고유 번호 | 접속한 게임 식별 및 알리바이 입증 | V | V |
| | Access Time | 접속 시간 | 타임라인 확인 | V | V |
| Server IP address, Port number | | | - | V | V |

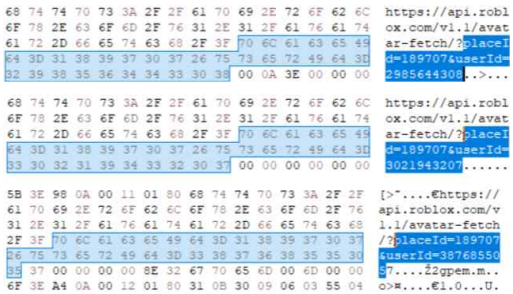
그 외 서버 IP와 포트 번호를 확인할 수 있었지만 타 사용자의 정보는 UserID만 확인할 수 있었다. Roblox Studio에서 하나의 게임에 여러 place의 추가가 가능함을 확인하였고, 이를 바탕으로 place마다 고유의 PlaceID가 배정됨을 확인하였다. 따라서 게임 내에서 장소 이동 시 PlaceID가 변경됨을 알 수 있다.




(그림 1) 메모리 덤프를 통해 획득한 로컬 사용자 관련 아티팩트 (PlaceID, GameID, UserID)

획득한 로컬 사용자 관련 아티팩트 정보는 (그림 1)과 같이 “UserID=40634063178088”, “PlaceID=189707”, “GameID=cle00ac7-000f-4ca8-8eef-859d53d15527” 형태로 나타난다. 해당 아티팩트를 통해 로컬 사용자의 UserID가 무엇인지, 어느 게임에 접속했으며 어떤 장소에 존재했는지에 대한 정보를 파악할 수 있다. UserID와 함께 확인 가능한 PlaceID를 바탕으로, 동일한 PlaceID를 가진 UserID를 찾아내는 것도 가능하다. 이를 통해, 범죄가 발생한 특정 시각에 해당 장소에 접속한 사용자를 추적할 수 있어 용의자 특정에 해당 아티팩트가 활용될 수 있다. 특히, 도출된 로컬 사용자의 PlaceID를 통해 특정 시각에 어느 장소에 접속하였는지 확인할 수 있다는 점에서 알리바이 입증에 유용한 증거로써 활용될 수 있다.

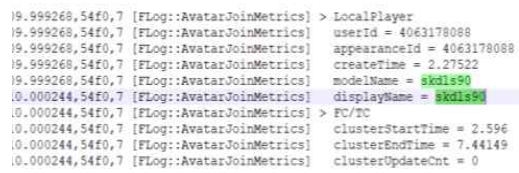
타 사용자들의 UserID와 PlaceID는 (그림 2)와 같다. (그림 2)의 타 사용자들의 아티팩트를 확인해보면 UserID는 모두 다르지만, PlaceID는 동일한 것으로 보아 같은 공간에 존재한 다른 사용자임을 확인할 수 있다. 이를 바탕으로 용의자와 피해자가 같은 메타버스 내 공간에서 동일한 시간에 존재하였음을 입증하는 증거로써 활용 가능하다.



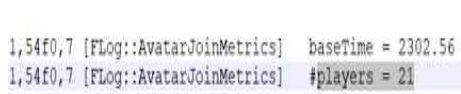

(그림 2) 메모리 덤프 파일 내 타 사용자의 아티팩트(UserID, PlaceID)

### 3.4 로그 분석

Roblox 어플리케이션을 실행할 시에 자체적으로 생성되는 로그 파악을 위해 게임 실행 후 업데이트된 파일을 분석하였으며, 이를 통해 관련 로그가 C:\Users\User\AppData\Local\Roblox\logs 경로에 생성됨을 확인하였다. 해당 파일을 분석한 결과, 확인할 수 있는 아티팩트는 로컬 사용자 정보, 타 사용자 정보 그리고 게임 정보이다. 이러한 정보들은 메모리 덤프 파일의 아티팩트 유형과 큰 범주에서 유사하다. 로컬 사용자의 정보는 계정명, UserID가, 게임 정보는 PlaceID, GameID, 접속 시간이, 그 외의 서버의 IP 및 포트 번호가 확인되었다. 그러나 타 사용자 정보의 경우, 메모리 덤프 파일에 비해 확인할 수 있는 정보가 많지 않았다. Roblox 로그에서는 게임을 실행했을 때 해당 게임의 같은 맵 상에 몇 명의 사용자가 존재하는지만 확인 가능했다. 반면, 메모리 덤프 파일에서는 플레이어의 인원수는 확인할 수 없지만, 로그 파일에서 수집할 수 없었던 타 사용자들의 UserID가 확인되었다.



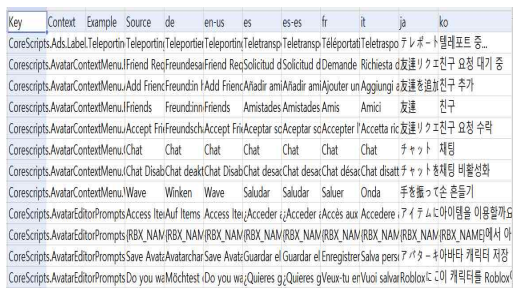

(그림 3) 저장매체 로그 내 User Data




(그림 4) 저장매체 로그 내 참여자 수

(그림 3)은 로그 분석을 통해 수집한 로컬 사용자의 UserID와 계정명, 접속한 GameID, PlaceID와 추가적인 연결 정보를 나타낸다. 또한, 저장매체 로그 분석을 통해 확인할 수 있는 해당 게임에 접속한 사용자 수는 (그림 4)와 같다. 이를 (그림 2)에서의 메모리 포렌식 아티팩트와 연결해보면, 로컬 사용자의 PlaceID와 타 사용자의 PlaceID가 동일하게 189707임을 알 수 있다. 이를 통해 로컬 사용자와 타 사용자들이 같은 공간에 존재했음을 확인할 수 있다. 이러한 분석 예시처럼, 아티팩트 연계를 통해 메타버스 내 발생한 범죄와 관련된 알리바이와 디지털 증거를 확보할 수 있다.

또한, 로그 분석을 통해 사용자 행위 분석에 효과적으로 활용 가능할 것으로 판단되는 Roblox 로그 파일을 추가로 확인하였다. C:\Users\User\AppData\Local\Roblox\Versions\version-ef16b6487a274455\ExtraContent\translations에 존재하는 CoreScriptLocalization.xls 파일은 Roblox 내에서 제공해주는 파일로, Key와 Context를 명시해 사용자가 어떤 행동을 하는지, 무엇을 시도하였는지를 파악하는 데 도움을 준다.




(그림 5) CoreScriptLocalization.xls

(그림 5)는 해당 CoreScriptLocalization.xls 파일의 일부를 나타낸 것이다. 해당 파일을 확인해보면 Key와 Context를 바탕으로 텔레포트, 친구 추가, 채팅, 손 흔들기 등과 같이 사용자의 행위 정보를 활용할 수

있도록 정리한 것을 알 수 있다. 따라서 이를 이용한다면 로그 파일에서 키워드 매칭을 통해 사용자의 행위를 심층적으로 분석할 수 있다.

# 4. Roblox 아티팩트 활용 시나리오

본 장에서는 수집한 아티팩트들이 증거로서의 효용성을 가지는지 판단하기 위해 각 범죄 시나리오를 설정하여 아티팩트를 적용하고자 한다. 아티팩트의 효과성을 정확히 판단하기 위해 실제 범죄 사례를 바탕으로 각색하여 시나리오를 설정하였다. 획득한 아티팩트의 대다수가 게임에 접속한 사용자와 관련된 정보이기에 사용자의 아바타에 직접 피해를 주는 시나리오와 채팅, 게시물 등 게임 내 콘텐츠를 이용하여 피해를 입히는 시나리오로 크게 2가지로 유형화하였다.

## 4.1 아바타에 대한 범죄 시나리오

접근성이 좋고 사용자의 익명성이 보장되는 특성으로 인해 개인의 아바타를 대상으로 하는 스토킹, 성폭력 등의 성범죄의 경우, 피해 사례가 매년 증가하고 있다. 실제로, 메타버스 플랫폼인 호라이즌 월드에서 한 여성의 아바타가 다수의 남성 아바타에게 집단 성폭행을 당한 뒤, 언어적 성희롱 피해를 본 사건이 발생하였다[6]. 해당 사건과 같이 특정 아바타를 향한 스토킹 및 성범죄 사건이 발생할 경우, 범죄 사실을 입증할 수 있는 증거 제시에 제약 사항이 존재한다.

3.1절에서 수집한 아티팩트인 UserID 및 PlaceID를 이용하여 피해자인 로컬 사용자와 동일 시각에 동일한 PlaceID를 가진 UserID를 찾아냄으로써 범죄 발생 시각에 동일한 장소에 존재하였는지를 판단할 수 있다. 이렇게 수집한 정보를 Roblox 서버 내 데이터베이스와 연계하여 용의자를 특정 지을 수 있기에, 해당 아티팩트들이 증거로써 활용될 수 있음을 알 수 있다.

## 4.2 콘텐츠를 이용한 범죄 시나리오

아바타를 대상으로 한 범죄 외에도, 메타버스 플랫폼의 콘텐츠를 이용한 범죄 또한 다수 발생하고 있다. 채팅, 아이템 거래 등 플랫폼에서 제공하는 콘텐츠가 다양하기 때문에 발생하는 범죄 유형 또한 매우 다양하다. 그중 빈번하게 발생하는 범죄인 거래 사기 시나리오에 대해서도 수집한 아티팩트를 활용할 수 있다.

메타버스의 이용자 다수가 10대인 점을 감안하여 14세 미만 아동 또는 청소년일 경우, 보호자의 동의와 실명인증이 우선되어야만 게임 이용 및 유료 결제가 가능하다. 하지만 이러한 규제는 성인 인증 계정을 사고파는 등의 방법으로 우회하면서 거래 사기 피해가 빈번하게 발생한다. 특히 경찰에 접수된 10대 대상 사이버 사기 피해자는 2020년 기준 약 2만 명에 달하였으며 매년 증가하는 추세이다[20]. 실제로, ZEPETO를 사용한 17세 사용자가 계정과 아이템을 거래하면서 300만 원의 사기 피해를 당한 사례가 있다[20]. 위와 같은 거래사기 범죄는 사용자의 익명성으로 인해 구매자와 판매자를 추적하기 어렵다.

거래 사기 등과 같은 콘텐츠 대상 범죄에서도 수집한 아티팩트인 UserID와 PlaceID를 이용하여 추적의 가능성을 높일 수 있다. 거래 당사자에 해당하는 사용자의 UserID와 거래가 이루어진 장소의 PlaceID를 확인하여 일치하는 범죄 용의자를 특정할 수 있다. 나아가 메타버스 플랫폼에서 사용자의 PlaceID 관련 로그를 지속적으로 생성하도록 하고 이를 수집할 수 있다면 추적에 더욱 유용한 증거로써 활용될 수 있다.

# 5. 제도적 미비점 및 제언

## 5.1 메타버스 범죄 사례

본 연구를 통해 수집한 아티팩트 활용을 위한 메타버스 게임 플랫폼 내 범죄 사례 외에도 다양한 메타버스 범죄 유형이 존재한다. 첫째로, 랜섬웨어 공격을 통해 Roblox 시스템을 감염시킨 후 자체 화폐인 '로벅스'를 요구한 사례가 있다. 이는 사용자가 게임을 만들어 배포할 때 랜섬웨어를 심어 유포한 것으로 추정된다[19, 21]. 또한, Roblox 내에서 라이센스 계약 없이 가상 음악 재생 장치를 통해 음악 저작물을 무단으로 이용해 저작권이 침해되기도 했다[22]. ZEPETO에서 아바타가 특정 포즈를 취해 상대 아바타의 신체를 접촉하는 방식으로 성희롱하거나, 쫓아다니며 스토킹하며, 조건만남을 시도하는 사례도 있다[23].

또한, 기업이 업무 공간으로 메타버스를 활용하기 시작하면서 산업기밀 유출 사고의 위험성이 증가하고

있다. 기밀 정보를 복제하여 외부로 유출할 수 있고, 아바타 복제를 통해 다수의 근무지에서 겸직하는 등 예상치 못한 피해가 발생할 수 있다[24]. 그 외에도, 아바타 사칭 범죄의 가능성도 존재한다. 메타버스 내에서는 개인과 기업 등이 아바타로 존재하므로 아바타를 사칭하는 것은 큰 파장을 불러일으킬 수 있다. 더욱이, 정부 기관을 대표하는 아바타를 사칭할 경우 국가적인 피해로 이어질 수 있으며, 기업 공식 아바타를 사칭하여 타 기업과 계약을 맺을 경우 막대한 손실이 발생할 수 있다[25].

### 5.2 제도적 미비점

메타버스 상에서 도박, 사기, 성범죄 등 현실 세계와 비슷한 범죄가 발생함에 따라 이를 처벌해야 한다는 목소리가 점점 설득력을 얻고 있다. 그럼에도 불구하고 메타버스 내 불법행위 처벌에 관한 법률은 상당히 제한적으로 마련되어 있어, 이에 대한 효율적인 대응이 쉽지 않은 상황이다. 현재는 플랫폼 내 자체 규정과 약관에 근거하여 사용자들의 행위를 규제하고 부당한 이득을 취득한 것이 발견되는 경우 활동을 제한하는 정도의 '소극적인' 제재만이 이루어지고 있는 실정이다[26].

국회에서 발의된 주요 메타버스 관련 법안은 메타버스 콘텐츠 진흥에 관한 법률, 메타버스산업 진흥법 2종, 가상융합경제 발전 및 지원에 관한 법률 등이 있다[27]. 해당 법안들은 모두 '자율규제'를 바탕으로 하나, 구체적인 방법에 있어 차이가 있다. 또한, 각 법안은 메타버스 산업 진흥을 목적으로 발의된 법안이며, 메타버스 내 발생하는 범죄 처벌 및 방지를 위한 내용을 중심으로 이루어지지 않았다는 한계가 있다[28]. 메타버스 내 범죄 처벌을 위해 정보통신망 이용촉진 및 정보보호 등에 관한 법률 일부 개정안[29], 과학기술정보통신부의 메타버스 생태계 활성화를 위한 선제적 규제혁신 방안[30] 등이 추진되고 있지만, 메타버스의 정의와 분류 기준조차 마련되어 있지 않아 법안 통과에 어려움을 겪고 있다.

특히, 메타버스는 아동·청소년의 이용 비율이 압도적으로 높고 이들 대상으로 새로운 형태의 성희롱이나 성범죄 발생에 대한 우려가 상당하다. 그러나 현존하는 메타버스 관련 법률에서는 메타버스 내 발생하는 새로운 양태의 성희롱이나 성범죄를 직접적으로 처벌할 수 있는 규정이 명문화되어 있지 않다.

해당 범죄가 아동 또는 청소년을 대상으로 발생한 경우, 「아동·청소년의 성보호에 관한 법률」(이하 '청소년성보호법')상 아동·청소년 성착취물에 관한 정의 규정과 관련 대법원 판례의 취지에 따라 '일부 또는 상당히 제한적으로' 형사법적 대응이 가능하다[14]. 해당 법 제2조 제5호에 따르면, 아동·청소년으로 인식될 수 있는 아바타를 대상으로 법 제2조 제4호 각 목의 어느 하나에 해당하는 행위 또는 그 밖의 성적 행위를 하는 내용을 담은 표현물은 아동·청소년성착취물에 속한다[14]. 또한, 대법원 2019. 5. 30. 선고 2015도863 판결에 따르면, '아동·청소년으로 인식될 수 있는 표현물'이란 사회 평균인의 시각에서 객관적으로 보아 명백하게 청소년으로 인식될 수 있는 표현물을 의미한다[31]. 이와 같은 법률과 대법원 판례의 취지를 종합적으로 고려하면 범죄 대상이 아동·청소년에 한하여 '제한적' 적용이 가능함을 알 수 있다.

하지만, 현행 실정법은 원칙적으로 아날로그(오프라인) 공간을 기반으로 하고 범행의 객체가 자연인을 대상으로 하고 있다. 이러한 상황에서 법인격이 부여되지 않는 아바타를 대상으로 새로운 양태의 범죄가 발생한다면, 아바타 운영 주체가 아동 또는 청소년이 아니거나 기존 구성요건 해당성을 다소 벗어나는 상황에서는 특히나, 청소년성보호법이나 성폭력처벌법 등과 같은 현행 법률을 적극적으로 적용하여 처벌하기가 굉장히 어려울 수밖에 없다[6]. 아날로그 증거와 메타버스에서의 디지털 증거 특성이 달라 기존의 법·제도를 적용하기 어렵고, 디지털 포렌식 수행에 관한 법률 역시 전무하다는 또 다른 한계점도 확인된다. 따라서 메타버스 내 새로운 유형의 범죄를 처벌할 수 있는 법적 및 제도적 보완이 매우 시급하고 필수적이라 할 것이다.

## 6. 결 론

비대면 시장의 수요 증가와 기술의 발전을 기반으로 메타버스 생태계는 급격히 성장하고 있다. 메타버스 시장은 한 분야에 치우치지 않고 문화예술, 교육, 관광 등 다양한 분야로 영역을 넓혀가고 있으며, 나아

가 사용 목적에 맞는 다양한 플랫폼이 생성되고 있다. 그러나, 메타버스 사용자의 급증으로 인한 부작용으로 여러 범죄나 사고가 발생하고 있다. 거래 사기 등과 같은 기존의 사이버 범죄뿐만 아니라 산업기밀 유출, 아바타 복제 등과 같은 새로운 유형의 범죄 등장이 우려된다.

새롭게 나타나는 메타버스 내 범죄의 경우, 기존 범죄들에 비해 증거로써 활용할 수 있는 디지털 증거가 한정적이기 때문에 아티팩트의 획득이 더욱 필수적이다. 이에 아티팩트를 수집하고자 메모리 분석 및 로그 분석을 수행하여 유의미한 아티팩트가 생성됨을 확인하였고, 이를 바탕으로 사용자의 행위 분석 가능 여부와 이후 활용 가능성을 파악하고자 하였다.

본 논문에서는 메타버스 상에서의 디지털 포렌식 분석의 필요성을 제기하고 메타버스 상에서 발생하는 범죄나 사고의 증거로써 활용할 수 있는 아티팩트를 제시하였다. 기존 연구와 달리, 특정 메타버스 플랫폼을 선정해 해당 플랫폼에서 얻을 수 있는 아티팩트의 종류를 확인하고 실제 사례를 각색한 시나리오에 해당 아티팩트를 증거로 적용해봄으로써 아티팩트의 실효성을 확보하였다.

저장매체 로그와 메모리 분석을 통해 도출된 UserID, PlaceID와 같은 아티팩트가 다양한 메타버스 범죄 시나리오에서 활용될 수 있음을 사례연구를 통해 확인하였다. 디지털 포렌식 관점에서 분석한 아티팩트가 향후 메타버스 범죄 및 사고 수사의 효율성 제고를 위해 활용할 수 있다.

끝으로, 메타버스 내에서 발생하는 범죄에 대하여 기존 현행법에 따른 제한적 적용이 아닌 디지털 공간이라는 특수성을 고려한 법적 및 제도적 보완이 이루어진다면 범죄 행위에 따른 적합한 처벌 뿐만 아니라 메타버스 내에 전반적으로 긍정적 영향을 끼칠 것으로 기대한다.

## 참고문헌


[1] 손효림, 이창근, “사용 목적과 체험 방식에 따른 메타버스 플랫폼 유형과 특성에 관한 연구,” 한국디지털콘텐츠학회 논문지, 제23권, 제11호, pp.2181-2190, 2022.

[2] 김효정, “메타버스 파고든 성범죄… 13세 여학생 가장해 들어가 보니,” 조선일보, https://www.chosun.com/national/2022/06/26/QKT7VT43RVATVCCBQRSW6VAXZ4/, (검색일: 2022.11.20.).

[3] 김영명, "'다크버스'가 뭐지? '메타버스'를 악용한 랜섬웨어 등 사기행위의 장", 보안뉴스, https://www.boannews.com/media/view.asp?idx=109374(검색일:2023.03.26.).

[4] "지멘스의 메타버스에서 민감한 기업 정보가 유출돼", 보안뉴스, https://www.boannews.com/media/view.asp?idx=117167, (검색일: 2023.08.04.).

[5] 최두선, “[특징주] 소프트캠프, MS 메타버스 '팀즈' 통합 추진 보안솔루션 공급↑,” 파이낸셜뉴스, https://www.fnnews.com/news/202111171004226661, (검색일: 2022.11.20.).

[6] 송혜진, 남완우, “메타버스 내 범죄발생 유형과 확장성에 관한 연구,” 한국재난정보학회논문집, 제18권, 제1호, pp. 218 - 227, 2022.

[7] 윤경로, “메타버스 표준화 동향,” 한국통신학회지, 제38권, 제9호, pp. 32-38, 2021.

[8] 민경식, 김관영, 박진상, 백종현, 권 혁, 장재동, “메타버스와 NFT, 사이버보안 위협 전망 및 분석,” KISA Insight, Vol. 4, 2022.

[9] 고은경, “'닌텐도 동물의 숲'에 美 바이든은 웃고 日 이시바는 울고,” 한국일보, https://www.hankookilbo.com/News/Read/A2020090911540002114,(검색일:2022.11.20.).

[10] 나호정, “메타버스 선거 유세, 6·1지방선거 등 향후 선거운동 대세될듯,” Ai타임스, http://www.aitimes.com/news/articleView.html?idxno=143401, (검색일: 2022.11.20.).

[11] 이찬진, 정목동, "Window8 관점에서의 디지털 포렌식 분석과 R 을 이용한 소셜 네트워크 관계도 분석 기법", 정보기술융합공학논문지, 제4권, 제2호, pp.19-25, 2014

[12] Y. Wang, Z. Su, N. Zhang, R. Xing, D. Liu, T. H. Luan, X. Shen, "A Survey on Metaverse: Fundamentals, Security, and Privacy," in IEEE Communications Surveys & Tutorials, vol. 25, no. 1, pp. 319-352, 2022.

[13] Y. W. Chow, W. Susilo, Y. Li, . Nguyen, “Visualization and Cybersecurity in the

Metaverse: A Survey", Journal of Imaging, Vol. 9, No. 1, 2023.

[14] 김정화, 김윤식, 차호동, "메타버스 공간에서의 성폭력 범죄와 형사법적 규제에 대한 연구 - 정보통신망 이용촉진 및 정보보호 등에 관한 법률 개정방향을 중심으로 -," 형사법의 신동향, 통권 75호, pp.1-33, 2022.

[15] J. Park, J. Kim, J. Seo, S. Kim, J. H. Lee, "DNN-Based Forensic Watermark Tracking System for Realistic Content Copyright Protection", Electronics, Vol. 12, No. 3, pp. 553, 2023.

[16] 박윤지, 정두원, "메타버스 범죄 동향 및 디지털 포렌식 대응 방안," 한국정보보호학회, 제32권, 제4호, pp. 41-47, 2022.

[17] M. H. Ligh, A. Case, J. Levy, and A. Walters, "The art of memory forensics: detecting malware and threats in windows, linux, and Mac memory.", John Wiley & Sons, pp. 17, 2014.

[18] ITWORLD, "로블록스, 데이터로 보는 2022년 주요 트렌드 공개..."일간 활성사용자수 5,600만," https://www.itworld.co.kr/news/277051#csidx2469261c9b3065fb672e4091c9ed0af(검색일: 2023.03.25.).

[19] 김국배, "메타버스에 빠진 해커? "랜섬웨어 몸값 '로벅스'로 내놔라"", 이데일리, https://www.edaily.co.kr/news/read?newsId=03168486629243752&mediaCodeNo=257, (검색일 : 2023.03.12.).

[20] 오유진, ""성교육 받을래?" 성희롱·사기 판쳐, 무법지대 된 메타버스," 중앙일보, https://www.joongang.co.kr/article/25076642#home, (검색일: 2023.03.25.).

[21] 김가은, ""로블록스도 당했다"…메타버스 노리는 보안 위협," Tech M, https://www.techm.kr/news/articleView.html?idxno=90655, (검색일: 2022.11.20.).

[22] 캐슬린 김, "전미음악출판협회, 로블록스 상대 저작권 침해 소송," 저작권 문화, http://webzine-copyright.or.kr/copyright_2108/7,(검색일: 2022.11.20.).

[23] 오동현, "[메타버스의 그늘, 다크버스①]아바타로 성희롱·스토킹…처벌할 수 있나," Newsis, https://www.newsis.com/view/?id=NISX20220929_0002031869, (검색일: 2022.11.20.).

[24] 전소은, 오예솔, 이일구, "메타버스 내 산업기밀 유출 대응을 위한 정책 및 제도에 관한 연구," 디지털융복합연구, 제20권, 제4호, pp. 377-388, 2022.

[25] 곽중희, "[IT트렌드] 메타버스, 범죄 무법지대 '다크버스' 될 수도 있다", CCTV news, https://www.cctvnews.co.kr/news/articleView.html?idxno=233372, (검색일: 2022.11.20.).

[26] 이혜선, "커지는 '메타버스'…법·제도는 '속수무책'," BIzwatch, http://news.bizwatch.co.kr/article/mobile/2021/11/26/0016, (검색일: 2023.03.25.).

[27] 변인호, "메타버스 산업 진흥 제도, 결국 해넘긴다," IT Chosun, https://it.chosun.com/site/data/html_dir/2022/12/17/2022121700077.html., (검색일: 2023.03.25.).

[28] 박진영, "[IT돋보기]국회 발의 메타버스 관련 법안들 어떻게 다를까," 아이뉴스24, https://www.inews24.com/view/1560239, (검색일: 2023.03.25.).

[29] 이재철, "[단독] 메타버스서 아바타 음란행위·스토킹 시 징역형," 매일경제, https://www.mk.co.kr/news/it/10406689, (검색일: 2023.03.25.).

[30] 윤선영, "메타버스 성범죄 관련 법 만든다…게임과는 영역구분," 디지털타임스, https://www.dt.co.kr/contents.html?article_no=2023030202109931820009, (검색일: 2023.03.25.).

[31] 대법원 2019. 5. 30. 선고 2015도863 판결.

## 〔저자소개〕


최 이 슬 (Yi-seul Choi)
2020년 03월 ~ 현재 성신여자대학교 학사과정

email : dltmf12279@gmail.com

조 정 은 (Jeong-eun Cho)
2020년 03월 ~ 현재 성신여자대학교 학사과정

email : 20200958@sungshin.ac.kr

이 은 빈 (Eun-been Lee)
2020년 03월 ~ 현재 성신여자대학교 학사과정

email : eun3in1ee@gmail.com

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

김 성 민 (Seong-min Kim)
2012년 2월 한국과학기술원 전기 및 전자공학과 졸업
2014년 2월 한국과학기술원 전기 및 전자공학과 석사
2019년 2월 한국과학기술원 정보보호대학원 박사
2019년 9월~2020년 8월 삼성전자 삼성리서치 Staff Engineer
2020년 9월~현재 성신여자대학교 융합보안공학과 조교수

email : sm.kim@sungshin.ac.kr