Digital forensic approaches for metaverse ecosystems

By:
Donghyun Kim, Subin Oh, Taeshik Shon

From the proceedings of
The Digital Forensic Research Conference
DFRWS APAC 2023
Oct 17-20, 2023

Forensic Science International: Digital Investigation 46 (2023) 301608

Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

journal homepage: www.elsevier.com/locate/fsidi

DFRWS 2023 APAC - Proceedings of the Third Annual DFRWS APAC

Digital forensic approaches for metaverse ecosystems

Donghyun Kim [a], Subin Oh [b], Taeshik Shon [a,b,*]

[a] Department of Cyber Security, Ajou University, World cup-ro 206, Suwon, 16499, Republic of Korea
[b] Department of AI Convergence Network, Ajou University, World cup-ro 206, Suwon, 16499, Republic of Korea

ARTICLE INFO

Keywords:
Digital Forensics
Metaverse
Augmented Reality (AR)
Virtual Reality (VR)
Ecosystem
Meta
Meta Quest

ABSTRACT

The accelerating pace of digital transformation has given rise to metaverses that can participate freely in contactless environments. More than just game content, metaverses are driving everyday innovation across industries. However, threats are also prevalent, with crimes such as child sexual exploitation and privacy violations occurring in metaverses that mimic reality, making digital forensics for metaverse threats essential. Nevertheless, technical standards for different types of metaverses have yet to be defined, making investigation difficult. Furthermore, even though metaverses are complex forms that combine multiple hardware devices and software applications, existing studies have either focused on a single component or not analyzed the real-world environment. In this study, we derived a metaverse ecosystem with common components that comprise a metaverse and analyzed the hardware and software used throughout the user's metaverse lifecycle from a digital forensics perspective. In particular, we applied real-case-based scenario to the metaverse environment of the most popular *Meta*'s currently in use to identify various artifacts that can be used across the ecosystem and validate the effectiveness of the process. We also developed a metaverse digital forensics tool for the first time in the current situation where open-source and commercial tools do not support metaverse investigations.

1. Introduction

The development of IT technology has the accelerated pace of digital transformation to solve issues in various fields such as economics, society, and environment (McKinsey, 2020). The metaverse, which allows users to have a sense of immersion comparable to reality without spacetime constraints as well as communicate with an unspecified number of users, has attracted considerable attention (Time, 2021).

PwC (2021) estimated the global metaverse market to be worth USD 47.69 billion in 2020, Gartner (2022) predicted that by 2026, 25% of people will spend at least an hour per day in the metaverse for work, shopping, education, social media, and entertainment. Big tech companies including *Apple* (Bloomberg, 2023), *Meta* (Forbes, 2023), and Microsoft (2022) are investing heavily in the metaverse and are developing hardware and software and metaverse platforms to advance their metaverse ecosystem. Therefore, metaverse can be applied and used at a rapid pace throughout our daily lives and industrial field (Deloitte, 2023).

1.1. Motivations

Metaverse is a representation of various elements of reality (such as ego, place, and currency) in a virtual form. Although this characteristic enhances the immersion of users in the metaverse, "Synchronization of Threats" that is, threats that exist in the real world are reimplemented. Threats, such as grooming, racism, and sexual violence, have been reported on metaverse (BBC, 2022). Furthermore, data leakage threats have been reported on the metaverse operated by *SIEMENS*, an industrial control system company (Cybernews, 2023).

The threats related to the metaverse are not hypothetical. Initially imitating real threats, threat types are becoming increasingly diverse and sophisticated, and the frequency of their occurrence is expected to increase (EUROPOL, 2022). The emergence of novel threats related to the metaverse poses challenges for law enforcement agencies worldwide. Therefore, digital forensic technology research is urgently required to mitigate these threats (INTERPOL, 2022). However, digital forensics for metaverse has many challenges. Because a technical standard is yet to be devised for the metaverse, metaverse environments developed by various companies have distinct architectures (Spectrum, 2022). Supported hardware and software differ considerably, and

* Corresponding author. Department of Cyber Security, Ajou University, World cup-ro 206, Suwon, 16499, Republic of Korea
E-mail address: tsshon@ajou.ac.kr (T. Shon).

https://doi.org/10.1016/j.fsidi.2023.301608

Available online 13 October 2023

configuration and operation methods are diverse. Furthermore, the absence of research or tools in digital forensics for the metaverse cause numerous difficulties to investigators. Therefore, the development of a universal digital forensic investigation process that can be applied to the entire metaverse ecosystem composed of various hardware devices and software applications should be devised.

1.2. Contributions

The contribution of this paper is as follows:

- A metaverse ecosystem was established by analyzing major metaverse common components.
- Digital forensics process was proposed for efficiently investigating metaverse ecosystems.
- Scenario based on real-cases were designed and applied to Meta, which has the highest usage rate. Furthermore, significant artifacts were identified, and the effectiveness of the proposed process was validated.
- Designed and developed tools to efficiently analyze metaverse artifacts from a variety of formats and sources.

The rest of the paper is organized as follows: In Section 2, the overall research trends on ecosystem-based digital forensics and metaverse digital forensics were reviewed. In Section 3, we identify common components by analyzing the metaverse architecture of major metaverse vendors (*Meta*, *HTC VIVE*, *PICO*). In Section 4, based on the identified components, a metaverse ecosystem is derived, and a corresponding digital forensic process is proposed. In Section 5, the effectiveness of the research is validated by designing scenario based on real-cases and applying them to the *Meta* environment, which has the highest usage rate, and its analysis is presented. In Section 6, the design and implementation of a metaverse digital forensic analysis tool based on the ecosystem are described. In Section 7, the limitations and implications of this paper are discussed. Finally, in Section 8, the conclusions and follow-up studies of this paper are discussed.

2. Related works

2.1. Digital forensics based on ecosystems

Many digital forensic studies have been conducted based on the derived ecosystem. These studies revealed that artifacts can be efficiently acquired and analyzed even in an environment in which various hardware and software are connected through the ecosystem. Recently, many studies have been conducted on IoT-based ecosystems that directly interact with users and transmit sensitive data.

Kebande and Ray (2016) proposed a digital forensic investigation framework (DFIF-IoT) for the existing IoT ecosystem, and subsequently proposed a digital forensic investigation framework applicable to the expanded IoT ecosystem (IDFIF-IoT).

Chung et al. (2017) proposed a methodology to investigate a large amount of evidence accurately by combining artifacts collected from local devices and artifacts that can be collected from the cloud, targeting *Amazon's Alexa* ecosystem.

Jo et al. (2019) proposed four artificial intelligence (AI) speaker models in Korea in the form of an ecosystem, and five digital forensic analysis methodologies (speaker and packet analysis for mobile devices, *Android* directory analysis, application decompilation, and Chip-off analysis).

Evangelos (2021) performed digital forensic analysis on a mobile application that can control the home environment using devices constituting the *Xiaomi* IoT ecosystem.

Kim et al. (2023) proposed a novel IoT forensic framework that can identify interconnected IoT devices in an IoT ecosystem with various devices to conduct efficient digital investigation on interactions between devices.

2.2. Digital forensics for metaverse

Before metaverse was established, digital forensics research was conducted on virtual reality. However, digital forensic research is yet to be conducted metaverse. Existing studies have focused on a single source, even though artifacts can be obtained from various hardware and software constituting the metaverse environment.

Yarramreddy et al. (2018) conducted a study on artifacts that occur when metaverse applications are executed using *HTC VIVE* and *Oculus Rift* devices. *Steam*, *Bigscreen*, *Altspace VR*, *Rec Room*, and *Facebook Spaces* were targeted, and network packet analysis was performed on application data. User-related data, such as system and application information and user behavior-related logs, could be analyzed.

Casey et al. (2019) identified architecture patterns through reverse engineering for coordinate information generated when using *HTC VIVE*. These architecture patterns could be acquired from memory, and coordinate value extraction was automated using *Volatility* plugin. This result was visualized with the derived coordinate values, and inferring the posture the user was wearing *HTC VIVE* at the time of the memory dump was possible.

Joshua (2022) conducted digital forensic research on the *Oculus Quest 2* device through the *DFIR Community Hardware* Fund. This study explained the process of acquiring files from external storage while pairing and using the *Oculus Quest 2* device. Subsequently, a case study on *Oculus Quest 2* device rooting and user activities was discussed. However, this study did not consider artifacts that remained and whether meaningful information could be obtained, and the study was conducted only for a single source of hardware.

3. Analysis architecture of major metaverse

In this section, we will analyze the metaverse architectures of major metaverse vendors, compare common components, and describe the process of deriving an ecosystem. In this paper, structural analysis is conducted on HMD (Head-Mounted Display) hardware and software that is used in connection with the top 3 vendors (*Meta*, *HTC VIVE*, *PICO*) based on the VRcompare (2023) database and on sale as of 2023 years.

3.1. Meta

Meta is a metaverse vendor that develops metaverse-related hardware and software. The inception of *Meta* can be traced to *Facebook* acquiring *Oculus VR* in 2014. The company is releasing standalone HMDs based on the *Android* operating system in the Quest series (*Meta Quest 2*, *Meta Quest Pro*). A *Meta* account is required to use the HMD, and a pairing is performed by installing a mobile application called Meta Quest. *Meta* develops and operates a metaverse platform called Horizon Worlds. And supports cloud backup for *Meta Quest*'s user settings and data.

3.2. HTC VIVE

HTC VIVE is a metaverse vendor jointly developed by *HTC* and *Valve Corporation*. The company is releasing two HMDs, namely a standalone HMD series (*VIVE FOCUS*) and a dependent HMD series (*VIVE PRO*, *VIVE COSMOS*). The standalone HMD series is operated based on the *Android* operating system and requires an *HTC* account. Pairing should be performed by installing a mobile application called VIVE Manager. In the dependent HMD series, an application called SteamVR should be installed on the desktop to operate. *HTC VIVE* develops and operates a metaverse platform called VIVERSE. Unlike other vendors, *HTC VIVE* does not provide cloud features for backup user settings and data. But other than that, *HTC VIVE* provides cloud features for business and contents (VIVEPORT Streaming).

3.3. PICO

PICO is a metaverse vendor developed by *ByteDance*. The company is releasing standalone HMD series (*PICO Neo3 Pro*, *PICO Neo3 Link*, *PICO4*). In all HMDs released by *PICO*, standalone HMDs equipped with PICO OS based on the *Android* operating system are used. Unlike other vendors, pairing through mobile applications is not compulsory for using HMDs. However, devices can be managed efficiently by installing a mobile application called PICO VR. *PICO* a separate metaverse platform is not operated. And supports cloud storage (PICO developer) for *PICO*'s user settings and data.

3.4. Common components

Table 1 details the common components identified by analyzing the metaverse architecture released or operated by three major metaverse vendors. The table describes the types of HMDs released by each vendor, followed by their applications, platforms, and clouds. First, the HMD is a device equipped with a display corresponding to two eyes and is a hardware device that helps users visually immerse themselves in the metaverse. HMDs can be classified into a dependent-type HMD that mirrors and displays other computing devices and a standalone-type HMD that has a built-in operating system and performs calculations on its own. A standalone-type HMD performs computing calculations and storage, and the user's data are stored in HMD storage. Although *Meta* and *PICO* have only released standalone HMDs, *HTC VIVE* has released both types of models. Furthermore, most standalone HMDs use an *Android*-based operating system.

The two types of HMDs have separate applications. For the standalone-type HMD, a mobile application was used for pairing and device management, and in the case of the dependent-type HMD, a desktop application such as *SteamVR* was used. *Meta* and *HTC VIVE* have their own platforms metaverse, but *PICO* is yet to develop a platform. All three vendors have cloud use for user data backup and business. We compared (Table 1) the common components of the metaverse by analyzing the architecture of the metaverse released or operated by major vendors. The results revealed that although the metaverses of major vendors have various architectures, several common components exist in the entire process until users access the metaverse. Identifying these common components can determine clear analysis points in the metaverse digital forensics, and are critical in setting collection and analysis strategies.

4. Digital forensics process for metaverse ecosystems

An metaverse ecosystem was drawn based on the key components constituting the aforementioned metaverse environments, and a digital forensic process based on this ecosystem was proposed. As mentioned in Section 1, the metaverse operates with various architectures depending on the developer and operator, and a technical standard is yet to be devised. For access to the metaverse and to perform various activities, essential core components that should be used or passed through are presented in Table 1. Based on this result, an ecosystem was derived (Fig. 1) and subjected to proposed the digital forensic process. The metaverse ecosystem is categorized into five areas, namely HMD, Client, Application, Platform, and Cloud areas. The areas reveal that analysis is performed in different ways and perspectives in each area, and the digital forensic process devised according to the characteristics of each area is displayed in Fig. 2.

4.1. HMD area

In this area, the HMD device and the storage system are identified, and artifacts or device information stored are collected. HMD is a hardware device similar to a monitor in the existing computer input/output system, it can be an important analysis target depending on the type of digital forensics about metaverse ecosystem. Therefore, in the first step of analyzing the HMD area, confirming the type of HMD to be analyzed is essential. As mentioned, if the HMD is standalone, that has storage for storing user data. To obtain the data, checking whether the device has a hardware port that can be externally connected as well as the manufacturer's manual or official document is essential. The model differs depending on the installed operating system, but if the device is based on the *Android* analyzed in Section 3, external storage can be accessed by connecting it to a desktop, and actions necessary for digital forensics (such as application installation, basic information collection) can be additionally performed using *Android* debug bridge (ADB). If obtaining the `root` permission is not possible, analysis methods such as universal asynchronous receiver/transmitter (UART) and joint test action group (JTAG) can be considered by analyzing the printed circuit board (PCB) of the HMD.

4.2. Client area

In this area, the operating system artifacts of client devices (desktop and mobile) paired with HMD or used as computing resources are collected to identify the connection relationship between devices or the used metaverse application. If the HMD identified in the previous area is a dependent-type HMD, pairing it with the main device is essential. Furthermore, if the HMD is standalone, this process may not be essential, but in the case of analysis in Section 3, vendors force or recommend that HMD devices should be linked using separate applications to provide management and service. In the case of the *Windows* operating system commonly used in device desktops for pairing, information on devices connected to the desktop can be collected by analyzing applications such as Registry Hive (ScienceDirect, 2023) or `setup.api.dev.log` (Microsoft, 2021), and whether the user uses the HMD or the user of the HMD is specified through the serial number or device-specific value acquired. Furthermore, in the *Android* operating system, related information of the connected device can be collected through the application installation log for device linking or the system's Bluetooth pairing log generated during the device linking process. Furthermore, known operating system artifacts can be used to obtain additional clues or information required in other areas.

4.3. Application area

In this area, information, such as accounts, devices, and services used until the user accesses the metaverse platform, is collected by the artifacts of applications linked with the metaverse platform. *Windows Mixed*

Table 1
Comparison of major Metaverse architectures based on analysis.

Vendor	HMD			Application		Platform	Cloud
	Type	Model	OS	Name	OS		
Meta	Standalone	Meta Quest 2, Meta Quest Pro	Based on Android	Meta Quest	Android, iOS	Horizon Worlds	Support
	Dependent	Not Support					
HTC VIVE	Standalone	VIVE FOCUS, XR Elite	Based on Android	Android, iOS	VIVE Manager	VIVERSE	Support
	Dependent	VIVE PRO, VIVE COSMOS	Not Support	SteamVR	Windows		
PICO	Standalone	PICO Neo3 Pro, PICO Neo 3 Link, PICO 4	PICO OS (Based on Android)	PICO VR	Android, iOS	Not Support	Support
	Dependent	Not Support					

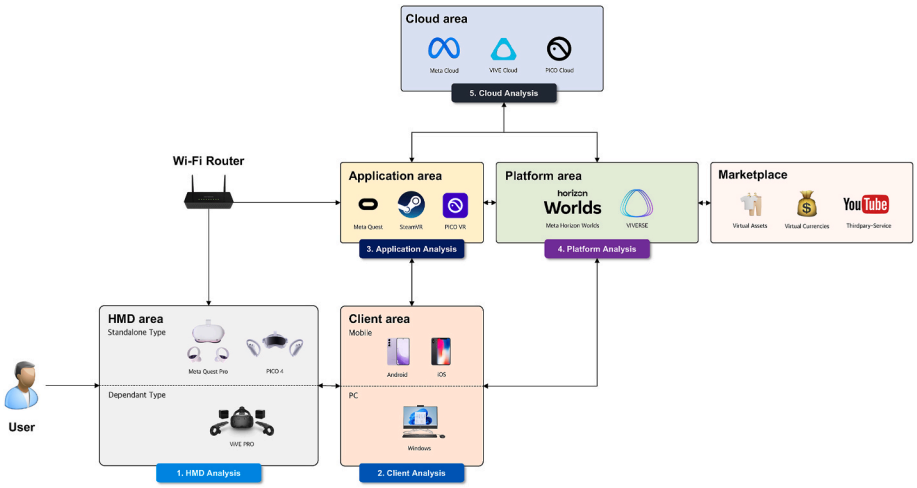


Fig. 1. Diagram of the metaverse ecosystems.

Reality application is built-in by default in *Windows 10 and 11*. *Steam*, an electronic software distribution platform, released an application called *SteamVR* to facilitate the use of HMD and metaverse-related services distributed by the company. *Meta* forces users to install and use an application called *Meta Quest* to use *Meta Quest* products and related services. In these applications, related information is stored locally so that users can access metaverse smoothly and maintain related devices. First, the client device that is supported by the application used in the metaverse to be investigated should be confirmed. Furthermore, if unique artifacts of applications installed in each client device are identified, user account information, paired devices, connected platforms, and community relationships can be collected.

4.4. Platform area

In this area, the storage system of the metaverse platform in which users activate is identified, and artifacts related to user information or actions on the metaverse are analyzed. Access and analysis methods may differ depending on the client device on which the metaverse platform is installed, and information that is collected and analyzed may vary depending on the characteristics of each platform. Therefore, the features and components of the metaverse platform can be analyzed in advance. In particular, it is necessary to explore and analyze artifacts based on information such as avatar, world, and interaction (text and voice), which are characteristics of the metaverse. Based on the result of the analysis, various information such as user information, conversation history, access world, and owned asset information can be determined.

4.5. Cloud area

In this area, user data stored in the cloud server are collected using the metaverse platform. Metaverse vendors store various user information and related information in the developer's cloud server for various purposes such as management or data synchronization. Furthermore, the metaverse platform uses RESTful API internally and externally to easily access and update cloud data for content creators and users. In this case, information is typically exchanged using the same ID system or parameters. This result can be used to verify information acquired in other areas or obtain additional information necessary for other investigations. Network communication data between the metaverse platform and the cloud segment can be collected. Because most of the HMDs are *Android*-based, network packets can be collected through proxy settings when connecting to a wireless network. However, for this data analysis, methods, such as installing a trusted certificate through routing, should be devised to decrypt encrypted network data by bypassing protection techniques including *SSL Pinning*, which should be prepared in advance.

4.6. Integrated analysis

In this process, analysis artifacts collected from the identified components of the metaverse ecosystem should be comprehensively analyzed. Among the artifacts, unique information that can identify the user and can track the user's behavior by combining time information are classified and organized separately in a timeline form or a form suitable to track the user's actions. If other user information is discovered in the process or information that requires additional investigation is confirmed, the digital forensic process is re-executed.

5. Case study: Meta's metaverse

In this section, the effectiveness of the digital forensic process based on the metaverse ecosystem derived from Section 4 is validated. Simulated scenario based on real cases are designed, an experimental environment is established, and artifacts are described that can be collected in the process-based analysis.

5.1. Setup environments

An experimental environment was established based on the derived ecosystem, and the list of configurations is presented in Table 2. The experimental environment was developed based on the metaverse environment of Meta, which has the highest usage rate (60.8%) based on the hardware survey (Steam, 2023) conducted by Steam, a well-known game distribution platform (architecture analyzed in Section 3). HMD used the *Meta Quest 2* product, which had the highest usage rate (41.4%) among *Meta*'s product series. *Samsung Galaxy S9* with the *Android* operating system was used as a client device to be paired with *Meta Quest 2*, and rooting was preceded to facilitate artifact collection. Furthermore, *Meta Quest 2* can be used only after pairing through the *Meta Quest* mobile application. The *Meta Quest* application was installed on the client device (*Samsung Galaxy S9*). And, connection to the same network is required to perform the pairing operation. A separate Wi-Fi router connected to the Internet was installed to perform pairing between the HMD and the client device. After completing the pairing process, the metaverse and various services can be used through *Meta Quest 2*. As a target metaverse platform, *Meta*'s *Horizon Worlds*, which has three hundred thousand users and has been reported in actual criminal cases, was installed.

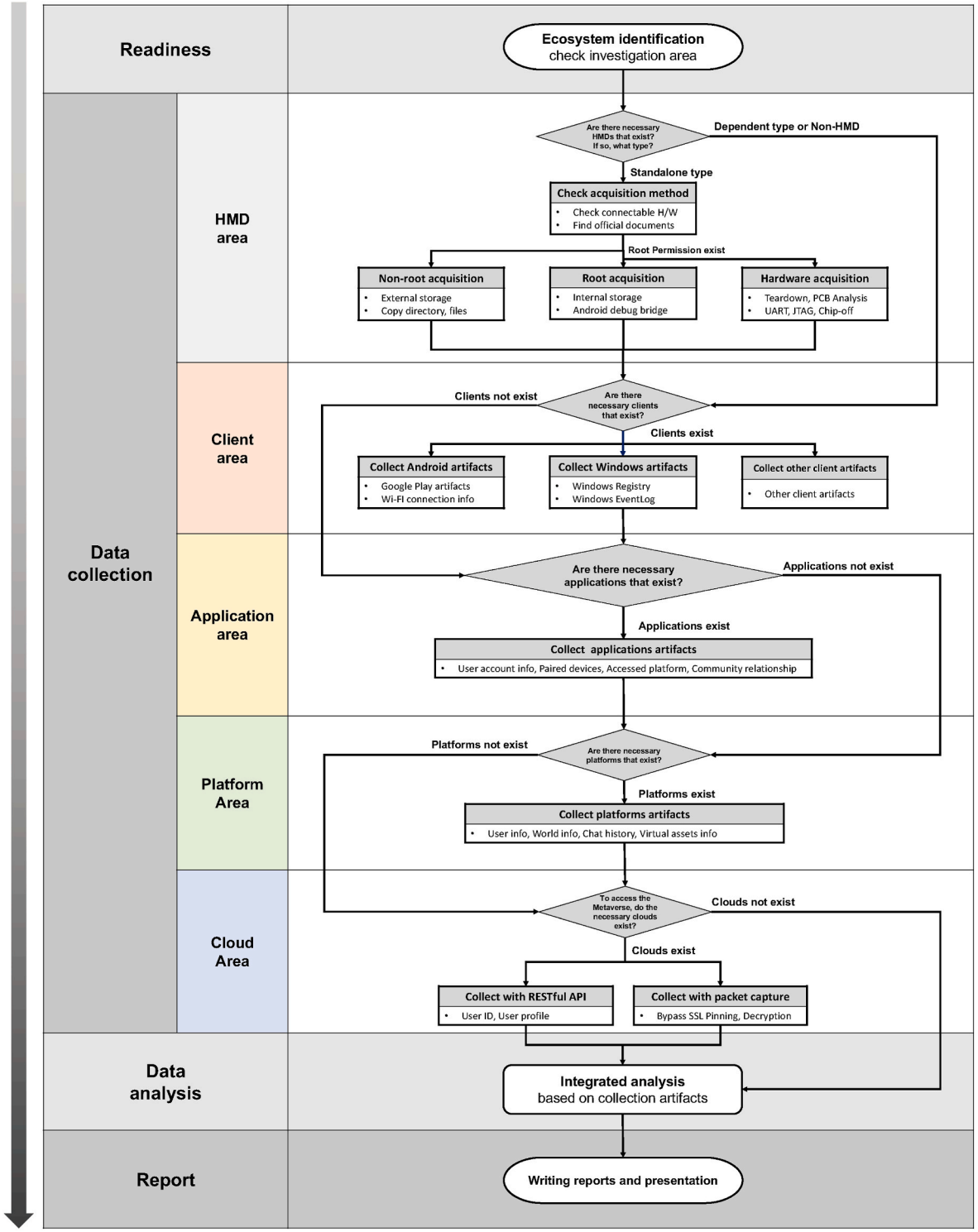


Fig. 2. Digital forensic process for metaverse ecosystem.

5.2. Design scenario

As mentioned in Section 1, among various threats and crime cases occurring on the metaverse, cases of online grooming between users and children and adolescents on the metaverse are the most serious issue. In *Meta*'s *Horizon Worlds* in 2021, a case of sexual assault and sexual harassment by accessors (SumOfUs, 2022) was reported. In 2022, *NAVER*'s *ZEPETO* attempted online grooming for children and adolescents and sexual exploitation; police conducted arrests in this case (Park, 2022).

A simulated crime scenario was designed in *Horizon Worlds*. Real incidents have been reported in this simulation. Based on the scenario, an investigation method corresponding to each area of the ecosystem was developed. The final designed scenario consists of five phases, and the actions for each phase are listed as follows:

Table 2
Experimental environments for metaverse ecosystems.

Area	Item	Description
HMD	Meta Quest 2	S/N: 1WMHHA******** OS Version: SQ3A.220605.009.A1
Client	Samsung Galaxy S9	S/N: R39K40**** OS Version: Android 9 Kernel Version: 4.9.59–16947869
Application	Meta Quest	App Version: 205.0.0.2.70
Platform	*Horizon Worlds*	Version: 107.0.0.7.169

(1) The suspect (Bob) installed the metaverse application (*Meta Quest*) on the client device (*Samsung Galaxy S9*) and activated and paired the HMD device (*Meta Quest 2*).
(2) The suspect (Bob) installed the metaverse platform (*Horizon Worlds*), and accessed a specific world (underage restricted).
(3) The suspect (Bob) in the metaverse world interacted with the user through movement and voice or captured pictures.
(4) The suspect (Bob) followed the victim (Alice) through the metaverse application (*Meta Quest*).
(5) The suspect (Bob) contacted the victim (Alice) through the message feature built into the metaverse application (*Meta Quest*) and share messages and links leading to another instant messenger (*Signal*).

Based on this scenario, we conducted our analysis assuming that we had seized the devices that comprised the suspect's metaverse ecosystem.

5.3. Metaverse ecosystem identification

Five areas (HMD, Client, Application, Platform, and Cloud areas) of the metaverse ecosystem that is identified from the experimental environment built above and the designed scenario were identified. A digital forensic process was applied to identify and analyze the artifacts collected in each area.

5.4. HMD area

As analyzed in Section 3, *Meta Quest 2* is an *Android*-based standalone HMD. Therefore, the storage system is also categorized into internal and external storage such as *Android*. However, how to get `root` permission or hardware unit data acquisition method (including UART, JTAG, Chip-off) of *Meta Quest 2* is not known. Therefore, in addition to internal storage that is inaccessible in the HMD area, data acquisition was attempted for accessible external storage, and artifacts were collected based on this result. In *Meta Quest 2*, if it is connected to a desktop through an external USB-C port such as a mobile device and allows access to data, we can access the data in the external storage. The storage system of the external storage of *Meta Quest 2* identified using this method is displayed in Fig. 3.

Device serial number: *Meta Quest 2* can be entered into the USB update mode by pressing the power button and volume down button simultaneously when booting. This mode provides features such as device information, factory reset, and sideload boot. If the device information menu is selected, meaningful information about the device (including device serial number, secure boot, lock state) is displayed like in Fig. 4. In particular, the device serial number of the device of 14 digits is confirmed by combining numbers and English letters.

Hibernation logs: *Meta Quest 2* enters a hibernate state when the user removes the HMD and does not use the display any longer, and the hibernate state is released when the user wears the HMD again. In `shellenv.log`, which is saved in the form of a text file in the Android/data/com.oculus.shellenv/files folder of the internal storage, logs about these hibernate states are recorded. These log files will be split into up to four parts, and except for the most recent log file (`shellenv.log`), the other three log files will have an index starting at 1 at the end of the file name. Through the log, when the user puts on and removes the HMD can be identified, Fig. 5, it consists of three parts (`Timestamp`, `Event Type`,

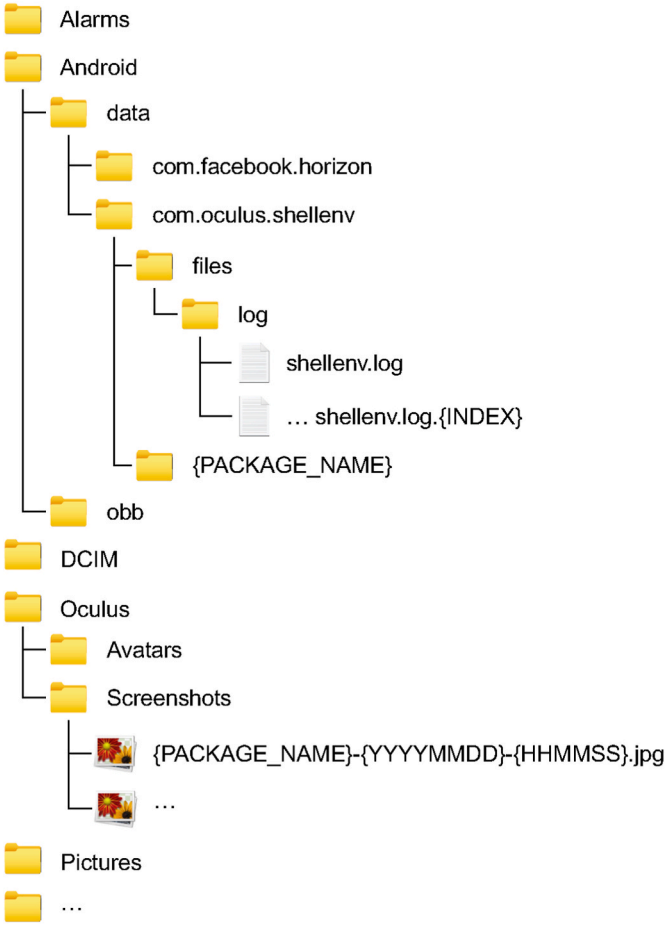


Fig. 3. Meta Quest 2 external storage structure.

Fig. 4. Meta Quest 2 recovery mode.

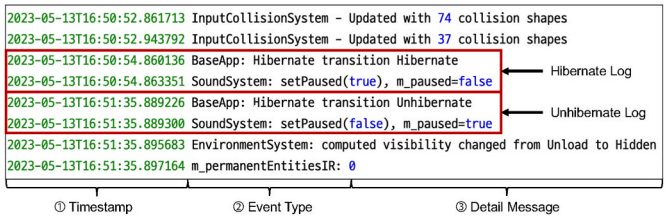


Fig. 5. Meta Quest 2 Hibernation log.

and `Detail Log`). The timezone of the timestamp recorded in this log is recorded based on the user's local timezone. Furthermore, when it is converted to the hibernate state, the log with event type of `BaseApp` records the log of the state transition called *"Hibernate transition Unhibernate"* and when the hibernate state is released, it records the *"Hibernate transition Hibernate"* log. The log was not deleted even after performing a factory reset. It is useful evidence to check the use of HMD.

Screenshots: *Meta Quest 2* can capture the photographs of the screen the user sees through the HMD like mobile devices. Screenshot image files (JPG format) taken by the user are stored in `{PACKAGE_NAME}-{YYYYMMDD}-{HHMMSS}.jpg` in the Oculus/Screenshots folder. The file name of the screenshot is composed (*Package Name*, *Timestamp*) as displayed in Fig. 6. The screen and application used by the user are checked through the screenshot file and package name, and the time when the user used the screen is identified through the timestamp data. The timezone of the timestamp has the user's local timezone.

5.5. Client area

As analyzed in Section 3, to use *Meta Quest 2*, an application called Meta Quest should be installed on a mobile device and paired. In the process, application installation information remaining in the *Android* operating system is analyzed.

Installed applications: By checking *Google Play* artifacts in the *Android* environment for traces related to the user's application installation and deletion. Application data for *Google Play* is stored in the/data/data/com.android.vending folder. To determine the installation time (UNIX Timestamp) of installed applications, check the installed applications and installation information in the `localappstate.db` file in the database folder. In the `localstate` table, we can find information such as package name, time of first download, and the account that downloaded it. By analyzing these artifacts, we can identify the installation information of the *Meta Quest* application, as shown in Fig. 7.

5.6. Application area

The *Meta Quest* application is an application that pairs and manages *Meta*'s HMD device. Access the internal storage of the client device (*Samsung Galaxy S9*) for collection, and the package folder/data/data/com.oculus.twilight of the application data were collected and analysis was performed.

Meta profile & messenger ID: `prefs_db`, which exists in the/data/data/com.oculus.twilight/databases path and has a SQLite3 database format, containing information about the user. Including application build and update versions, user ID (`MetaProfileActiveId`) for the *Meta Portal*, and messenger user ID (`MetaProfileGenericAuthMap.Communicator.userID`) used inside the *Meta Quest* application in `preferences` table, as shown in Fig. 8.

HMD pairing information: `RKStorage`, which exists in the/data/data/com.oculus.twilight/databases path and has a SQLite3 database format, containing information on HMD devices used by pairing with applications. For HMD devices, information on the first pairing time, last pairing time, the device serial number assigned to each device, and details of which devices are pairing are stored. This information is stored as the value of the `reduxPersist:pairedHeadsets` key in the `catalystLocalStorage` table, as shown in Fig. 9. The device serial number that is checked in this database file and the information of the

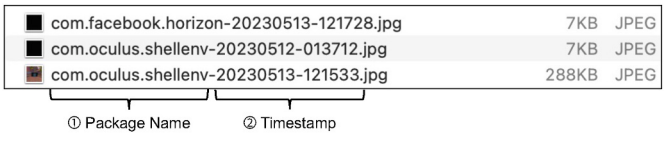


Fig. 6. Meta Quest 2 Screenshots.

	package_name	first_download_ms	account	title
1	com.oculus.twilight	1663148306458	[redacted]	Oculus

Fig. 7. Meta Quest application installation info.

device used for pairing matches the device serial number recorded in Fig. 4.

Messenger database: `messengervr_msys_database_{MESSENGER_ID}.db`, which exists in the/data/data/com.oculus.twilight/databases path and has an SQLite3 database format, stores messages exchanged with other users through the application. The `id` and `name` columns in the `contacts` table give us information about the people who have sent and received messages in the *Meta Quest* application. The `messages` table also stores messages sent and received between users. The `thread_key` represents a conversation, and the `timestamp_ms` represents the time of sending. `text` contains the content of the message, and `sender_id` is the ID of the sender, which can be compared with the `contact` table to trace the sender. These relationships are shown in Fig. 10.

5.7. Platform area

Meta Quest 2 officially supports the metaverse platform called *Horizon Worlds* developed by *Meta*. As of 2020, the total number of users is about three hundred thousand, and it supports various services from basic communication to work. *Horizon Worlds* communicates with various users through HMD, gestures through controllers, and voice through microphones. We can enter worlds with different purposes and teleport to each world.

Horizon Worlds activity log: These *Horizon Worlds* should be installed and operate inside *Meta Quest 2*. Therefore, the save log for *Horizon Worlds* should be collected from the HMD's data folder. The logs are stored in the following path:/Android/data/com.facebook.horizon/Horizon/Logs and are saved as a text file named `socialvr_{TIMESTAMP}.log`. This log stores some of our behavior while using *Horizon Worlds*. For example, we can see the names and ID values of the worlds that users have visited, as well as the *Meta* profile IDs of the avatars that have joined the world and when they joined. These logs are shown in Fig. 11.

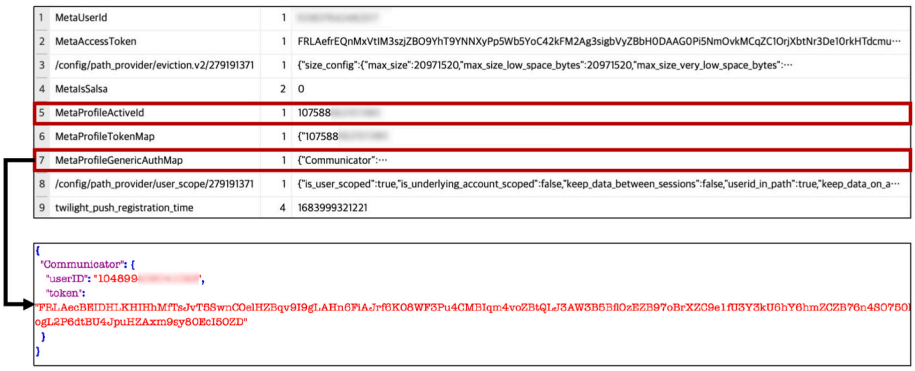
5.8. Cloud area

Horizon Worlds connected with Cloud area *Meta Quest 2* manages users and stores related information in conjunction with the official *Meta Quest* website. When accessing the metaverse on a new device, the information stored in the cloud is downloaded through the linked account. This measure allows to act in the metaverse with the same avatar that was accessed from the existing device.

User profile & information: *Meta Quest* official website manages user profiles by user profile ID, configures URL (oculus.com/profile/PROFILE_ID), and provides it in the form of a web page. Information about the user can be obtained by requesting the cloud server using the *Meta*'s user profile ID collected from the device as a URL parameter. The information currently provided includes user profile picture, username, and following list in Fig. 12 is provided. User information collected in other areas is verified or used to obtain additional information. Furthermore, we tried to collect by area between cloud servers targeting *Horizon Worlds*, but analysis was not possible because the method to register trusted certificates in *Meta Quest 2* is limited in the absence of `root` permission.

5.9. Integrated analysis

The detailed information collected from the artifacts are presented in Appendix A, and the timeline constructed by comprehensive analysis based on them is displayed in Fig. 13. Through the timeline, the time the



1	MetaUserId	1	
2	MetaAccessToken	1	FRLAefrEQnMxVtIM3szjZBO9YhT9YNNXyPp5Wb5YoC42kFM2Ag3sigbVyZBbH0DAAG0Pi5NmOvkMCqZC1OrjXbtNr3De1OrkHTdcmu···
3	/config/path_provider/eviction.v2/279191371	1	{"size_config":{"max_size":20971520,"max_size_low_space_bytes":20971520,"max_size_very_low_space_bytes":···
4	MetaIsSalsa	2	0
5	MetaProfileActiveId	1	107588
6	MetaProfileTokenMap	1	{"107588
7	MetaProfileGenericAuthMap	1	{"Communicator":···
8	/config/path_provider/user_scope/279191371	1	{"is_user_scoped":true,"is_underlying_account_scoped":false,"keep_data_between_sessions":false,"userid_in_path":true,"keep_data_on_a···
9	twilight_push_registration_time	4	1683999321221


```
{
 'Communicator': {
  "userID": "104899",
  "token":
"FRLAecBEIDHLKHIHhMfTsJvT8SwnCOelHZBqv9I9gLAHn6FiAJrf6KO8WF3Pu4CMBIqm4voZBtQLJ3AW3B5fl0zEZB97oBrXZC9e1fU3Y3kU6hY6hmZCZB76n4S07601
ogL2P6dtBU4JpuHZAxm9ey80EcI6OZD"
 }
}
```


Fig. 8. Meta Quest user profile & messenger ID.


```
[
 {
  "serialNumber": "1WMHHA",
  "type": "HOLLYWOOD",
  "deviceManifest": {
   "creationTime": 1663149780,
   "lastSyncTime": 1682927201,
   "id": "107602",
   "userDefinedDeviceName": null,
   "displayedDeviceName": "Meta Quest 2",
   "supports_eye_tracking": false,
   "supports_face_tracking": false,
   "hardware": [
    {
     "serial": "1WMHHA",
     "connection": "CONNECTED",
     "battery": "DISCHARGING",
     "battery_percent": 22,
     "last_synced_time": 1683045330,
     "type": "STANDALONE_HMD_BATTERY"
    }
   ]
  }
 }
]
```


Fig. 9. Meta Quest pairing device information.

suspect built and used the HMD environment in the scenario can be determined and confirmed by the device serial number that the HMD linked to the mobile device matched the confiscated HMD. The *Horizon Worlds* log confirmed that there was contact with the victim, and the messenger log built into the application confirmed that the suspect sent a message inviting the victim to an anonymous messenger.

6. Digital forensic analysis tools for metaverse ecosystems

In this section, we designed a digital forensic analysis tool based on

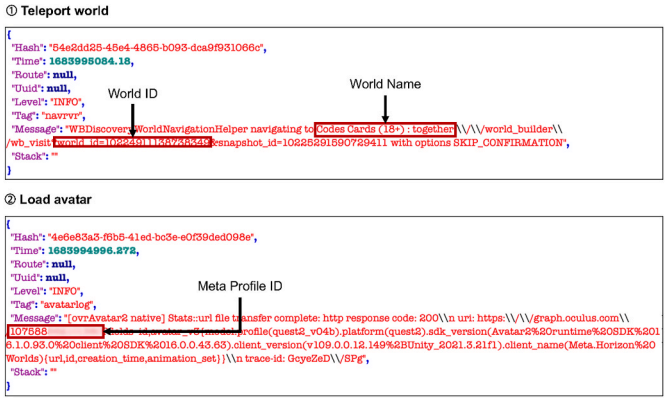
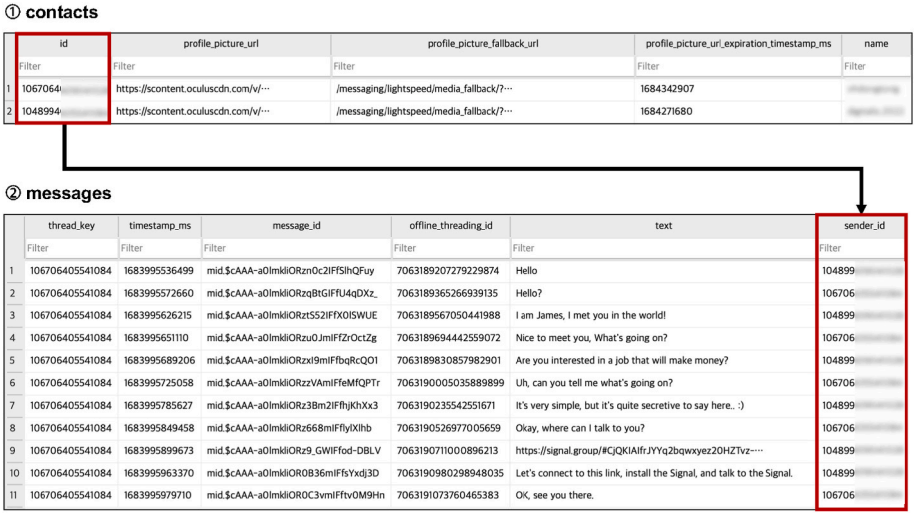


Fig. 11. Horizon Worlds teleport world & load avatar logs.



① contacts

	id	profile_picture_url	profile_picture_fallback_url	profile_picture_url_expiration_timestamp_ms	name
	Filter	Filter	Filter	Filter	Filter
1	1067064	https://scontent.oculuscdn.com/v/···	/messaging/lightspeed/media_fallback/?···	1684342907	
2	1048994	https://scontent.oculuscdn.com/v/···	/messaging/lightspeed/media_fallback/?···	1684271680	

② messages

	thread_key	timestamp_ms	message_id	offline_threading_id	text	sender_id
	Filter	Filter	Filter	Filter	Filter	Filter
1	106706405541084	1683995536499	mid.$cAAA-a0lmkliORzn0c2IFfSlhQFuy	7063189207279229874	Hello	104899
2	106706405541084	1683995572660	mid.$cAAA-a0lmkliORzqBtGIFfU4qDXz_	7063189365266939135	Hello?	106706
3	106706405541084	1683995626215	mid.$cAAA-a0lmkliORztS52IFfX0I5WUE	7063189567050441988	I am James, I met you in the world!	104899
4	106706405541084	1683995651110	mid.$cAAA-a0lmkliORzu0JmIFfZrOctZg	7063189694442559072	Nice to meet you, What's going on?	106706
5	106706405541084	1683995689206	mid.$cAAA-a0lmkliORzxI9mIFfbqRcQO1	7063189830857982901	Are you interested in a job that will make money?	104899
6	106706405541084	1683995725058	mid.$cAAA-a0lmkliORzzVAmIFfeMfQPTr	7063190005035889899	Uh, can you tell me what's going on?	106706
7	106706405541084	1683995785627	mid.$cAAA-a0lmkliORz3Bm2IFfhjKhXx3	7063190235542551671	It's very simple, but it's quite secretive to say here.. :)	104899
8	106706405541084	1683995849458	mid.$cAAA-a0lmkliORz668mIFfIyIXlhb	7063190526977005659	Okay, where can I talk to you?	106706
9	106706405541084	1683995899673	mid.$cAAA-a0lmkliORz9_GWIFfod-DBLV	7063190711000896213	https://signal.group/#CjQKIAlfrJYYq2bqwxyez20HZTvz····	104899
10	106706405541084	1683995963370	mid.$cAAA-a0lmkliOR0B36mIFfsYxdj3D	7063190980298948035	Let's connect to this link, install the Signal, and talk to the Signal.	104899
11	106706405541084	1683995979710	mid.$cAAA-a0lmkliOR0C3vmIFftv0M9Hn	7063191073760465383	OK, see you there.	106706

Fig. 10. Meta Quest application message databases.

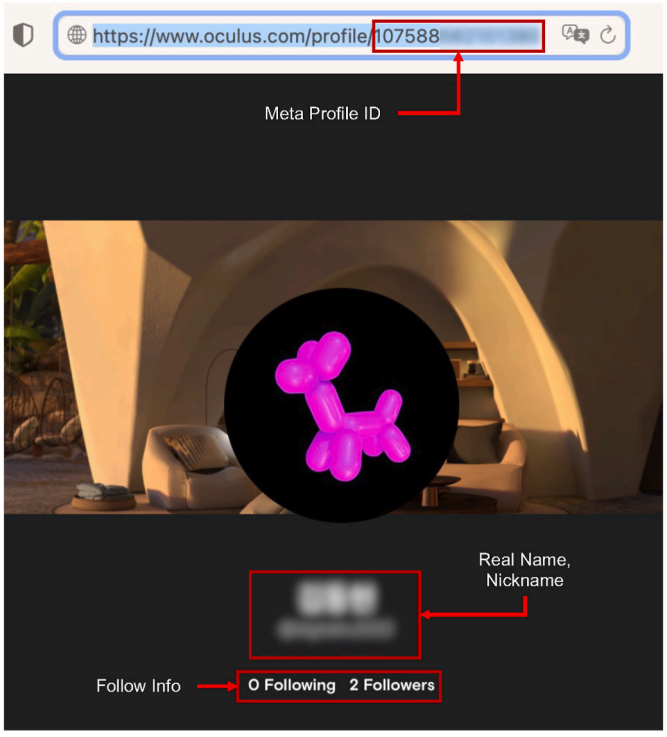


Fig. 12. Get Meta user information using profile ID.

the metaverse ecosystem derived from Section 4 and the proposed process. Based on the design, the analysis process discussed in Section 5 is automatically implemented, and the results are interpreted.

To perform digital forensics on the metaverse ecosystem derived in this paper, artifacts should be collected and analyzed in various areas. Analyzing artifacts generated in such a multi-source environment provides considerable information but to comprehensively analyze a number of artifacts in various formats, the help of an automated tool is required. However, at this point, commercial digital forensic tools such as *EnCase* and *Magnet AXIOM* or open-source digital forensic tools such as *Autopsy* do not have features or plugins that can perform digital forensics in relation to the metaverse. Therefore, a digital forensic analysis tool was developed to facilitate the digital forensic process based on the derived metaverse ecosystem.

6.1. Design consideration

Extensibility should be considered when designing the metaverse digital forensic tool. The structure of the tool designed considering this requirements is displayed in Fig. 14. As mentioned, in addition to the metaverses dealt with in this paper, other metaverses exist. The structure of the tool should have a form in which common artifacts can be reused and new artifacts can be easily developed and applied to other metaverse artifacts. Therefore, several concepts were introduced in this tool as follows:

- **Engine** refers to the code that parses and analyzes data in the tool. The engine is developed in the form of a library and designed so that it can perform its original role even if the web-based interface or command line-based interface (CLI) framework that connects it is changed.
- **Layer** processes the common file format of each artifact. It is inefficient to write a code to process each artifact having a file format such as text, SQLite3 database, or property list (PLIST). Artifacts having a common file format were designed to be processed in the same layer.
- **Object** stores requirements (artifact path, value query) that each artifact have in the JSON format. If there is a change in the artifact or

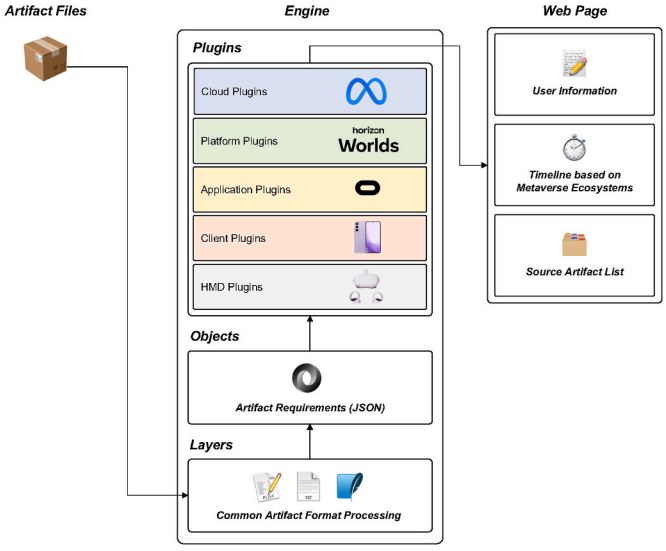


Fig. 14. Flow of the metaverse digital forensic analysis tool.

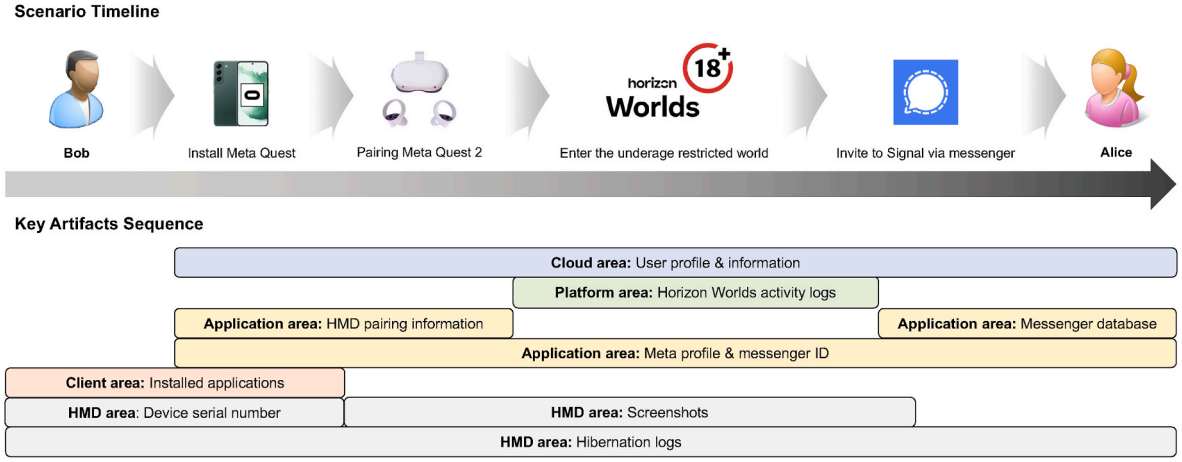


Fig. 13. Sequence diagram of artifacts that can be utilized in a scenario.

a change in the structure, then it is designed to faithfully perform the original feature by changing the data inside the object without modifying the plugin.

- **Plugins** process unique data for each artifact, and constant values or processing codes (such as UNIX Timestamp conversion and ID query) required for this are declared. Plugins are stored in separate folders based on the metaverse ecosystem derived from this paper. Each plugin corresponding to the entered artifact data and the metaverse ecosystem of the vendor to be analyzed was designed to parse the data required for analysis.

6.2. Implementation

We developed the first metaverse digital forensic tool based on the design and using *Python3*. This tool receives artifacts collected from various areas (HMD, Client, Application, Platform, Cloud areas) of the metaverse ecosystem in file units. Next, the tool is parsed based on the artifact value declared in the plugin and object inside the engine. Then, *Flask*, a *Python3*-based web framework, receives the parsed data and renders and visualizes it in the HyperText Markup Language (HTML) format. In this paper, plugins were developed and applied to tools targeting *Meta*, which was the subject of experimentation and analysis.

6.3. Interpretation

We applied and tested the tool developed based on the experimental datasets created in Section 5, and the results are displayed in Fig. 15. The resulting web page is largely composed of three areas. The first area displays basic information collected from artifacts. In the corresponding area, it can be confirmed that personal information such as user name, user profile ID, and serial number of the device is displayed. The second area provides an integrated timeline based on data collected from all areas of the metaverse ecosystem. The third area provides the hash value (SHA-256) for source artifact files constituting the timeline is provided. Section 5 of this paper shows that if a timeline is composed directly

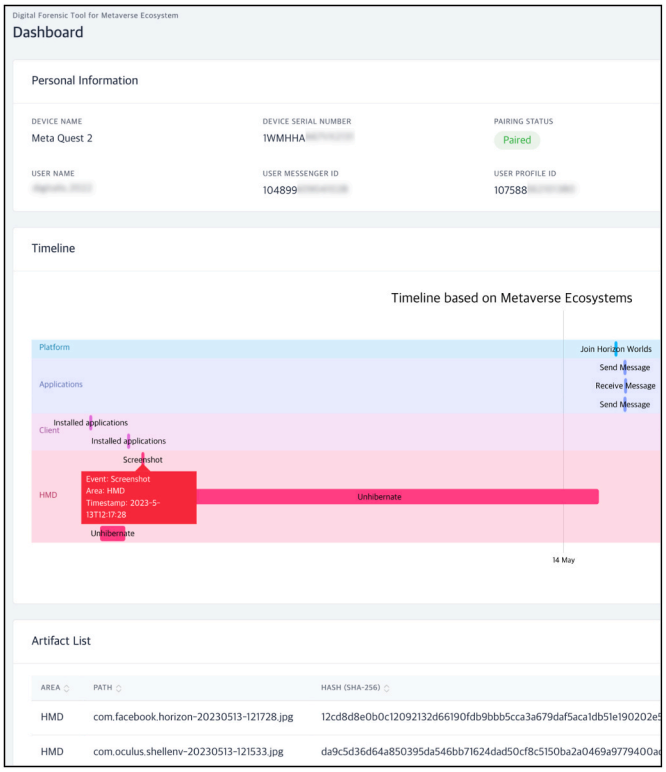


Fig. 15. A digital forensics tool for metaverse ecosystem.

through analysis according to digital forensic procedures, the user's timeline is conveniently tracked through a tool. This tool shorten the analysis time and provides clear analysis.

7. Discussion

This study showed digital forensic processes and analysis cases for threats in metaverse environments. The current situation special environment and without the technical standards of metaverse has become a challenge for forensic investigators. A digital forensic process based on the metaverse ecosystem was proposed, and through scenario-based analysis, unique artifacts (HMD device information, application installation information, HMD device pairing information, and messenger information) remaining in the five areas (HMD, Client, Application, Platform, Cloud areas) constituting metaverse were identified. This metaverse ecosystem derivation process and the digital forensic process based on it could be used to perform formal analysis even in a metaverse environment with a complex architecture. Furthermore, existing research has been conducted only on a single area that constitutes a metaverse, but in this paper, collection/analysis was performed throughout the metaverse components based on the ecosystem. This phenomenon allowed us to identify detailed artifact collection points (five areas) and provided a wider analysis perspective.

In addition to these contributions, digital forensics for the metaverse environment needs to be discussed and advanced. The following paragraphs describe the discussions.

7.1. Privacy issues

In this study, our proposed process allowed us to collect a variety of artifacts, including personal information. Personal information is a key piece of information in digital forensics and investigations. However, we must be concerned that we may be collecting too much of it. In particular, the metaverse is a place where many people congregate. In the process of collecting evidence through our proposed process, we may end up collecting the personal information of many different people who are separate from the target of the investigation. To avoid this situation, selective seizure should be considered in the digital forensics process, and more research should be done on how real-world legal systems would proceed and handle digital evidence collection on the metaverse.

7.2. Enhanced logging

Some limitations were identified in the scenario-based analysis process. Investigating the avatar's detailed behavior (such as motion information, voice conversation content) inside the metaverse platform only with the currently identified artifacts is difficult. This phenomenon may vary depending on the type of metaverse platform to be analyzed or future updates. However, current metaverse platforms cannot check specific behavioral data because of performance and various security issues. Therefore, metaverse service providers should enhance logging to collect on local devices for social responsibility for the metaverse environment or store detailed logs on the server. If these technical standards or institutions are preceded, additional artifacts related to users' behavior inside the metaverse platform can be obtained through the metaverse digital forensic processes covered in this paper. Using the secured identity information or circumstantial evidence related to metaverse users, investigative agencies can issue search warrants against metaverse service providers.

8. Conclusion

In this study, an metaverse ecosystem was derived as a common component that constitutes a major metaverse and a corresponding digital forensic process was proposed. To verify the effectiveness of the proposed process, an experimental environment was developed based

on *Meta*'s metaverse environment, which is currently the most used, and a scenario based on real-world cases was adapted. The result of the analysis of each area constituting the metaverse ecosystem based on the scenario and process allowed identification of various and meaningful artifacts. Furthermore, efficient digital forensic analysis was possible by designing and developing the first metaverse digital forensic tool based on the derived metaverse ecosystem.

The artifacts of *Meta*'s metaverse environment that was confirmed based on the derived metaverse ecosystem are as follows: usage records for HMD in the HMD area and unique serial information of the device were obtained. Furthermore, installation information of the application was obtained in the client area. In the application area, when the mobile client device and HMD were paired, information on the paired HMD, user information and messenger conversation history were available. In the platform area, checking the unique logs of the metaverse platform accessed by the user allowed determination of the world the user visited on the metaverse and interacted with other users. In the cloud area, information about users could be collected and verified through portals managed by *Meta* based on user profile IDs collected in other areas.

Based on the metaverse ecosystem derived from this study, artifacts unique to each area constituting the metaverse were collected. By analyzing this result in an integrated approach, one timeline required to track user behavior in the scenario could be constructed. We developed a digital forensics tool to automate this process, automatically generating a timeline and providing a list of artifacts and basic information to support an investigation.

In future studies, more artifacts should be analyzed on the metaverse ecosystem, and the limitations of this study should be overcome. Through precise data extraction research on HMD in hardware units or exploitation based on *Android* Kernel, we collect and analyze data on internal storage with `root` permissions. And we will evolve into a metaverse integrated digital forensics framework by adding plugins to other metaverse vendors based on the proposed tools.

CRediT author statement

Donghyun Kim: Methodology, Investigation, Formal analysis, Software, Writing - original draft. **Subin Oh:** Investigation, Software, Writing - review & editing. **Taeshik Shon:** Conceptualization, Writing - review & editing, Resources, Supervision.

Data availability

The data and tools that support the findings of this study are available from the corresponding author, upon reasonable request.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

The authors sincerely thank Jonghyun Kim of MXspace, Yongki Won of Bae, Kim & Lee, and Won Yeong Choi of the Korea National Police University for their advice in making this paper publish. This research was supported by Energy Cloud R&D Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT (NRF-2019M3F2A1073385)

A Meta's metaverse key artifacts based on metaverse ecosystem

Area	Artifact source	Example data	Descriptions
HMD	USB Update Mode	1WMHHA********	Device serial number
HMD	Android/data/com.oculus.shellenv/files/shellenv.log Android/data/com.oculus.shellenv/files/shellenv.log.{INDEX}	2023-05-13T16:48:37.451332 BaseApp: Hibernate transition Hibernate 2023-05-13T16:48:38.327047 BaseApp: Hibernate transition Unhibernate	Hibernate state logs Unhibernate state logs
HMD	Oculus/Screenshots/{PACKAGE_NAME}-{YYYYMMDD}-{HHMMSS}.jpg	com.facebook.horizon −20230513-121728.jpg com.oculus.shellenv −20230512-013712.jpg	Photograph files taken by users (Package name, Taken time)
Client	/data/data/com.android.vending/localappstate.db Table: `appstate`	`package_name:` com.oculus.twilight `first_download_ms:` 1663148306458 `account:` *******@gmail.com	Installed applications info (First installed date, Installed account)
Application	/data/data/com.oculus.twilight/databases/prefs_db Table: `preferences`	`MetaProfileActiveId:` 107588********** `MetaProfileGenericAuthMap:` {"Communicator":{"userID":"104899**********"}	Meta profile ID, Meta Quest messenger ID
Application	/data/data/com.oculus.twilight/databases/RKStorage Table: `catalystStorage`	`reduxPersist:pairedHeadsets:` {"serialNumber":"1WMHHA********", "deviceManifest": {"creationTime":1663149780,"lastSyncTime": 1682927201,"id": "107602**********","displayedDeviceName": "Meta Quest 2", "hardware": [{"connection": "CONNECTED","battery": "DISCHARGING","battery_percent": 22,"last_synced_time": 1683045330}]}} (ellipsis)	Paired HMD info (Pairing time, Device serial number, Charge info)
Application	/data/data/com.oculus.twilight/databases/messengervr_msys_databased_{MESSENGER_ID}.db Table: `contacts`, `messages`	`contacts.id:` 104899**********, `contacts.name:` *****, `messages.thread_key:` 106706405541084, `messages.timestamp_ms:` 1683995689206,	Exchanged messages with other users (Contacts info, Messages info)

(*continued on next page*)

(*continued*)

Area	Artifact source	Example data	Descriptions
		`messages.text:` Are you interested in a job that will make money?, `messages.sender_id:` 104899********	
Platform	/Android/data/com.facebook.horizon/Horizon/Logs/socialvr_{TIMESTAMP}.log	`Teleport world:` WBDiscovery WorldNavigationHelper navigating to Codes Cards (18+): together: /world_builder/wb_visit?world_id=10224911138738349 (ellipsis) `Load avatar:` Stats::url file transfer complete: http response code: 200 uri: https://graph.oculus.com/107588**********?fields = id (ellipsis)	Horizon Worlds activity logs (Teleport world, Load avatar)
Cloud	oculus.com/profile/{PROFILE_ID}	`URL:` https://www.oculus.com/profile/107588********* `Following:2, Follower:0` `Nickname:` *****, `Real name:` ***	User profile info (Nickname, Real name, Follow info)

References

BBC, 2022. Metaverse App Allows Kids into Virtual Strip Clubs. BBC. https://www.bbc.com/news/technology-60415317 (Accessed May 2023).

Bloomberg, 2023. When will apple launch the reality pro mixed-reality headset? apple 2023 devices. https://www.bloomberg.com/news/newsletters/2023-01-08/when-will-apple-launch-the-reality-pro-mixed-reality-headset-apple-2023-devices-lcnfzkc7 (Accessed May 2023).

Casey, P., Lindsay-Decusati, R., Baggili, I., Breitinger, F., 2019. Inception: virtual space in memory space in real space–memory forensics of immersive virtual reality with the htc vive. Digit. Invest. 29, S13–S21.

Chung, H., Park, J., Lee, S., 2017. Digital forensic approaches for amazon alexa ecosystem. Digit. Invest. 22, S15–S25.

Cybernews, 2023. Siemens Metaverse Exposes Sensitive Corporate Data. Cybernews. https://cybernews.com/security/siemens-metaverse-data-leak/ (Accessed July 2023).

Deloitte, 2023. The future of the metaverse. https://www2.deloitte.com/us/en/pages/technology/articles/what-does-the-metaverse-mean.html (Accessed July 2023).

EUROPOL, 2022. Policing in the Metaverse: what Law Enforcement Needs to Know.

Evangelos, D., 2021. Forensic analysis of xiaomi iot ecosystem. https://dfrws.org/presentation/forensic-analysis-of-xiaomi-iot-ecosyste m/.

Forbes, 2023. Council post: the metaverse could be better than the best internet game-or simply a security pipe dream. https://www.forbes.com/sites/forbesfinancecouncil/2023/01/05/the-metaverse-could-be-better-than-the-best-internet-game-or-simply-a-security-pipe-drea m/?sh=1175dc4b61d6 (Accessed July 2023).

Gartner, 2022. Gartner predicts 25% of people will spend at least one hour per day in the metaverse by 2026. https://www.gartner.com/en/newsroom/press-releases/2022-02-07-gartner-predicts-25-percent-of-people-will-spend-at-least-one-hour-per-day-in-the-metaverse-by-2026 (Accessed July 2023).

IEEE Spectrum, 2022. The metaverse needs standards, too. https://spectrum.ieee.org/metaverse-standards-forum (Accessed July 2023).

INTERPOL, 2022. Interpol Technology Assessment Report on Metaverse.

Jo, W., Shin, Y., Kim, H., Yoo, D., Kim, D., Kang, C., Jin, J., Oh, J., Na, B., Shon, T., 2019. Digital forensic practices and methodologies for ai speaker ecosystems. Digit. Invest. 29, S80–S93.

Joshua, I.J., 2022. Dfir community hardware fund. DFIRScience. https://github.com/DFIRScience/DFIRCommunityHardwareFund (Accessed July 2023).

Kebande, V.R., Ray, I., 2016. A generic digital forensic investigation framework for internet of things (iot). In: 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), IEEE, pp. 356–362.

Kim, J., Park, J., Lee, S., 2023. An improved iot forensic model to identify interconnectivity between things. Forensic Sci. Int.: Digit. Invest. 44, 301499.

McKinsey & Company, 2020. Digital strategy in a time of crisis. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-strategy-in-a-time-of-crisis (Accessed July 2023).

Microsoft, 2021. Usb device registry entries windows drivers. https://learn.microsoft.com/en-us/windows-hardware/drivers/install/setupapi-device-installation-log-entries (Accessed July 2023).

Microsoft, 2022. Microsoft to acquire activision blizzard to bring the joy and community of gaming to everyone, across every device. https://news.microsoft.com/2022/01/18/microsoft-to-acquire-activision-b.lizzard-to-bring-the-joy-and-community-of-gaming-to-everyone-across-every-device/ (Accessed July 2023).

Park, D., 2022. S.Korean man gets four years for sexual abuse in metaverse. https://forkast.news/headlines/skorea-man-four-years-sexual-abuse-metaverse/ (Accessed July 2023).

PwC, 2021. How is the metaverse set to shape the future of business? https://www.pwc.in/consulting/technology/emerging-tech/how-is-the-metav.erse-set-to-shape-the-future-of-business.html (Accessed July 2023).

ScienceDirect, 2023. Installed application. https://www.sciencedirect.com/topics/computer-science/installed-application (Accessed July 2023).

Steam, 2023. Steam hardware & software survey: March 2023. https://store.steampowered.com/hwsurvey/ (Accessed July 2023).

SumOfUs, 2022. Metaverse: another cesspool of toxic content. SumOfUs. https://www.eko.org/media/new-research-documents-sexual-assault-within-hours-of-entering-metas-virtual-reality-platform/ (Accessed July 2023).

Time, 2021. What is the metaverse? here's why it matters. https://time.com/6116826/what-is-the-metaverse/ (Accessed July 2023).

VRcompare, 2023. Vrcompare - the internet's largest vr & ar headset database. https://vr-compare.com/ (Accessed July 2023).

Yarramreddy, A., Gromkowski, P., Baggili, I., 2018. Forensic analysis of immersive virtual reality social applications: a primary account. In: 2018 IEEE Security and Privacy Workshops (SPW), IEEE, pp. 186–196.

Donghyun Kim is undergraduate student in Cyber Security at Ajou University in Suwon, Republic of Korea since 2017. He was a security engineer of ZIGBANG Co., Ltd (2019–2022). Also he was a winner of various digital forensics challenges sponsored by the Supreme Prosecutors' Office, the National Police Agency, and the National Intelligence Service in Republic of Korea. His research interests overall area of Digital Forensics.

Subin Oh received the B.S degree in cyber security from Ajou University, Suwon, Republic of Korea, in 2023. Since 2023, she is in the master's degree at Ajou University. Her research interest includes digital forensics for Mobile devices, Network, IoT devices, Smart City and Metaverse.

Taeshik Shon received his Ph.D. degree in Information Security from Korea University, Seoul, Korea in 2005 and his M.S. and B.S. degree in Computer Engineering from Ajou University, Suwon, Korea in 2000 and 2002, respectively. While he was working toward his Ph.D. degree, he was awarded a KOSEF scholarship to be a research scholar in the Digital Technology Center, University of Minnesota, Minneapolis, USA, from February 2004 to February 2005. From Aug. 2005 to Feb. 2011, Dr. Shon had been a senior engineer in the Convergence S/W Lab, DMC R&D Center of Samsung Electronics Co., Ltd. He is a visiting professor of Electrical Computer Engineering Department at Illinois Institute of Technology, Chicago, USA, in 2017. He is currently a professor at the Division of Cyber Security, College of Information Technology, Ajou University, Suwon, Korea. He was awarded the Gold Prize for the Sixth Information Security Best Paper Award from the Korea Information Security Agency in 2003, the Honorable Prize for the 24th Student Best Paper Award from Microsoft-KISS, 2005, the Bronze Prize for the Samsung Best Paper Award, 2006, the Second Level of TRIZ Specialist certification in compliance with the International TRIZ Association requirements, 2008, and the Silver, Bronze, Excellent Publication Prize for Ajou University Award, 2013, 2014, 2016. He is a senior member of IEEE and also serving as a guest editor, an editorial staff and review committee of Computers and Electrical Engineering - Elsevier, Mobile Network & Applications - Springer, Security and Communication Networks - Wiley InterScience, Wireless Personal Communications - Springer, Journal of The Korea Institute of Information Security and

Cryptology, IAENG International Journal of Computer Science, and other journals. His research interests include Industrial Control System, Anomaly Detection Algorithms, and Digital Forensics.