



# Article Digital Forensics for Analyzing Cyber Threats in the XR Technology Ecosystem within Digital Twins

Subin Oh<sup>1</sup> and Taeshik Shon<sup>2,\*</sup>

- <sup>1</sup> Department of Artificial Intelligence Convergence Network, Ajou University, Suwon 16499, Republic of Korea; osb0408@ajou.ac.kr
- <sup>2</sup> Department of Cybersecurity, Ajou University, Suwon 16499, Republic of Korea
- Correspondence: tsshon@ajou.ac.kr

**Abstract:** Recently, advancements in digital twin and extended reality (XR) technologies, along with industrial control systems (ICSs), have driven the transition to Industry 5.0. Digital twins mimic and simulate real-world systems and play a crucial role in various industries. XR provides innovative user experiences through virtual reality (VR), augmented reality (AR), and mixed reality (MR). By integrating digital twin simulations into XR devices, these technologies are utilized in various industrial fields. However, the prevalence of XR devices has increased the exposure to cybersecurity threats in ICS and digital twin environments. Because XR devices are connected to networks, the control and production data they process are at risk of being exposed to cyberattackers. Attackers can infiltrate XR devices through malicious code or hacking attacks to take control of the ICS or digital twin or paralyze the system. Therefore, this study emphasizes the cybersecurity threats in the ecosystem of XR devices used in ICSs and conducts research based on digital forensics. It identifies potentially sensitive data and artifacts in XR devices and proposes secure and reliable security response measures in the Industry 5.0 environment.

Keywords: industrial control system; digital twin; XR devices; cybersecurity; digital forensics



**Citation:** Oh, S.; Shon, T. Digital Forensics for Analyzing Cyber Threats in the XR Technology Ecosystem within Digital Twins. *Electronics* **2024**, *13*, 2653. https://doi.org/10.3390/ electronics13132653

Academic Editors: Nadia Kanwal, Mohammad Samar Ansari, Yuhang Ye and Brian Lee

Received: 30 May 2024 Revised: 2 July 2024 Accepted: 3 July 2024 Published: 6 July 2024



**Copyright:** © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https:// creativecommons.org/licenses/by/ 4.0/).

# 1. Introduction

Recently, advancements in digital twin and extended reality (XR) technologies, along with industrial control systems (ICSs), have driven the transition to Industry 5.0. A digital twin is a virtual replica of a physical system used to mimic and simulate real-world systems. According to the global market research firm MarketsandMarkets, the digital twin market was estimated to be worth USD 10.1 billion in 2023 and is expected to reach USD 110.1 billion by 2028 [1]. This technology plays a crucial role in various industrial fields, such as optimizing product development processes [2,3]. Digital twins are applied across different life cycle stages of industries, including design, manufacturing, and service stages. In the design stage, it enables the optimization of the fusion between information models and physical models of products, thereby shortening the design cycle and reducing rework costs. In the manufacturing stage, the actual manufacturing process is implemented using digital twins for real-time monitoring and control. The predictive maintenance sector is expected to be the largest segment in the digital twin market. Digital twins facilitate the analysis of equipment conditions and the prediction of potential failures or malfunctions by utilizing real-time sensor data and historical performance records. Such predictive maintenance offers benefits in terms of cost savings, operational efficiency, and equipment uptime [4–6].

Meanwhile, XR technology, which includes virtual reality (VR), augmented reality (AR), and mixed reality, merges the real and virtual worlds to provide new user experiences. By integrating digital twin simulations into XR devices, it can be utilized in various industrial fields for different purposes, such as equipment testing and real-time editing of

three-dimensional work [7]. VR technology transports users into a virtual world, allowing them to explore new environments. VR devices mimic real-world equipment or systems to provide training and simulation environments, thereby enhancing workers' skills. Workers performing high-risk tasks can be trained in a safe environment by simulating dangerous situations through VR devices. In this process, the digital twin makes training more realistic by reflecting the status of the actual system in real time. AR technology enhances the user's experience by adding virtual elements to the real world. AR devices provide workers with real-time work instructions and safety information, thereby improving their task efficiency and safety. The real-time status of facilities based on digital twins can be visualized through AR devices, and the necessary information for maintenance work can be provided in real time.

Thus, digital twin and XR technologies can interact with ICSs and are revolutionizing the industrial environment. To support this, XR devices are demonstrating high performance. Consequently, XR devices have independent operating systems and storage capabilities, enabling interaction with smartphones and Internet of Things (IoT) devices. However, such innovations simultaneously raise security issues. The increasing proliferation of XR devices has led to heightened security threats in ICSs and digital twin systems, including the leakage of personal and sensitive data as well as system intrusions via networks [8–11]. Because XR devices are connected to networks, the control and production data they process are at risk of being exposed to cyberattackers. If an attacker infiltrates an XR device through malicious code or hacking attacks, they can take control of the ICS or digital twin or paralyze the system. Moreover, if an XR device with access to the digital twin is stolen and there are no user authentication mechanisms in place, all information accessible through the device could be exposed. Such attacks can cause enormous damage by disrupting the operation of industrial facilities, incurring damage costs, and reducing productivity. Moreover, as the performance of XR devices continues to advance, it is not yet clear what data will be stored on these devices. Personal information, location data, health information, and other sensitive data could be stored in an XR device's storage. If such information is leaked, it could result in severe privacy breaches.

Therefore, this study emphasizes cybersecurity threats in the ecosystem of XR devices used in ICSs and conducts research based on digital forensics. The protection of users' personal information can be enhanced by investigating the storage of XR devices through digital forensics. Investigating and analyzing the filesystem of an XR device's storage to identify data structures and artifacts can help assess the potential for personal information leakage. Additionally, it can respond to cyberattacks targeting storage and can be used in the post-investigation process if a cyberattack occurs. Previous studies have demonstrated the application of digital forensics to enhance security measures within the automotive and IoT sectors, serving similar objectives [12–14]. Additionally, digital forensic research is actively being conducted to enhance security across various fields, such as filesystems, generative artificial intelligence (AI), and memory [15–22]. Likewise, this study is expected to contribute to a safe and reliable industrial system by identifying security vulnerabilities in industrial environments using digital twin and XR technology and proposing practical countermeasures. Therefore, the contributions of this study are as follows:

- The XR device ecosystem was derived by analyzing existing and new XR devices, and the potential cybersecurity threats within this ecosystem were identified.
- Potential filesystems for use in future XR devices were identified, and methods for acquiring filesystem storage data from XR devices for digital forensics were proposed.
- Digital forensics was conducted to address cybersecurity threats within the XR device ecosystem. The filesystems of XR devices were analyzed and artifacts examined to establish effective measures against cybersecurity threats.

The remainder of this paper is organized as follows: In Section 2, cybersecurity research trends for XR devices are discussed. In Section 3, an ecosystem of XR devices is derived by analyzing major XR devices, and the cybersecurity threats that may occur within this ecosystem are emphasized. Section 4 describes the process of acquiring storage data

from XR devices and identifying their filesystems. In Section 5, the identified filesystems are analyzed to assess the potential for cybersecurity threats, such as personal information leakage. In Section 6, the implications and limitations of this study are discussed. In Section 7, we present our findings and suggest directions for future research.

#### 2. Related Works

Among XR devices, head-mounted displays (HMDs) are the most widespread, leading to various cybersecurity studies being conducted on them. Noah et al. [23] conducted security and privacy assessments of AR/VR devices and their applications in various industries. These included HoloLens, Oculus, Google Glass, Valve Index, HTC Vive, Raptor AR, Psious (Amelia), Magic Leap, Epson Moverio, and IKEA Place AR devices and applications. They identified common vulnerabilities and exposures, which are publicly known security vulnerabilities potentially exploitable by attackers. Additionally, they found that the analyzed devices had information privacy policy flaws and provided recommendations for the secure use of these devices.

As VR HMDs transition users from the real world to a new virtual world, crimes in the real world can extend to the virtual world, causing significant issues. Moreover, because the virtual world is a digital space, cyberattacks are possible. Consequently, various digital forensic studies have been conducted to address crimes and cyberattacks in the virtual world. Kim et al. [24] conducted digital forensic research to respond to crimes such as child sexual exploitation and personal information breaches in a metaverse ecosystem. This study identified the major components of the metaverse, analyzed the hardware and software used during the user's metaverse lifecycle, and derived a metaverse ecosystem. They proposed a process to identify various artifacts that could be used in criminal investigations across the ecosystem and applied real-case-based scenarios to Meta Quest 2 and Horizon Worlds. Additionally, they developed the first digital forensic tool applicable to the metaverse based on the proposed methodology. Seo et al. [25] conducted digital forensic research in response to real-world crimes that can occur in a metaverse world. They presented a conceptual architecture of the metaverse and discussed the crimes that could occur within it, referred to as meta crimes. They also explored the need for digital forensic investigations in the metaverse and proposed the first metaverse forensic framework based on NIST's digital forensic guide. They discussed the challenges of digital forensic investigations in the metaverse from three perspectives: data ownership, antiforensics, and privacy. Al Ali et al. [26] proposed a metaverse digital forensic framework targeting Meta Quest VR headsets and an Oculus VR application. They described four types of cyberattacks related to the metaverse and provided scenario examples for each attack, explaining how to conduct forensic investigations using state-of-the-art forensic solutions and tools. They developed a metaverse forensic framework for investigating cyberattacks in the metaverse world so that forensic investigators, security researchers, and the general scientific community can utilize it for metaverse security. Ho [27] conducted digital forensic research targeting Oculus Go, Meta Quest, and Meta Quest 2 VR devices using Magnet AXIOM and Wireshark. They discovered specific forensic and network-based artifacts in eight social community applications by tracking users' personally identifiable information, application usage records, Wi-Fi network details, and multimedia content. Raymer et al. [28] conducted digital forensic research targeting Meta Quest 2 using the AXIOM tool. They demonstrated that various digital artifacts, such as user activities and device information, can be extracted using forensic methods. They also detailed the artifact acquisition process using digital forensics and studied methods for identifying and recovering internal file storage locations.

Previous studies have primarily conducted digital forensic research focusing on VR HMDs. However, most were limited to collecting a restricted range of data without obtaining administrative privileges for the devices or acquiring the internal storage data of the devices using commercial tools. In contrast, this study adopts a novel approach by physically accessing XR devices to extract file systems from the internal storage data of VR

HMDs. By identifying and analyzing the filesystems used on the devices, it was possible to develop a different artifact acquisition methodology from previous studies. Furthermore, by analyzing the filesystem of AR glasses, which are expected to become more widespread in the future, this study was able to derive important research findings that can enhance the cybersecurity level of XR devices.

# 3. Analysis of XR Device Ecosystem

In this section, the XR device ecosystem is derived by analyzing XR devices, and the potential cybersecurity threats within this ecosystem are identified. The timeline of XR devices released by major XR companies over the past five years is summarized in Table 1. As presented in Table 1, big tech companies and companies specializing in XR devices generally release devices in the form of VR HMDs and AR glasses. Therefore, this study focuses on analyzing VR HMDs and AR glasses. Major XR devices were selected and analyzed using VR Compare [29], which provides information on the specifications and features of VR/AR devices and big tech companies. For the VR HMDs, Meta Quest 2, Pico 4, and Apple Vision Pro were selected, whereas for AR glasses, Google Glass Enterprise Edition 2, Ray-Ban smart glasses 2, and TCL RayNeo X2 were chosen.

Table 1. Timeline of XR devices released by major companies.

Release Year	Device	Туре	Model
2024	VR HMD	Standalone	Apple Vision Pro
2024	AR Glasses	Standalone	TCL RayNeo X2
			Meta Quest 3
		Chan dalama	HTC Vive XR Elite
2023	VKHMD	Standalone	Pico G3
			Pimax Portal QLED View
	AR Glasses	Dependent	Ray-Ban Smart Glasses 2
2022		Standalone	Meta Quest Pro
2022	V K HIVID	Standarone	Pico 4
		Standalone	Pico Neo Link
2021	VR HMD	Dependent	HTC Vive Pro 2
2021			HP Reverb G2 Omnicept Edition
	AR Glasses	Dependent	TCL NXTWEAR G
		Standalone	Meta Quest 2
2020			HTC Vive Cosmos Elite
2020	VKHMD	Dependent	Pimax 5K Super
			HP Reverb G2
			HTC Vive Pro Eye
2010	VR HMD	Dependent	Meta (Oculus) Rift S
2019			HP Reverb
	AR Glasses	Standalone	Google Glass Enterprise Edition 2

# 3.1. XR Devices Ecosystem

The XR devices were analyzed by categorizing their key specifications to determine their performance and features. These specifications were divided into three main categories: information, connectivity, and system. Detailed specifications were distinguished within each category. By organizing the specifications by category, this study highlights the critical aspects that significantly affect the performance and user experience of XR devices. Table 2 presents the results of the analysis of major XR devices based on these categories.

Table 2. XR ecosystem derived from the analysis of major XR devices.

VR HMD	Specs	Meta Quest 2	Pico 4	Apple Vision Pro
	Release Date	2020.10	2022.10	2024.02
	Manufacturer	Meta (formerly Oculus)	Pico	Apple
Information	Туре	Standalone	Standalone	Standalone
	Platform <sup>1</sup>	Meta Home, Steam VR	Pico Store	visionOS
	Controller	Meta Touch (3 Gen)	Pico 4 Controller	Х
Connectivity	Ports	Universal Serial Bus (USB) Type-C	USB Type-C	USB Type-C
-	Wireless	Wi-Fi 6/Bluetooth 5.0 LE	Wi-Fi 6/Bluetooth 5.1	Wi-Fi 6/Bluetooth 5.3
	OS	Android 10	Pico OS 5.0 (Android)	visionOS
	Chipset	Qualcomm Snapdragon XR2	Qualcomm Snapdragon XR2	Apple M2 (Main) + Apple R1 (Secondary)
System	Memory	6 GB	8 GB LPDDR4	16 GB LPDDR5
	Storage	64 GB */128 GB/256 GB	128 GB/256 GB	256 GB/512 GB/1 TB
	SD Card	Х	Х	Х
AR Glasses	Specs	Google Glass Enterprise Edition 2 *	Ray-Ban Smart Glasses 2	TCL RayNeo X2
	Release Date	2019.05	2023.10	2024.02
	Manufacturer	Google	Meta	TCL
Information	Туре	Standalone	Dependent (Pairing with phone)	Standalone
	Platform	-	Meta View	RayNeo AR
Connectivity	Ports	USB Type-C	USB Type-C (in case) <sup>2</sup>	USB Type-C
Connectivity	Wireless	Wi-Fi 6/Bluetooth 5	Wi-Fi 6/Bluetooth 5.2	Wi-Fi 5/Bluetooth 5.2
	OS	Android 8.1	Х	RayNeo OS (Android)
	Chipset	Qualcomm Snapdragon XR1	Qualcomm Snapdragon AR1	Qualcomm Snapdragon XR2
System	Memory	3 GB	Х	6 GB
-	Storage	32 GB	32 GB	128 GB
	SD Card	Х	Х	Х
	AI	Х	Meta AI	AI assistant

<sup>1</sup> Platform: when using XR devices, essential or optional applications. <sup>2</sup> A port located not in the device but in the charging case. \* End of life.

# 3.1.1. Information

The information category covers basic information regarding XR devices. This category includes release date, manufacturer, type, platform, and controller. The type is classified based on the usage of the device, primarily divided into stand-alone, which can operate independently, and dependent, which requires a connection to a companion device (PC, mobile). A platform refers to a system installed within an XR device or a companion device that provides users with various applications or programs. Platform installation is not mandatory but enhances the convenience of using the device by offering various functions, such as social networking service and content exploration, through an account when installed. The controller transmits user input to the XR device and is primarily used

in VR HMDs. AR glasses, conversely, can be operated through hand gestures or voice commands without a controller.

#### 3.1.2. Connectivity

The connectivity category covers information about the wired and wireless communication methods supported by the device. This category included ports and wireless networks. Ports refer to the physical connections available on a device that are used for data transfer, device charging, or connecting to other peripherals. Wireless refers to technologies that enable devices to communicate with wireless networks or other devices, including Wi-Fi and Bluetooth. Wired and wireless communication allow users to connect to companion devices for a wider range of tasks, access new content via the internet, and update software.

#### 3.1.3. System

The system category includes important information, such as the core hardware and system of the device. This category includes operating systems (OS), chipsets, memory, storage, secure digital (SD) card slots, and AI. Each specification is a key element in determining the performance and functionality of an XR device. The OS manages the overall operation of the device, providing an environment for user interfaces and applications. The chipset includes processors, graphic processing units, and various other hardware components and is an important component in determining the device's processing power and power consumption. Memory temporarily stores data while the device performs tasks, with higher memory capacity allowing the handling of multiple tasks simultaneously and quickly. Storage is a space for user data, such as applications, media files, and documents, with various capacity options optimized according to the type and characteristics of the XR device. The SD card slot offers an option for additional external storage space, allowing users to expand their storage flexibly. AI plays an important role in AR glasses, helping XR devices interact with users more naturally and supporting advanced features such as object and voice recognition. AI assistants in AR glasses enhance the user experience by providing real-time information and improving interaction accuracy.

## 3.1.4. XR Device Development

Analysis of XR devices reveals the direction of technological advancement. As presented in Table 1, many VR HMDs were dependent until 2021; however, from 2022 onwards, standalone VR HMDs have predominantly been released. Although AR glasses have been released in both standalone and dependent forms, they are expected to primarily transition to standalone devices for user convenience, similar to VR HMDs. Table 2 shows that standalone devices use their own OS, most of which are Android-based. This implies that XR devices can independently perform a wide range of complex functions. The Androidbased OS provides a familiar environment for developers, facilitating the development of XR devices.

High-performance chipsets, large memory, and storage capacities are intended to satisfy the demands of complex graphics and data processing. This reflects technological progress aimed at providing users with a more immersive VR experience. While most XR devices prefer Qualcomm products, Apple Vision Pro adopts a multi-chipset approach, separating the main and secondary chipsets to offer better performance. Small IoT devices rely on external storage devices, such as SD cards, due to limited internal storage or the absence of internal storage. In contrast, XR devices have large built-in memory and storage and therefore do not usually require additional SD cards. Support for wired and wireless communication and controllers increases the compatibility between devices and diversifies user interactions.

AR glasses are advancing towards providing diverse and enhanced functions through AI integration, which innovatively improves the user experience. For instance, AI provides a more intuitive interface by tracking user gaze, recognizing gestures, and analyzing the environment in real-time to overlay relevant information on the AR glasses display. Additionally, AI assistants offer convenient functions through direct interaction with users. For instance, when conversing in different languages, an AI assistant can provide real-time translations displayed on AR glasses, enabling users to communicate without language barriers.

## 3.2. Cybersecurity of XR Devices

Figure 1 presents the potential attack vectors within the XR device ecosystem derived from the analysis of XR devices. From a cybersecurity perspective, the specifications of XR devices are important factors to consider. By analyzing the types and platforms of specific XR devices, attackers can identify vulnerabilities and plan their attacks. Most platforms used in devices may have security flaws, and attacks that exploit these vulnerabilities can threaten the devices. Additionally, the physical components of a device, including ports, can be exploited for physical access attacks or malware injections. External devices containing malicious code can be connected through a USB Type-C port designed for charging, thereby infecting the system. At the hardware level, memory and storage can lead to the leakage of sensitive data, such as personal information and user data, through physical access methods such as chip-off. Although such attacks require direct physical access to the devices, they can be effective for attackers.



Figure 1. Threats of XR device ecosystem.

OS vulnerabilities are also important components that attackers can exploit to obtain system permissions. Because most XR devices use an Android-based OS, vulnerabilities in a specific Android-based OS can pose risks to other OSs with the same base. Attackers can control a device through unpatched vulnerabilities, thereby exposing user data to risks. Wireless communication technologies such as Wi-Fi and Bluetooth also provide important information that can be utilized for network-based attacks. If a vulnerability is discovered in a specific wireless communication version, various XR devices using the same version can face the risk of network attacks. If a security vulnerability is discovered in a certain version of the Wi-Fi protocol, all the XR devices that use this protocol can become targets for attackers.

XR devices are exposed to various attack vectors. However, because the vulnerabilities of XR devices have not been sufficiently identified, they are particularly vulnerable to physical attacks. One such physical attack is the "chip-off" method, which accesses data on memory chips. There has been insufficient research or analysis of the physical storage data of XR devices. To understand the vulnerabilities associated with physically accessing the storage of XR devices, digital forensics focusing on storage were conducted.

#### 4. XR Device Filesystem Identification

This section describes the process of acquiring storage data from XR devices and identifying their filesystems. Storage includes essential data for the system's operation, such as the bootloader and OS, as well as various other data, such as user application data and documents. The filesystem enables efficient management and access to various types of data. By acquiring storage data from XR devices through physical attacks and analyzing the filesystem, deleted files can be recovered, file creation and modification times can be verified, and user activity can be tracked. Consequently, it is important to examine the potential for personal user information leakage by studying XR device storage filesystems.

Figure 2 presents an overview of the study described in this section. Currently, there is a lack of research on methods for obtaining internal data from XR devices by gaining administrative permission. Therefore, approaches that use chip-off and public data have been applied to acquire storage data from XR devices without administrator permission. The devices selected for storage data acquisition were Meta Quest 2 and Pico 4 for VR HMDs and Google Glass Enterprise Edition 2 for AR glasses. These devices are early standalone models equipped with independent OS, representing the trend in XR devices from dependent to standalone forms. Because these XR devices are equipped with an Android-based OS, they are likely to have similar filesystem structures. Thus, although the selected devices are early models, filesystem research centered on these devices is significant, considering that similar filesystems are likely to be used in current and future XR devices. The acquired storage data were analyzed using "binwalk" and "HxD" tools to identify the filesystems.



Figure 2. XR devices' filesystem research overview.

#### 4.1. XR Device Storage Data Acquisition

#### 4.1.1. Chip-Off

Figure 3 presents the storage chips obtained by disassembling Meta Quest 2 and Pico 4. Meta Quest 2 uses SK Hynix's HN8T05BZGKX015 (UHD-UFS-BGA153) storage, and Pico 4 uses Samsung's KLUDG4UHDC B0E1 (UHD-UFS-BGA153) storage. Because both devices use UFS-BGA153 storage, a JC UFS Programmer U15 reader was employed to acquire data from these chips. Figure 4 presents the process of acquiring storage data using a reader. After attaching the chip to the reader through a socket suitable for the chip type and connecting the reader to a PC, the device lights up, as shown in the bottom left of the figure. When the reader is properly connected to the PC and the JCID program is executed on the PC, the program automatically identifies the chip and provides information, as shown on the right side of the figure. The left screen of the program shows the chip information, whereas the right screen shows the chip partition information. Storage data can be saved on a PC using the backup function at the bottom of the program. The acquisition of storage data from Meta Quest 2 was successful. However, the Pico 4 chip was damaged, allowing only confirmation of the storage structure. Detailed information on the data obtained from the Meta Quest 2 storage and the structure of the Pico 4 storage is provided in Tables A1 and A2.



**Figure 3.** (Top) Meta Quest 2 storage chip/(Bottom) Pico 4 storage chip.

**JCID Repair Program** 



#### Data Extraction

Figure 4. Acquisition of storage data from XR devices through the JC U15 UFS Programmer.

4.1.2. Public System Image

Despite the discontinuation of Google Glass Enterprise Edition 2, Google continues to release system images for Android flashing [30]. An analysis of the latest released system images revealed that it consists of boot, bootloader, fpga, recovery, system, and

xloader partitions. Google has announced plans to launch Android-based AR devices [31]. Consequently, the filesystem analysis of the system images provided by Google offers valuable insights for future research on Google's AR devices.

#### 4.2. XR Device Filesystem Identification

Depending on their intended purpose, not all partitions use filesystems, making it necessary to identify the presence and type of filesystem in each partition. Binwalk and HxD were used to identify the filesystems in the acquired storage data. Initially, binwalk was used to identify areas where filesystems were present in each storage partition. Because binwalk can occasionally produce false positives based on magic numbers unique to filesystems, HxD was used to verify and extract valid filesystem areas. By examining the binary data with HxD, it was confirmed whether the superblock metadata area of the filesystem was valid and whether the offset location of the data area matched. Using this method, a list of identified filesystems obtained from the analysis of previously acquired storage partitions is presented in Table 3. Ext4 filesystems were identified in two partitions of Meta Quest 2 and one partition of Google Glass Enterprise Edition 2. Because both Meta Quest 2 and Google Glass Enterprise Edition 2 use Android-based operating systems, their storage is configured in Android partition formats. In Meta Quest 2, the user data partition, where user application data is stored, was encrypted, making direct analysis impossible.

Table 3. Summary of the identified XR device filesystem.

	XR Device	Data Acquisition	Partition	Filesystem
VR HMD	Mota Quest 2	Chip-off	persist	Ext4
	Wieta Quest 2	Chip-on	super	Ext4
	Pico 4	X *		-
AR Glasses	Google Glass Enterprise Edition 2	Public System Image	system	Ext4

\* The chip is damaged.

During the process of identifying filesystems from the extracted areas, different cases were found between the filesystems identified by binwalk and those analyzed using HxD. Figure 5 presents an example of a superblock from the filesystem obtained from an XR device. To distinguish between Ext2/3/4 filesystems, the values at  $0 \times 5C \sim 0 \times 5F$  and  $0 \times 60 \sim 0 \times 64$  in the superblock are used. The  $0 \times 4$  flag at  $0 \times 5 C \sim 0 \times 5F$  indicates whether journaling is used, while the  $0 \times 40$  flag at  $0 \times 60 \sim 0 \times 64$  indicates whether extents are used. Typically, both journal and extent flags are active in the Ext4 filesystem. However, the filesystems obtained from the XR device only contained the extent of flag activity. Binwalk identified this as Ext2; however, a direct analysis using HxD revealed it to be Ext4 without journal usage. Some Ext4 partitions do not use the journal area, making it impossible to recover deleted files even if a physical attack is attempted.

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000400	10	11	00	00	26	31	06	00	00	00	00	00	D5	04	00	00	&1Õ
00000410	1A	00	00	00	00	00	00	00	02	00	00	00	02	00	00	00	
00000420	00	80	00	00	00	80	00	00	50	01	00	00	00	00	00	00	.€€₽
00000430	80	07	5C	49	00	00	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	53	EF	01	00	01	00	00	00	€.\IÿÿSï
00000440	80	07	5C	49	00	00	00	00	00	00	00	00	01	00	00	00	€.\I
00000450	00	00	00	00	0B	00	00	00	00	01	00	00	28	00	00	00	
00000460	42	00	00	00	7B	40	00	00	D7	B8	71	D2	E8	DE	53	D5	B{@×,qÒè⊉SÕ

Ext3 or Ext4

Ext2 or Ext3/4

Figure 5. Meta Quest 2 super partition superblock.

# 5. XR Device Filesystem Analysis

To evaluate the cybersecurity threats posed by physical attacks on XR devices, storage data were acquired, and their filesystems were identified. This section analyzes the identified filesystems to evaluate the possibility of cybersecurity threats, such as personal information leakage. Binwalk and HxD were used to extract and analyze the files within the filesystem. If the filesystem had a normal structure, the files within the filesystem could be automatically extracted using binwalk. However, if automatic file extraction with binwalk was not possible, files were directly extracted from the binary data using HxD based on metadata analysis.

#### 5.1. VR HMD: Meta Quest 2

Persisting and super partitions have normal filesystem structures, and files within the filesystem can be extracted using binwalk. The persistent partition in the Android OS stores data that does not change on the device, and the analysis identifies data such as serial numbers, UUIDs, and MAC addresses. The super partition in the Android OS is a dynamic partition containing multiple partitions; however, the analysis found no special artifacts, only resource files and system application data.

#### 5.2. AR Glasses: Google Glass Enterprise Edition 2

There were no problems with the filesystem data of the system partition; however, data misalignment was observed. Figure 6 presents an example of a data misalignment in the system partition. The normal position of the magic number in the Ext4 superblock is at  $0 \times 38 \sim 0 \times 39$ , but in the system partition, it was located at  $0 \times 60 \sim 0 \times 61$ . A similar misalignment was observed in other areas, making it impossible to accurately obtain files within the filesystem based on the offset.

Normal Superblock	0F	0E	0D	0C	0B	0A	09	80	07	06	05	04	03	02	01	00	Offset(h)
Magic Number Location	00	00	39	0F	00	00	00	A3	00	00	40	00	00	00	40	00	00000400
q :	00	00	00	02	00	00	00	02	00	00	00	00	00	00	3F	71	00000410
.€€	00	00	00	28	00	00	40	00	00	00	80	00	00	00	80	00	00000420
ó•YdÿÿSï	00	00	00	01	00	01	EF	53	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	00	01	64	59	95	F3	00000430
-œ<`	00	00	00	01	00	00	00	00	00	00	00	00	60	8B	9C	96	00000440
<€<	00	00	00	3C	00	00	00	80	00	00	00	0B	00	00	00	00	00000450
B{&Éoc¢9HW	57	48	39	A2	63	6F	С9	26	00	00	00	7B	00	00	00	42	00000460
§§yy,vøc	00	00	00	00	00	00	00	00	63	F8	76	82	79	79	A7	A7	00000470
/persist	74	73	69	73	72	65	70	2F	00	00	00	00	00	00	00	00	00000480
Error Superblock	0F	0E	0D	0C	0B	0A	09	08	07	06	05	04	03	02	01	00	Offset(h)
Error Superblock Magic Number Location	0F	0E 00	0D 00	0C 00	0B 00	0A 00	09	08 00	07 00	06	05 00	04	03	02	<b>01</b> 00	00	Offset(h) 00000400
Error Superblock Magic Number Location (0x60-0x61)	0F 00 00	0E 00 00	0D 00 00	0C 00 00	0B 00 00	0A 00 00	<b>09</b> 00 00	08 00 00	07 00 00	06 00 00	05 00 00	04 00 00	03 00 00	02 00 00	01 00 00	00	Offset(h) 00000400 00000410
Error Superblock Magic Number Location (0x60-0x61)	0F 00 00	0E 00 00 04	0D 00 00 00	0C 00 00 00	0B 00 00 00	0A 00 00 01	<b>09</b> 00 00 00	08 00 00 00	07 00 00 00	06 00 00 00	05 00 00 00	04 00 00 00	03 00 00 00	02 00 00 00	01 00 00 00	00 00 00 00	Offset(h) 00000400 00000410 00000420
Error Superblock Magic Number Location (0x60-0x61)	0F 00 00 00	0E 00 00 04 00	0D 00 00 00 00	0C 00 00 00 00	0B 00 00 00 00	0A 00 00 01 00	09 00 00 00 FA	08 00 00 00 8D	07 00 00 00 00	06 00 00 00 01	05 00 00 00 8C	04 00 00 00 87	03 00 00 00 00	02 00 00 00 00	01 00 00 00 00	00 00 00 00 00	Offset(h) 00000400 00000410 00000420 00000430
Error Superblock Magic Number Location (0x60-0x61) ‡	0F 00 00 00 00	0E 00 00 04 00 00	0D 00 00 00 00 80	0C 00 00 00 00	0B 00 00 00 00	0A 00 00 01 00 00	09 00 00 FA 80	08 00 00 00 8D 00	07 00 00 00 00 00	06 00 00 00 01 00	05 00 00 00 8C 00	04 00 00 87 02	03 00 00 00 00 00	02 00 00 00 00 00	01 00 00 00 00	00 00 00 00 00 02	Offset(h) 00000400 00000410 00000420 00000430 00000440
Error Superblock Magic Number Location (0x60-0x61) 	0F 00 00 00 00 00 00 FF	0E 00 04 00 00 FF	0D 00 00 00 00 80 00	0C 00 00 00 00 00	0B 00 00 00 00 00 00	0A 00 01 00 00 00	09 00 00 FA 80 00	08 00 00 00 8D 00 00	07 00 00 00 00 00 00	06 00 00 01 00 00	05 00 00 00 8C 00 00	04 00 00 87 02 00	03 00 00 00 00 00 00	02 00 00 00 00 00 00	01 00 00 00 00 00 20	00 00 00 00 00 02 00	Offset(h) 00000400 00000410 00000420 00000430 00000440 00000450
Error Superblock Magic Number Location (0x60-0x61) ‡Œú. €€. ÿý	0F 00 00 00 00 00 FF 00	0E 00 00 04 00 00 FF 00	0D 00 00 00 80 00 00	0C 00 00 00 00 00 00	0B 00 00 00 00 00 00 00	0A 00 01 00 00 00 00	09 00 00 FA 80 00 00	08 00 00 8D 00 00 00 00	07 00 00 00 00 00 00 00	06 00 00 01 00 00 00 00	05 00 00 00 8C 00 00 00	04 00 00 87 02 00 02	03 00 00 00 00 00 00 00	02 00 00 00 00 00 00 00 01	01 00 00 00 00 20 EF	00 00 00 00 00 02 00 53	Offset(h) 0000400 0000410 0000420 0000430 0000440 00000450 00000460
Error Superblock Magic Number Location (0x60-0x61) ‡Eú. EE. 	0F 00 00 00 00 00 FF 00 00	0E 00 04 00 00 FF 00 00	0D 00 00 00 80 00 00 00	0C 00 00 00 00 00 00 00 00 00 00	0B 00 00 00 00 00 00 00 00	0A 00 01 00 00 00 00 00 00	09 00 00 FA 80 00 00 00	08 00 00 8D 00 00 00 00 00	07 00 00 00 00 00 00 00 00	06 00 00 01 00 00 00 00 00	05 00 00 8C 00 00 00 00 00	04 00 00 87 02 00 02 01	03 00 00 00 00 00 00 00 00	02 00 00 00 00 00 00 01 00	01 00 00 00 00 20 EF 00	00 00 00 00 02 00 53 00	Offset(h) 00000400 0000410 0000420 0000430 00000430 00000450 00000460 00000470

Figure 6. Example of data misalignment.

In the Ext4 filesystem, the fact that the locations of key areas for analysis, such as the superblock, inode table, and directory entries, differ from the metadata means that existing metadata-based Ext4 filesystem analysis tools cannot be used. If such misalignments are induced by specific rules, they can be considered an intentional measure to prevent file acquisition through filesystem analysis. Because these are public data, the purpose could be to prevent file leakage within the filesystem. Therefore, it is necessary to verify whether the same method has been applied to the filesystem data obtained from an actual device. If the same method is applied to an actual device, it can be concluded that Google Glass Enterprise Edition 2 effectively implements security techniques to prevent data leaks. Despite these challenges, analyzing the filesystem structure using HxD revealed the presence of necessary resource files for the system configuration. This suggests that the

system partition primarily contains system-related resource data for the XR device and that the likelihood of user-related personal information leakage is low.

#### 5.3. Examination of Potential Cybersecurity Threats

Table 4 presents a list of artifacts identified through analysis of the filesystem of the XR device. The analysis identified device-specific information such as serial numbers, UUIDs, and MAC addresses in the persistent partition, but no special artifacts were found in the other partitions. This indicates that effective security techniques are applied to the storage systems of XR devices, particularly to prevent access to partitions that store users' personal information or sensitive data. Because MAC addresses are used to identify devices on a network, they pose a potential risk of network attacks. However, this information alone is unlikely to directly leak personal information. Serial numbers and UUIDs can also be used for user identification, but extracting these data using chip-off techniques would provide no additional information if the device is no longer operational. Consequently, the likelihood of data leakage through physical attacks on XR devices is considered low.

Table 4. Artifacts of the analyzed XR device filesystem.

Device	Partition	Filesystem	Path	Artifact
			/calibration/display/screen_offset.json	Device
			/calibration/display/uniformity_offset.json	Serial Number
			/SYSTEM_SN	
	poreist	Ext4	/controller_sn_left.txt	Controller
Meta Quest 2	persist	EX14	/controller_sn_right.txt	Serial Number
			/controller_uuid_left.txt	Controller UIUID
			/controller_uuid_right.txt	controller 001D
			/wlan_mac.bin	MAC Address
	super	Ext4	-	
Google Glass Enterprise Edition 2	system	Ext4	-	

Nevertheless, information such as serial numbers, UUIDs, and MAC addresses can be important in the investigative process. For instance, this information can be used to track a specific device used in a crime or to locate stolen devices. Additionally, this information can provide essential clues for law enforcement agencies to link specific individuals or activities to devices. From this perspective, an analysis of the XR device's filesystem can provide valuable information related to criminal investigations.

#### 6. Results and Discussion

In this study, an XR device ecosystem was derived by analyzing XR devices, and potential cybersecurity threats within this ecosystem were identified. Due to the current lack of research on the vulnerabilities of XR devices, digital forensic research focusing on the storage of XR devices was conducted to examine the risk of the most threatening physical attacks and establish countermeasures. For the research devices, Meta Quest 2 and Pico 4 were selected for the VR HMDs, and Google Glass Enterprise Edition 2 for the AR glasses. These XR devices are early models that represent the trend toward standalone devices with their own OS. As most XR devices are equipped with an Android-based OS, it is likely that they have similar filesystem structures. Therefore, considering the high likelihood of similar filesystem usage in current and future XR devices, devices that were early standalone models and had high sales were selected for this study.

Methods for accessing the internal storage of XR devices through vulnerabilities have not been researched, and approaches using chip-off and public data have been applied to acquire the storage data of XR devices. The acquired storage data were analyzed, and the Ext4 filesystem was identified in two partitions of Meta Quest 2 and one partition of Google Glass Enterprise Edition 2 using binwalk and HxD. When analyzing the structure of the identified filesystem, some parts, despite being Ext4, did not use the journal area, making it impossible to recover the deleted files through the filesystem. Additionally, the user data partition where the user application data is stored is encrypted, making direct analysis impossible. By analyzing files existing in the filesystem, it was possible to confirm device-specific information (serial numbers, UUIDs, and MAC addresses), resources, and system app data as artifacts. Even if these data were extracted using the chip-off method, no further information could be obtained if the device was no longer in operation. Therefore, the risk of personal information leakage through physical attacks on XR devices is low.

This study extracts data from XR devices using the chip-off method, which has not been previously attempted. It can be utilized as an integrated XR device data analysis approach along with existing XR device data extraction methods. For example, data related to XR devices can be collected from a broader area by gathering not only hardware data through chip-off but also network and companion device data. Such comprehensive data can provide crucial clues for responding to cyberattacks and criminal investigations. They can be used to track the use of a specific device in a crime or to locate a stolen device, offering essential clues for law enforcement to link specific individuals or actions to a device. In conclusion, the filesystem analysis of XR devices confirms that, while there is no risk of personal information leakage during physical attacks, they can provide highly valuable information in criminal investigations. Furthermore, countermeasures for enhancing the security of current and future XR devices are proposed. Based on the artifact information derived from the filesystem analysis of XR devices, manufacturers can introduce hardware and software designs that consider security from the initial design stage. For instance, measures can be applied to enhance access control by encrypting or storing crucial device information (serial numbers, UUIDs, and MAC addresses) as hash values. Therefore, the results of this study, along with other research findings, can be utilized to enhance the security of XR devices, necessitating continuous research and development based on these findings.

However, this study has several limitations. First, it cannot identify the vulnerabilities of the XR devices. If the vulnerabilities of XR devices can be identified, a wide range of cybersecurity threats and research countermeasures can be identified. Second, the chip-off method used in this study has limitations in responding to cybersecurity threats because it damages the devices. When the chip-off process is successful on devices such as MetaQuest 2, the device can be restored through a reballing process that reattaches the chip to the device. However, when disassembling a VR HMD device, the device will inevitably be damaged to obtain the chip. If it were possible to disassemble a complex VR HMD device without damage, it would have additional research value as it could be used to respond to cybersecurity threats without the limitation of device damage through reballing. Conversely, if excessive heat is applied to the chip during the chip-off process, it can be damaged, making data acquisition impossible. For the Pico 4 used in this study, storage data acquisition was not possible because of chip damage during the chip-off process. Nevertheless, Pico 4 uses an Android-based OS, and its storage chip type was identified as Samsung's KLUDG4UHDC B0E1 (UHD-UFS-BGA153); therefore, it is expected that data acquisition would have been possible, similar to Meta Quest 2.

#### 7. Conclusions

Digital twin and XR technologies interact with ICSs to revolutionize the industrial environment. To support this, XR devices have demonstrated high performance. However, this innovation simultaneously causes security issues, particularly because the prevalence of XR devices increases the cybersecurity threats in ICS and digital twin environments. Therefore, this study emphasizes the cybersecurity threats in the ecosystem of XR devices used in ICSs and conducts research based on digital forensics.

To address the most vulnerable physical attacks in the current situation, the potential for personal information leakage was examined by analyzing the filesystem of the XR device storage and identifying artifacts. Ext4 filesystems were identified from three partitions acquired from the storage data of Meta Quest 2, Pico 4, and Google Glass Enterprise Edition 2. By analyzing the filesystem structure and the files present within it, cybersecurity threats were examined, and methods to utilize artifacts for digital forensic investigations were proposed.

Based on the results of this study, several future research directions are proposed. Firstly, we aim to research the decryption of user data partitions or vulnerabilities in XR devices to obtain and analyze internal storage data, enabling a deeper understanding of the data and addressing security issues. Secondly, we aim to expand the digital forensic methodologies used in this study to develop forensic tools and techniques that can respond to cybersecurity threats across various ICS components and not just XR devices. Finally, to effectively utilize digital twins and XR technologies in industrial environments, it is essential to research technical and policy measures that can enhance user privacy protection and data security. Through such research, digital twins and XR technologies can lead to innovations in safe and sustainable industrial environments.

**Author Contributions:** Conceptualization, S.O. and T.S.; methodology, S.O. and T.S.; validation, S.O.; formal analysis, S.O.; investigation, S.O.; writing—original draft preparation, S.O.; writing—review and editing, S.O. and T.S.; project administration, S.O. All authors have read and agreed to the published version of the manuscript.

**Funding:** This work was supported by Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korean government (MIST) (No. 2022-0-01022, Development of Collection and Integrated Analysis Methods of Automotive Inter/Intra System Artifacts through Construction of Event-based experimental system).

Data Availability Statement: Data is contained within the article.

Conflicts of Interest: The authors declare no conflicts of interest.

#### Appendix A

Table A1. Meta Quest 2 storage information.

Part	Partition Name	Start Address	Length	Size
	PrimaryGPT_0	0  imes 0	0 × 6000	24 KiB
	ssd	0 × 6000	0  imes 2000	8 KiB
	persist	$0 \times 8000$	0  imes 4000000	64 MiB
	isc	0  imes 4008000	$0 \times 100000$	1024 KiB
LUN0	frp	0 imes 4108000	0  imes 80000	512 KiB
(Unit0)	xros_a	0 imes 4188000	$0 \times 8008000$	128 MiB
	super	0 × C190000	$0 \times 180000000$	6 GiB
	xros_b	0 × 18C190000	$0 \times 8008000$	128 MiB
	metadata	0 imes 194198000	$0 \times 100000$	16 MiB
	userdata	0  imes 195198000	0 × 1C1126	112.3 GiB
	BackupGPT_0	0 × 1DA63FB000	$0 \times 5000$	20 KiB

Part	Partition Name	Start Address	Length	Size
	PrimaryGPT_1	0  imes 0	0 × 6000	24 KiB
	xbl_a	0 × 6000	0 × 380000	3.5 MiB
LUN1 (Boot A)	xbl_config_a	0 × 386000	0  imes 20000	128 KiB
(DOOL 11)	last_parti	$0 \times 3A6000$	0 imes 455000	4.3 MiB
	BackupGPT_2	$0 \times 7FB000$	$0 \times 5000$	20 KiB
	PrimaryGPT_2	0  imes 0	0 × 6000	24 KiB
	xbl_b	0 × 6000	0 × 380000	3.5 MiB
LUN2	xbl_config_b	0 × 386000	$0 \times 20000$	128 KiB
(DOOL D)	last_parti	$0 \times 3A6000$	0  imes 455000	4.3 MiB
	BackupGPT_2	$0 \times 7FB000$	0  imes 5000	20 KiB
	PrimaryGPT_3	0  imes 0	$0 \times 6000$	24 KiB
	ALIGN_TO_128k_1	0 × 6000	$0 \times 1A000$	104 KiB
LUN3	cdt	0 × 20000	0  imes 20000	128 KiB
(Unit3)	ddr	0  imes 40000	0 × 200000	2 MiB
	last_parti	$0 \times 240000$	0 × 5BB000	5.7 MiB
	BackupGPT_3	0 × 7FB000	0 × 5000	20 KiB
	PrimaryGPT_4	0 × 0	0 × 6000	24 KiB
-	aop_a	0 × 6000	0 × 80000	512 KiB
	tz_a	0 × 86000	0 × 400000	4 MiB
	hyp_a	0 × 486000	0 × 800000	8 MiB
	modem_a	0 × C86000	$0 \times 4000000$	64 MiB
	abl_a	$0 \times 4C86000$	0 × 200000	2 MiB
	keymaster_a	0  imes 4E86000	0 × 280000	512 KiB
	boot_a	0  imes 4F06000	0 × 5000000	80 MiB
	cmnlib_a	0 × 9F06000	0 × 80000	512 KiB
	cmnlib64_a	0 × 9F86000	0 × 80000	512 KiB
	devcfg a	0 × A006000	$0 \times 20000$	128 KiB
LUN4	gupfw a	0 × A026000	$0 \times 14000$	80 KiB
(Unit4)	vbmeta a	0 × A03A000	0 × 10000	64 KiB
	dtbo_a	$0 \times A04A000$	0 × 800000	8 MiB
	uefisecapp a	$0 \times A84A000$	0 × 200000	2 MiB
	fetenabler a	$0 \times AA4A000$	0  imes 20000	128 KiB
	imagefy a	$0 \times AA6A000$	$0 \times 200000$	2 MiB
	recovery a	0 × AC6A000	0 × 4000000	64 KiB
	vbmeta system a	$0 \times \text{EC6A000}$	0 × 10000	64 KiB
	vbmeta vendor a	$0 \times \text{EC7A000}$	0 × 10000	64 MiB
	hyp xros a	$0 \times \text{EC8A000}$	0 × 1000000	16 MiB
	aop b	$0 \times FC8A000$	0 × 80000	512 KiB
	tz h	$0 \times FD0A000$	0 × 400000	4 MiB
	hvn_h	0 × 1010 Δ 000	0 ~ 800000	2 MiP

# Table A1. Cont.

Table A1. Cont.

Part	Partition Name	Start Address	Length	Size
	modem_b	0 × 1090A000	0 × 4000000	64 MiB
	abl_b	0 × 1490A000	0 × 200000	2 MiB
	keymaster_b	0 × 14B0A000	$0 \times 80000$	512 KiB
	b	$0 \times 14B8A000$	$0 \times 5000000$	80 MiB
	cmnlib_b	$0 \times 19B8A000$	$0 \times 80000$	512 KiB
	cmnlib64_b	0 × 19C0A000	$0 \times 80000$	512 KiB
	devcfg_b	$0 \times 19C8A000$	$0 \times 20000$	128 KiB
	qupfw_b	$0 \times 19$ CAA000	$0 \times 14000$	80 KiB
	vbmeta_b	$0 \times 19CBE000$	$0 \times 10000$	64 KiB
	dtbo_b	0 × 19CCE000	$0 \times 800000$	8 MiB
	uefisecapp_b	$0 \times 1A4CE000$	$0 \times 200000$	2 MiB
	featenabler_b	0 × 1A6CE000	0  imes 20000	128 KiB
	imagefv_b	$0 \times 1A6EE000$	0 × 200000	2 MiB
LUN4	recovery_b	$0 \times 1A8EE000$	0  imes 4000000	64 MiB
(Unit4)	vbmeta_system_b	$0 \times 1E8EE000$	0 × 10000	64 KiB
	vbmeta_vendor_b	$0 \times 1E8FE000$	0 × 10000	64 KiB
	hyp_xros_b	$0 \times 1E90E000$	$0 \times 1000000$	16 MiB
	devinfo	$0 \times 1F90E000$	0  imes 1000	4 KiB
	apdp	$0 \times 1F90F000$	0  imes 40000	256 KiB
	msadp	$0 \times 1F94F000$	0  imes 40000	256 KiB
	spunvm	$0 \times 1F98F000$	0  imes 2000000	32 MiB
	limits	0  imes 2198F000	0  imes 1000	4 KiB
	limits-cdsp	0  imes 21990000	0  imes 1000	4 KiB
	pstore	$0 \times 21991000$	$0 \times 200000$	2 MiB
	storsec	$0 \times 21B91000$	0  imes 20000	128 KiB
	uefivarstore	$0 \times 21BB1000$	$0 \times 80000$	512 KiB
	secdata	$0 \times 21C31000$	$0 \times 6000$	24 KiB
	last_parti	$0 \times 21C37000$	$0 \times 7C4000$	7.8 MiB
	Backup_GPT_4	$0 \times 223FB000$	0  imes 5000	20 KiB
	ParimaryGPT_5	0  imes 0	0  imes 6000	24 KiB
	ALIGN_TO_128K_2	$0 \times 6000$	$0 \times 1A000$	104 KiB
	modemst1	$0 \times 20000$	$0 \times 200000$	2 MiB
LUN5	modemst2	0  imes 220000	$0 \times 200000$	2 MiB
(Unitb)	fsg	0  imes 420000	0 × 200000	2 MiB
	fsc	0 × 620000	0 × 200000	128 KiB
	last_parti	$0 \times 640000$	$0 \times 1BB000$	1.7 MiB
	BackupGPT_5	$0 \times 7FB000$	0  imes 5000	20 KiB

Part	Partition Name	Start Address	Length	Size
	PrimaryGPT_0			
-	ssd			
-	persist			
-	cache			
-	misc			
-	keystore			
-	frp			
LUN0 (Unit0) -	super			
	recovery			
	vbmeta_system			
	vbmeta_systembak			
	metadata			
	vm-system			
	vm-systembak			
	rawdump			
-	picocfg			
-	BackupGPT_0		_ *	
	PrimaryGPT_1			
-	xbl			
LUN1	xbl_config			
(Boot A) –	last_parti			
-	BackupGPT_1			
	PrimaryGPT_2			
-	xblbak			
LUN2	xbl_configbak			
(Boot B) –	last_parti			
-	BackupGPT_2			
	PrimaryGPT_3			
-	ALIGN_TO_128K_1			
-	cdt			
LUN3 - (Unit3)	ddr			
	mdmddr			
-	lat_parti			
-	Paraluur CDT 2			

 Table A2. Pico 4 storage information.

Table A2. Cont.

Part	Partition Name	Start Address	Length	Size
	PrimaryGPT_4			
_	aop			
_	tz			
_	hyp			
_	modem			
_	bluetooth			
_	mdtpsecapp			
-	mdtp			
-	abl			
-	dsp			
-	keymaster			
-	boot			
_	cmnlib			
_	cmnlib64			
-	devcfg			
-	qupfw			
-	vbmeta			
-	dtbo			
-	uefisecapp			
LUN4	multiimgoem			
(Unit4)	multiimgqti			
	vm-linux			
	featenabler			
	imagefv			
	aopbak			
	tzbak			
_	hybak			
	modembak			
_	bluetoothbak			
	mdtpsecappbak			
	mdtpbak			
	ablbak			
	dspbak			
_	keymasterbak			
-	bootbak			
-	cmnlibbak			
-	cmnlib64bak			
-	devcfgbak			
-	qupfwbak			
-	vmetabak			

Part	Partition Name	Start Address	Length	Size
	dtbobak			
	uefisecappbak			
	multiimgoembak			
	multiimgqtibak			
	vm-linuxbak			
	featenablerbak			
	imagefvbak			
	devinfo			
	dip			
	apdp			
I I INIA	msadp			
(Unit4)	spunvm			
	limits			
	limits-cdsp			
	logfs			
	logdump			
	storesc			
	uefivarstore			
	secdata			
	vm-keystore			
	vm-data			
	last_parti			
	BackupGPT_4			
	PrimaryGPT_5			
	ALIGN_TO_128K_2			
	modemst1			
	modemst2			
	fsg			
LUN5	fsc			
(Unit5)	mdm1m9kefs3			
	mdm1m9kefs1			
	mdm1m9kefs2			
	mdm1m9kefsc			
	last_parti			
	BackupGPT_5			
	=			

Table A2. Cont.

\* The chip was damaged, making data acquisition impossible.

# References

- 1. Digital Twin Market Size, Share, Statistics and Industry Growth Analysis Report by Application, Enterprise and Geography— Global Growth Driver and Industry Forecast to 2028. Available online: https://www.marketsandmarkets.com/Market-Reports/ digital-twin-market-225269522.html (accessed on 13 April 2024).
- 2. Javaid, M.; Haleem, A.; Suman, R. Digital twin applications toward industry 4.0: A review. Cogn. Robot. 2023, 3, 71–92. [CrossRef]

- Liu, M.; Fang, S.; Dong, H.; Xu, C. Review of digital twin about concepts, technologies, and industrial applications. *J. Manuf. Syst.* 2021, 58, 346–361. [CrossRef]
- Zhong, D.; Xia, Z.; Zhu, Y.; Duan, J. Overview of predictive maintenance based on digital twin technology. *Heliyon* 2023, 9, e14534. [CrossRef] [PubMed]
- 5. Using a Digital Twin in Predictive Maintenance. Available online: https://jpt.spe.org/using-digital-twin-predictive-maintenance (accessed on 14 April 2024).
- 6. Decoding Digital Twins: Exploring the 6 Main Applications and Their Benefits. Available online: https://iot-analytics.com/6main-digital-twin-applications-and-their-benefits (accessed on 14 April 2024).
- 7. Pairing AR/VR with Digital Twins. Available online: https://www.eetimes.com/pairing-ar-vr-with-digital-twins (accessed on 14 April 2024).
- 8. Qayyum, A.; Butt, M.A.; Ali, H.; Usman, M.; Halabi, O.; Al-Fuqaha, A.; Abbasi, Q.H.; Imran, M.A.; Qadir, J. Secure and trustworthy artificial intelligence-extended reality (AI-XR) for metaverses. *ACM Comput. Surv.* **2023**, *56*, 1–38. [CrossRef]
- Yamakami, T. A privacy threat model in xr applications. In Proceedings of the 8th International Conference on Emerging Internet, Data and Web Technologies, Japan, Kitakyushu, 24–26 February 2020.
- Abraham, M.; Saeghe, P.; Mcgill, M.; Khamis, M. Implications of XR on Privacy, Security and Behaviour: Insights from Experts. In Proceedings of the NordiCHI '22: Nordic Human-Computer Interaction Conference, Aarhus, Denmark, 8–12 October 2022; Volume 30, pp. 1–12.
- 'Inception Attacks' on Meta VR Headsets Can Trap Users in a Fake VR Environment, Researchers Found. Available online: https://www.businessinsider.com/meta-headset-inception-attacks-trap-users-fake-environment-study-2024-3 (accessed on 14 April 2024).
- 12. Jo, W.; Kim, S.; Kim, H.; Shin, Y.; Shon, T. Automatic whitelist generation system for ethernet based in-vehicle network. *Comput. Ind.* **2022**, *142*, 103735. [CrossRef]
- 13. Jo, W.; Shin, Y.; Kim, H.; Yoo, D.; Kim, D.; Kang, C.; Shon, T. Digital forensic practices and methodologies for AI speaker ecosystems. *Digit. Investig.* **2019**, *29*, S80–S93. [CrossRef]
- 14. Shin, Y.; Kim, H.; Kim, S.; Yoo, D.; Jo, W.; Shon, T. Certificate injection-based encrypted traffic forensics in AI speaker ecosystem. *Forensic Sci. Int. Digit. Investig.* **2020**, *33*, 301010. [CrossRef]
- 15. Sirivaram, S.B.; Sankardas, R. Deleted File Recovery for the Linux File System (Ext4): Finding the State-of-the-Art. In Proceedings of the 12th International Symposium on Digital Forensics and Security (ISDFS), San Antonio, TX, USA, 29–30 April 2024.
- 16. Deutschmann, M.; Baier, H. Ubi est indicium? On forensic analysis of the UBI file system. *Forensic Sci. Int. Digit. Investig.* **2024**, 48, 301689. [CrossRef]
- Lee, J.; Shon, T. Analysis and Acquisition of APFS Data from a Forensic Perspective. In Proceedings of the 2021 International Conference on Security and Information Technologies with AI, Internet Computing and Bit-Data Applications, National Chung Hsing University, Taichung, Taiwan, 18–29 November 2021.
- 18. Yigit, Y.; Buchanan, W.J.; Tehrani, M.G.; Maglaras, L. Review of Generative AI Methods in Cybersecurity. *arXiv* 2024, arXiv:2403.08701.
- 19. Oh, S.; Shon, T. Cybersecurity Issues in Generative AI. In Proceedings of the 2023 International Conference on Platform Technology and Service (PlatCon), Busan, Republic of Korea, 16–18 August 2023.
- 20. Gupta, M.; Akiri, C.K.; Aryal, K.; Parker, E. From chatgpt to threatgpt: Impact of generative ai in cybersecurity and privacy. *IEEE Access* 2023, *11*, 80218–80245. [CrossRef]
- 21. Karimov, B. Digital Forensic Challenges. Role Sci. Innov. Mod. World 2024, 3, 9–12.
- 22. Kim, D.; Shon, T. Future of Kernel Object-Based Memory Forensics. In Proceedings of the 2023 International Conference on Platform Technology and Service (PlatCon), Busan, Republic of Korea, 16–18 August 2023.
- Noah, N.; Shearer, S.; Das, S. Security and privacy evaluation of popular augmented and virtual reality technologies. In Proceedings of the 2022 IEEE International Conference on Metrology for eXtended Reality, Artificial Intelligence, and Neural Engineering, Italy, Rome, 26–28 October 2022.
- 24. Kim, D.; Oh, S.; Shon, T. Digital forensic approaches for metaverse ecosystems. *Forensic Sci. Int. Digit. Investig.* **2023**, *46*, 301608. [CrossRef]
- 25. Seo, S.; Seok, B.; Lee, C. Digital forensic investigation framework for the metaverse. J. Supercomput. 2023, 79, 9467–9485. [CrossRef]
- 26. Al Ali, T.; Alfulaiti, S.; Abuzour, M. Digital Forensic in a Virtual World: A Case of Metaverse and VR. In Proceedings of the 22rd European Conference on Cyber Warfare and Security, Greece, Athens, 22–23 June 2023.
- Ho, S.L.F. Digital Trails in Virtual Worlds: A Forensic Investigation of Virtual Reality Social Community Applications on Oculus Platforms. Doctoral Dissertation, Purdue University Graduate School, West Lafayette, IN, USA, 2023.
- Raymer, E.; MacDermott, Á.; Akinbi, A. Virtual reality forensics: Forensic analysis of Meta Quest 2. Forensic Sci. Int. Digit. Investig. 2023, 47, 301658. [CrossRef]
- 29. VRcompare. Available online: https://vr-compare.com/ (accessed on 24 April 2024).

- 30. Glass Enterprise Edition 2 System Image. Available online: https://developers.google.com/glass-enterprise/downloads/systemimages (accessed on 17 May 2024).
- 31. Google Kills Its Smart Glasses Project, Shifts to Developing an "Android for AR". Available online: https://mixed-news.com/ en/google-kills-smart-glasses-develops-ar-android/ (accessed on 17 May 2024).

**Disclaimer/Publisher's Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.