Digital Forensic in a Virtual World: A Case of Metaverse and VR

Tayba Al Ali, Sara Alfulaiti, Manal Abuzour, Sheikha Almaqahami and Richard Ikuesan
Computing and Applied Technology Department, College of Technological Innovation, Zayed University, Abu Dhabi, United Arab Emirates

Tiiba-m7md@hotmail.com
sara.alfulaiti@hotmail.com
Manal_mohammed1970@outlook.com
sheikha113k@gmail.com
richard.ikuesan@zu.ac.ae

Abstract: Metaverse is a virtual space where users can interact with each other. It is a combination of virtual reality, augmented reality, and mixed reality. This evolving technology can offer many exciting opportunities that can be used for individuals and businesses. Although this technology has many advantages, people are misusing it for their benefit. Many cyberattacks are occurring in the metaverse world because it has various vulnerabilities and privacy issues. This paper explains four cyberattacks and a case scenario of each attack as it relates to the metaverse. Additionally, this study developed a metaverse forensic framework that can be used to investigate cyberattacks in the metaverse world. Furthermore, this study describes how forensic examiners can conduct a forensic investigation using state-of-the-art forensic solutions and tools. The developed framework can be used by forensic examiners, security researchers, as well as the general scientific community for the security of the metaverse.

Keywords: metaverse forensics, metaverse security, virtual world forensics, metaverse forensic framework.

1. Introduction

Digital forensics is the aspect of information assurance that entails the proactive and reactive process of understanding the who, how, what, and how an event occurred in a digital medium with a probable application in litigation (Adeyemi et al., 2013; Al-Dhaqm et al., 2021; Ellison et al., 2019). Given that digital mediums play a critical role in human daily living, it suffices to highlight that the increasing crime rate provides a frequent need for digital forensics. Recent technological advances illustrate the insatiability of users, with a more targeted drift from physical to virtual reality. Virtual reality (VR) is a technology that enables immersion in a digital environment. It provides promising opportunities for teaching and learning, particularly for the transfer of practical skills. This technology offers benefits, such as time and cost savings, as well as increases in training effectiveness and safety in industries including manufacturing, construction, and healthcare (Ghobadi, Mohsen and M.E. Sepasgozar, 2020). To aid flexibility, a VR world can be placed on removable media which implies that the installed operating systems reside on an external storage device. System administrators have found these tools to be very helpful, as it aids the projection of physical quantity into an intangible environment while maintaining all elements of a physical environment.

The notion of the virtuality continuum has also been extended to include augmented reality (a process in which digital information is overlaid in the real world) and mixed reality. An illustrative depiction of the relationship between these terminologies is further highlighted in Figure 1. Mixed reality (MR) can be expressed as the combination of augmented and virtual reality. In the context of the Metaverse, mixed reality refers to the integration of MR technologies into the metaverse, allowing users to experience and interact with the virtual world in a more immersive and interactive way. In recent years, the application of VR technology has increased across several sectors (Ghobadi, Mohsen and M.E. Sepasgozar, 2020). One of these is the construction sector, which has the potential to provide stakeholders with an immersive experience of the intended architectural masterpiece. It also provides the potential to identify risks and faults in design to some stakeholders (Ghobadi, Mohsen and M.E. Sepasgozar, 2020). Similarly, the entertainment and gaming industry share great benefits from VR as it provides a better interactive platform for user immersive experience. However, with these advantages comes a high probability of misuse. The VR platform can be leveraged to conduct several cyber-related attacks including but not limited to insider misuse, espionage, information leakage, impersonation attack, cyber sabotage, misinformation dissemination, cyberstalking, information theft, as well as covert recruitment.

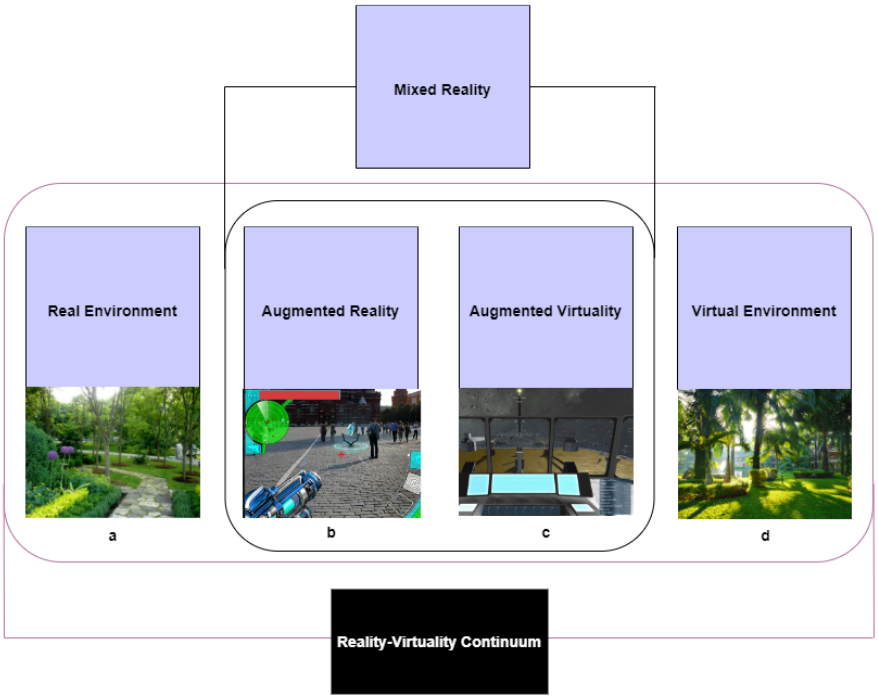

Figure 1: Reality-Virtuality Continuum that Indicates the Stages Between Real and Virtual Environment (Ghobadi, Mohsen and M.E. Sepasgozar, 2020)

However, the list of potential crimes will only grow as more people use VR technology and its associated advances (Aloqaily et al., 2022; Chow et al., 2023; Qin et al., 2022; Wang et al., 2022). This may further include financial fraud, ransomware, and phishing (INTERPOL, 2022; Odeleye et al., 2023; Vondrek et al., 2022). Whilst the Metaverse provides some inherent mechanisms for preventing some attacks, through deterrence and detection, some of these risks could be relatively difficult to investigate. A probable justification for this assertion is that both legal and illegal actions could be carried out using the same content, albeit, with a different context. Also, a virtual world requires some degree of creativity which is unique to each platform. Thus, some actions which are considered illegal in the physical environment may be accepted in some Metaverse platforms, as an immersive experience. Therefore, not all malicious act in the real world is illegal in the virtual environment. VR technology is one of the technologies used in the Metaverse experience. Any other technology that replicates or improves real-world experiences with technology may be referred to as the metaverse. According to GlobalData ("The Outlook of Metaverse Market 2022-2030," 2022), from 2022 to 2030 the worldwide metaverse market would increase from USD 22.79 billion to USD 996.42 billion, with a compound annual growth rate (CAGR) of 39.8%. It is the upcoming major trend in digital media, while VR and AR are key technologies fostering its growth ("The Outlook of Metaverse Market 2022-2030," 2022).

Metaverse is being used nowadays dramatically in advanced blockchains where Bitcoin, Ether, and Dogecoin are all powered by blockchain technology. The advanced blockchain facilitates the development of digital assets known as non-fungible tokens (NFTs) and applications while serving as a distributed ledger for recording peer-to-peer transactions (LeewayHertz, 2022). Other than that, Businesses are moving away from the two-dimensional surface of e-commerce and embracing lifelike virtualized worlds for a meaningful experience thanks to the growing application of the Metaverse. Owners of e-commerce businesses may conduct trade formalities including product inspection, negotiations, and transaction closure with merchants in a virtual setting. Additionally, rather than depending on digital marketing strategies, companies may better impact customers by creating engaging and realistic marketing material (LeewayHertz, 2022). However, recent statistics revealed that the metaverse poses diverse dangers to Internet users. This includes addiction, mental and physical health challenges, and privacy issues. A breakdown of the distribution is further presented in Figure 2.

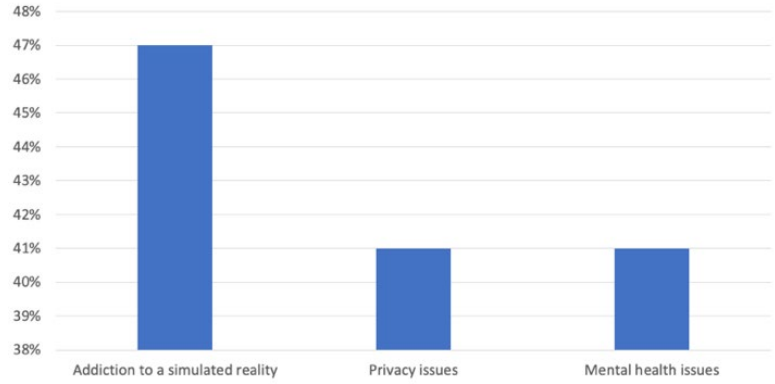

Figure 2: Dangers of the Metaverse According to Internet Worldwide in 2021 (Statista, 2022)

As illustrated in Figure 2, Users and society at large may experience certain unforeseen effects of the metaverse. 47% of the sampled population asserts that addiction to a virtual or simulated environment is a potential menace that should be adequately remediated. Furthermore, given that there is a need to investigate crimes associated with digital platforms, law enforcement, and digital forensics units must create and maintain an efficient quality assurance system to ensure that potential digital evidence (PDE) is gathered, kept, reviewed, or transmitted in a way that protects the correctness and dependability of the PDE. Standard operating procedures (SOPs) and/or models that adhere to the chain of custody are the initial component of this system. These rely on the digital forensics "process-phase-procedure-task-subtask" sequence (Bulbul et al., 2013). To the best of the Authors' knowledge, this is the first study that attempts to provide a typical SOP for conducting a digital investigation in a virtual platform using potential cyber-attacks. The remainder of this manuscript is structured as follows: in the next section, the methodology adopted in this study is presented. This is followed by a hypothetical case study and the result of the experimental process. A concise discussion and potential future works are thereafter provided.

2. Methodology

This study leverages an experimental approach to metaverse framework development. To do so, the operational framework shown in Figure 3 is followed. The operational framework comprises 3 phases which are further explained.

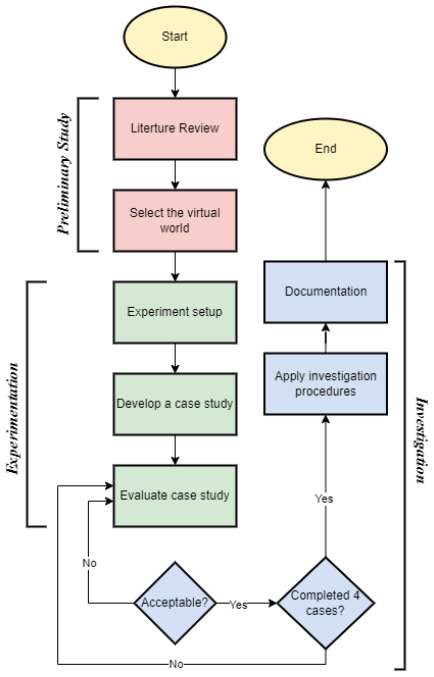

Figure 3: Operation Framework Flow Model

Given that the goal of this paper is to develop a metaverse forensic framework that examiners can follow to be able to investigate a metaverse case. This was achieved by conducting an extensive literature review where a particular category of metaverse was selected, which is Virtual Reality (VR), precisely the fully immersive virtual reality. This virtual world of interest was selected because it offers a state-of-the-art on metaverse. Virtual reality, or VR, is a technology that creates a simulation of a 3D environment that enables the user to interact and explore a virtual surrounding that simulates a real-world experience through the senses of the user ("The Outlook of Metaverse Market 2022-2030," 2022). After the technology of the VR was selected, an experimental setup was established. The experimental setup includes setting up an account in Oculus VR and integrating (wired or wirelessly) a Meta Quest VR headset. Steps to create an Oculus account and interfacing the Meta Quest VR headset to a workstation are further provided in Figures 3 and 4. The workstation comprises a core i7 10th generation, 32GB RAM, and runs on a Microsoft Windows 10 Professional. To ascertain the experiment process, case studies were developed and evaluated. Each case study describes a cyberattack scenario applicable within the virtual reality world. When a case study was created, it was reviewed iteratively until a forensic investigation process can be initiated. This implies that each attack aligns with Locard's exchange principle. Using this heuristic selection approach, a total of four cases were developed, upon which the investigation and documentation stages are undertaken. The result of the respective case studies is presented in the proceeding section.

3. Result and Analysis

To enter the metaverse, users will take the form of digital avatars that are complemented with VR/ AR technologies that help in ensuring a sense of existence in the metaverse. The user can control the environment, look around at any scene, or interact with the objects in the scene using the headset. Newer headsets such as the Oculus Rift, PlayStation VR, and Samsung Gear VR tend to provide better interactivity. The Meta Quest VR headset is adopted in the first scenario. The process model provided in Figure 4 describes the process of using this headset. This is a stepwise process required to access the Oculus account.

After creating an account, the Meta Quest application was installed on the workstation, and user access was granted by logging into a newly created account. Once logged in, the VR Meta Quest headset can be connected in two ways: wired or wirelessly. The process model presented in Figure 5 was used to establish the VR headset connectivity in this study, both in wired and wireless modes. These steps were adapted for this study as they can enhance experimental repeatability. To substantiate the need for a forensic investigation framework, this study leverages an attack approach to scenario development. These are presented in the next subsection.

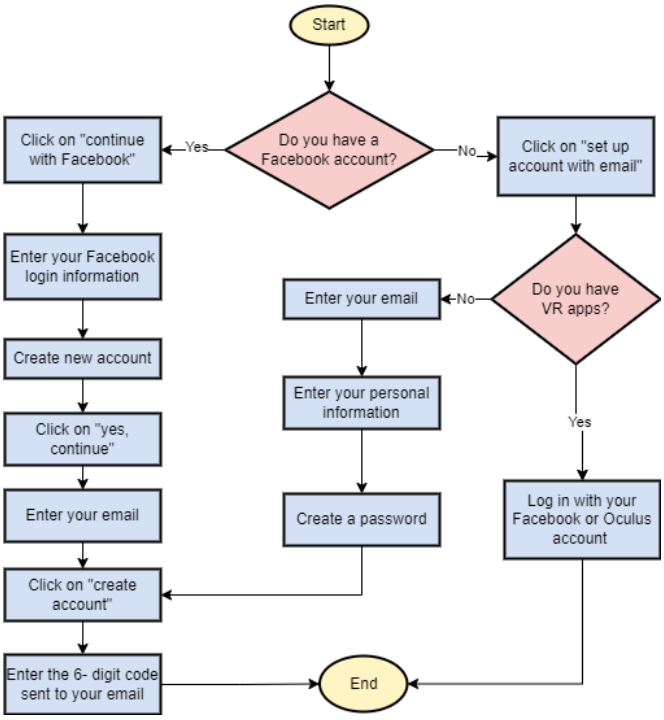

Figure 4: Signing Up for Oculus Account Flow Model

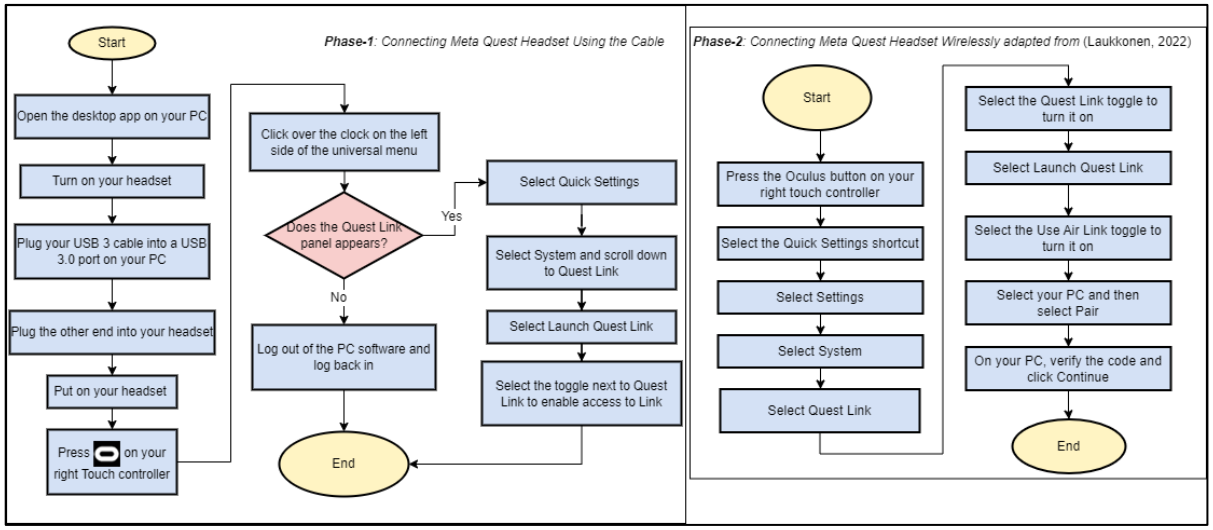

Figure 5: MetaQuest Headset Process model

3.1 Downloading Malicious Codes

An employee, Mr. Mark, for Globe-Star PLC is responsible for creating an interactive VR environment for entertainment purposes. Thus, he used a special workstation PC in the company to connect his Head-Mounted Device (HMD) to download his special software. However, one day the IT team informed him that his PC was involved in downloading malicious codes that are embedded VR based games. Mr. Mark told them that he didn't download this application and he was only doing his job. To investigate such a case, forensic investigators can prove that Mark was not the one who downloaded this application by first collecting the evidence, the VR headset and the computer. Second, secure the evidence by storing it in a secure forensic lab. Third, collect information about the main user and the tools that were used as well as the software. Fourth, collect data by connecting the VR headset to a computer and running String VR on it. Using these steps, the software will generate four reports:

1. *Device.txt*: stores the list of devices that are connected and other important information, for example, which connected ports.
2. *Logs.txt*: contains the logs of different users with the accurate timing, as well as any inside and outside processes that transverse outside and inside the network.
3. *Main.txt*: contains general information about the software used and how devices connect to it, what time, which port, and other information.
4. *Raw.txt*: stores raw information that is not yet processed to give specific information.

Fifth, extract data using FTK Imager. This program will allow them to facilitate data viewing and imaging. The output of the analysis is further shown in Figures 6 and 7.

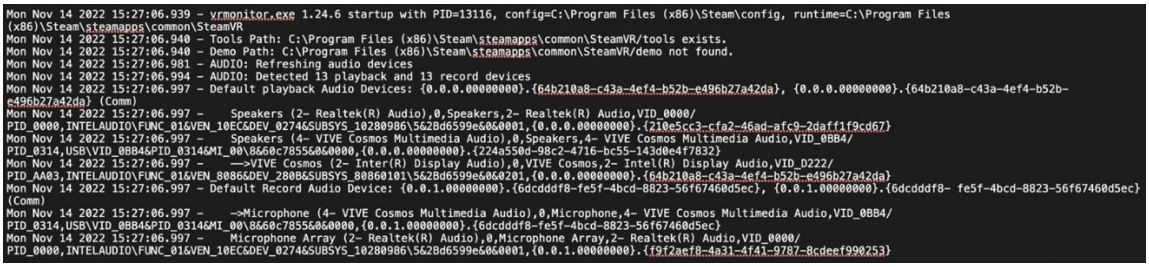

Figure 6: Devices Used to Access the Software

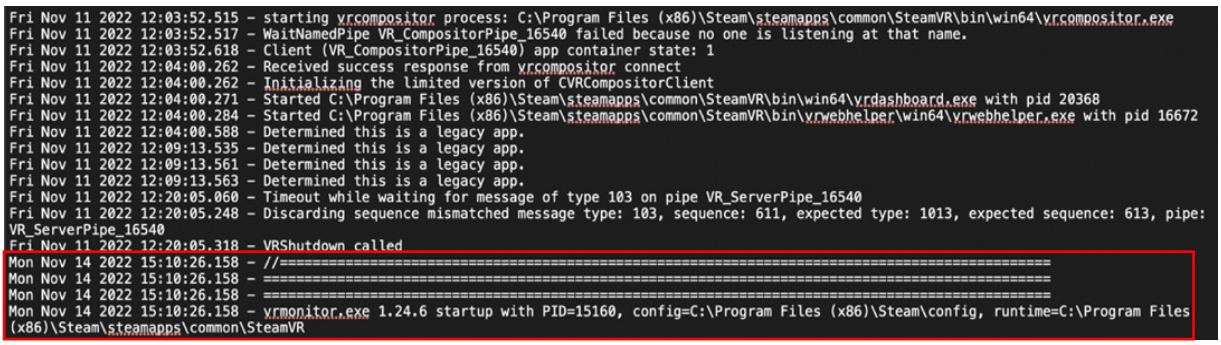

Figure 7: The Device Logins by Mr. Mark

The log file displays the specific date and time Mark used the software and how he used it. The evidence shows that he was inside the workstation place on the dates: 11/11/2022 and 14/11/2022. According to the permission granted to Mark, he usually accessed the workstation on Monday and Friday only. On 15/11/2022, an unknown user was found, and the user created an account with the profile name *8000****. The result of the FTK image allowed for the discovery of all downloaded games during the days that Mark wasn't in the workstation (Date →15/11/2022). The device that was used is presented in Figures 8a and 8b. Furthermore, the log file, Figure 8c, showed that there was a log attempt between 5:00 pm and 6:00 pm on 15/11/2022. This corroborative evidence can be used to support the claim of Mr. Mark, as he was not within the premise on the stipulated day.

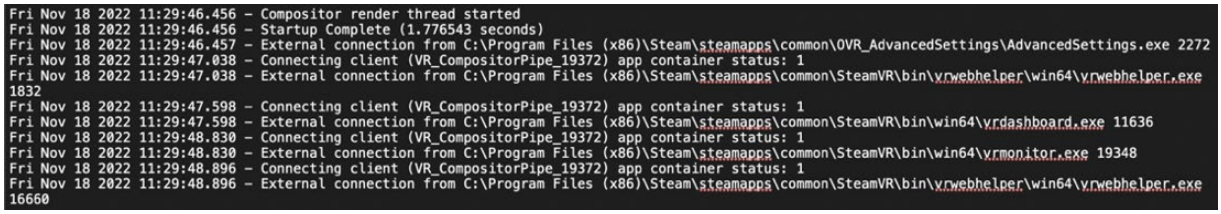

Figure 8a: Date and Time Mr. Mark Connected and Accessed the Workstation.

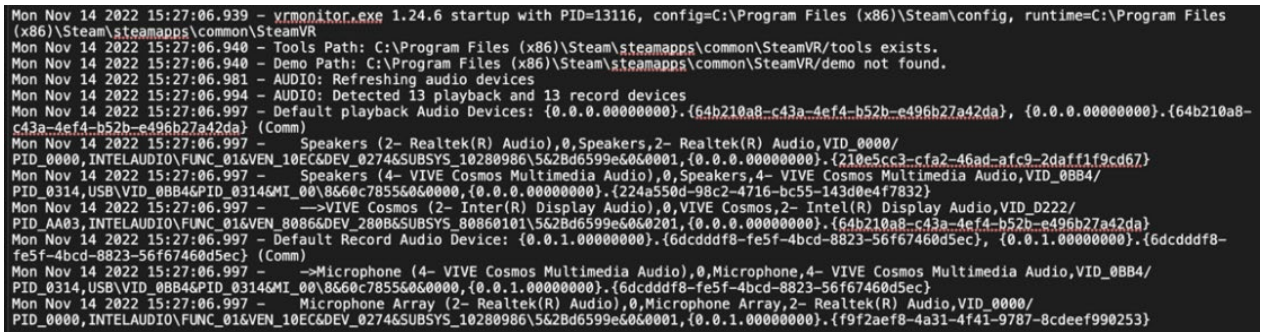

Figure 8b: Devices Used

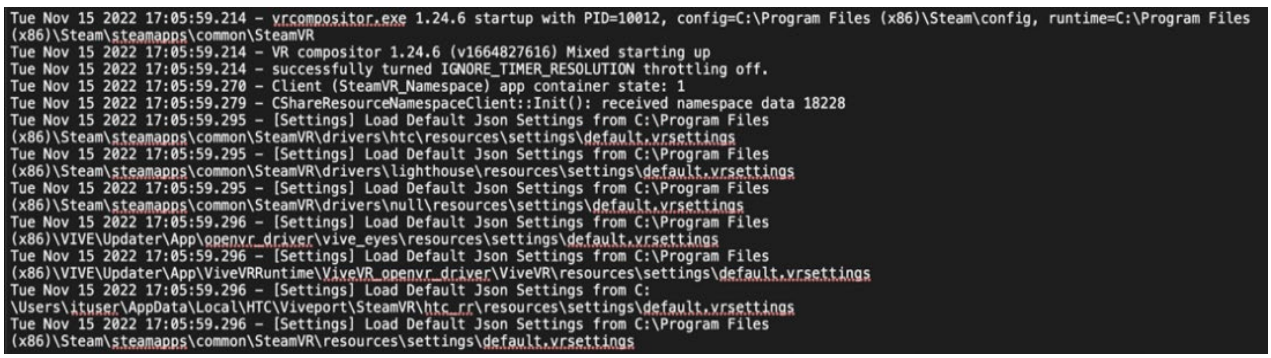

Figure 8c: Date and Time of Mr. Mark's Account Logins.

As a result, the forensic examiners can conclude that Mr. Mark is not involved in the misuse raised against him because the login and the application downloaded prove that Mr. Mark was not available in the vicinity during the time of the incident. In addition, the person who accessed Mr. Marks' computer left traces of information such as a username that could be used for attribution.

3.2 Case 2: Impersonation

JohnSmith and his friend TashaCoin share all online login credentials irrespective of the platform. Both of them have the Oculus VR headset and their account credential. As JohnSmith was attempting to login into his oculus account, he saw TashaCoin looking at the keyboard but he didn't say anything because he trusts his friend. One day, JohnSmith accessed his account and found some strange applications on his PlayStation account. Furthermore, some strange messages with unknown entities that relate to bullying were also found in the account. Given that JohnSmith did not carry out these actions, and TashaCoin claimed ignorance, there was a need to investigate this case to gain insight into the perpetrator. To do so, a forensic examiner begins by logging into JohnSmith's Oculus account using this link https://auth.meta.com/. Once logged in, navigate to settings>Account > view your information > Security and login information. In this directory, the dataset for event correlation can be extracted from the account. The information typically includes active sessions, location history, devices used, recently viewed items, login history, as well network-related potential digital evidence (PDE). As a PDE, the network parameter of interest includes IP address, MAC address, and well geolocation data. The experimental approach and outcome are further elucidated:

1. We logged into the Oculus account through this link: https://auth.meta.com/
2. Navigate to Settings > Account > View your information > Security and login information. The output of the experimental process is further presented in Figure 9.

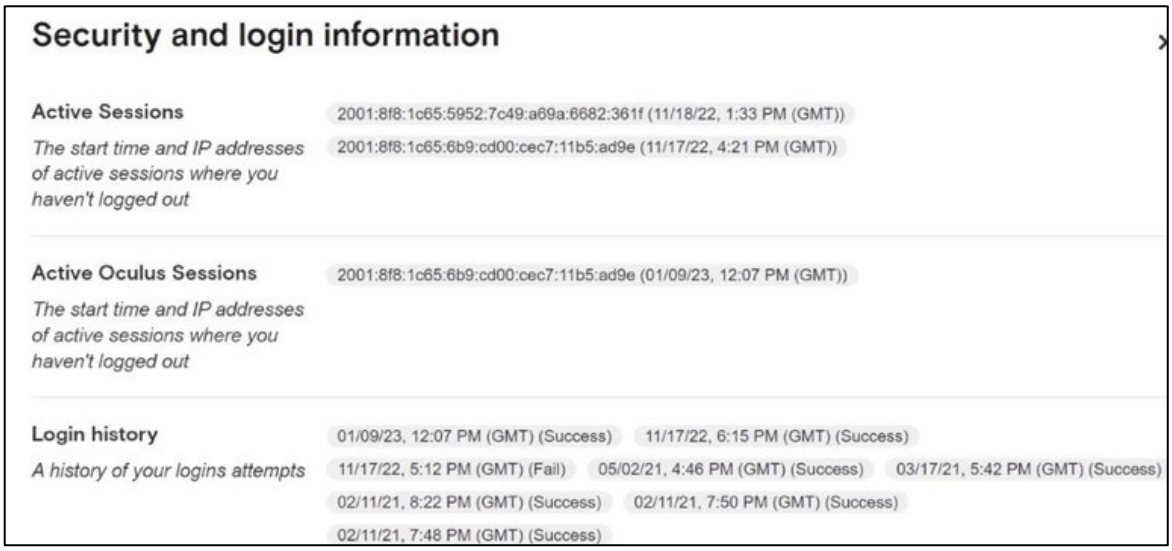

Figure 9: Result of the Experimental Process of Impersonation Investigation

3. Two IPV6 addresses are displayed in the active session which indicates that two people logged in to this account.
4. Investigating further, the command "ipconfig/all" was instantiated on the workstation terminal. It revealed the IPV6 address of 2001:8f8:1c65:6b9:cd00:cec7:11b5:ad9e.
5. To confirm this, the Ipv6 of all suspects was analyzed. This revealed IP address of TashaCoin was 2001:8f8:1c65:5952:7c49:a69a:6682:361f.
6. This showed that TashaCoin logged into JohnSmith's account on 11/18/2022 at 1:33 PM (GMT).

3.3 Case 3: Data Leakage

There is a student named Asma who owns a VR headset. One day she decided to bring her headset to the university so her friends can play with it. After they were done playing, they left the PC running and went to the cafeteria to get some food. However, they spent hours eating and the PC was still unlocked. When they got back their friend told them that Asma's information was leaked including her credit card details. Asma realized that

someone used the PC and gone through her account while they were gone. She looked around and saw a lot of students in the lab and when she asked them who used the PC, they all said that three students used that computer. She was unable to know which one did it as all of them claimed that they were just finishing their university work. Forensic examiners can investigate the source of the leak by capturing and examining the keystroke forensics and the mouse dynamics of the computer. This will allow them to collect data about the actions that were done on the computer. Moreover, they will be able to know which pattern belongs to which suspect. Once the data is collected and they know when the attack happened, they can go to the keystroke database and extract the keystroke and mouse dynamics and analyze them. Moreover, they can now view the surveillance camera video and create the timeline of the attack. Once they reach the time of the attack, they will be able to know which student leaked Asma's information as they will appear on the video.

3.4 Case 4: Malware

Sheikha has an Oculus Rift VR headset that she uses all the time. One day when she tried to start up her PC, all her files were corrupted. She realized that an attacker might have installed malware on her computer as she clicked on a suspicious link yesterday while she was using her Oculus account. Sheikha started to get worried as all her files on the computer were important. Forensic examiners can conduct their investigation by going through the event log, and network log, and checking the running processes. As a result, they will be able to collect evidence and see how the attacker was able to install the malware and track him down. A summary of the overall forensic usefulness of the explored case studies is provided in Table 1.

Table 1: Forensic Usefulness of the Metaverse Case studies

Case studies	Attack Type	Potential digital forensic evidence location	Nature of the potential evidence
Case - 1	Overlay attack	Oculus VR headset	non-volatile
Case - 2	Impersonation	Oculus account settings	non-volatile
Case - 3	Data leakage	Computer database (keystroke and mouse dynamics) and the surveillance camera	non-volatile
Case - 4	Malware	Event log, and network log, and checking the running processes	non-volatile

4. Discussion and Recommendation

With reasonable certainty, it can be asserted that all VR systems are vulnerable to these types of attacks as explored in the respective cases. With such technological improvement, there is a greater need for enhanced security. As asserted in existing studies (Odeleye et al., 2023; Vondrek et al., 2022), the metaverse presents a platform for enhanced user interactivity which can be leveraged for several nefarious activities. With the growing adoption of the metaverse, especially in the e-commerce industry, it is essential to develop a threat-based use-case scenario for metaverse security. Given that the metaverse could transcend traditional online interaction into a more personal immersive ecosystem, the potential consequence of malicious attacks could lead to psychological and physical defects. Whilst the current study targeted the Oculus VR system, the Authors believe that the attacks identified in the cases can happen to all VR systems. The security of the VR and its safety features need further protection and improvement. Although there are some benefits in having the user manually enter their private information to create their account, gaining access to this data should be guarded. The user's data should be protected so that the attacker cannot have access to the user's data.

To protect the data, this study found that it is better to encrypt such data as it was revealed that some data were stored in plaintext. Moreover, access to the services should be restricted, as this will aid integrity preservation and data usefulness. Virtual world data is vulnerable to many attacks in comparison with standard screens given that virtual reality (VR) offers new ways to perceive data. Also, it is inherently portable and offers more connectivity possibilities. Existing findings and the implications found in security studies include manipulatable 3D objects used for authentication, which can be correlated to the considerable cognitive effort needed to simultaneously monitor many visual channels, including hand motions while seeing the manipulations (Mathis et al., 2020). The metaverse world can exploit several opportunities in the coming years, as it requires

multisensory interactions with several technologies: virtual environments, digital objects, and people immersive technologies, virtual reality (VR), augmented reality (AR), mixed reality (MR), and extended reality (XR) (Trunfio & Rossi, 2022). These technologies support the creation of the metaverse and facilitate immersive experiences in the digital world. Virtual reality technology provides users with a connected experience in the metaverse. On the other hand, augmented reality expands the use of virtual reality by overlaying digital information onto the physical environment. XR is an extended reality, a term used to include VR, AR, and MR. XR is used for virtual commerce or v-commerce to create computer-mediated indirect experiences (Trunfio & Rossi, 2022). With the growing need for virtual reality, specifically with the Metaverse, it is evident that cybercrime will evolve.

The findings from this current reveal the relevance of logs and systems documentation. This includes the device log, as well as the connectivity log. As highlighted in Table 1, these logs could be leveraged for a different context. Furthermore, from a forensic standpoint, it will be helpful to forensics examiners as they will know how they could conduct their investigation based on what attack happened. This also relates to the reliability and admissibility of forensic evidence. Understanding that some content of the VR headset can be manipulated by an adversary presents a logic for further analysis of results obtained from the virtual world. Forensic examiners would then be required to provide a suitable means to identify the users and corroborate claims where applicable. Studies have alluded to the need for a forensic readiness approach to volatile environments (Lagrasse et al., 2020; Munkhondya et al., 2019, 2020) to ensure potential evidence availability and reliability. This is specifically applicable in the virtual reality platform where potential evidence might not be available after the occurrence of the incident. Whilst the logs considered in this current study relate to non-volatile PDE, this might not be the case for some special cases. For instance, a situation whereby an ongoing attack is to be investigated while the malicious actor is still using the platform. Therefore, the findings from this study provide a veritable process model for investigating incidents in the metaverse, based on the devices used. The finding in the study is, however, limited to log-related evidence correlation and event corroboration. Further study will be carried out on the feasibility of developing a real-experience metaverse crime which could leverage approaches such as impersonation of known users, identity theft, as well as false information dissemination. These attacks are postulated to require a near-real-time potential digital evidence collection and event correlation. This is, in addition, to the observable logs. Furthermore, the exploration of such processes would lead to the development of a forensic readiness mechanism for metaverse forensics. The latter observation can complement the find in this study, but developing a process for a forensically ready log-generation mechanism.

5. Conclusion and Future Works

Metaverse technology employs avatars and infrastructure, platforms, and gadgets that allow immersive experiences, and create a mixed-reality environment where people and objects may interact synchronously and live outside of time and space. Virtual reality is a useful technology that helps people interact with each other. Though platforms such as Metaverse create an environment for interaction for people who are worlds apart, there are cybersecurity-related risks associated with such platforms which may compromise the privacy of users on such platforms. This study explored how forensic investigators can leverage various logs within the metaverse platform to conduct an investigation. However, in the case of privacy violations and other forms of cyberattacks, Digital forensics tools such as FTK Imager can be used to investigate and trace the specific user actions that led to the attack/violation, which could uncover the real culprit for legal actions.

References

Adeyemi, I. R., Razak, S. A., & Azhan, N. A. N. (2013). A review of current research in network forensic analysis. *International Journal of Digital Crime and Forensics*, *5*(1), 1–26. https://doi.org/10.4018/jdcf.2013010101

Al-Dhaqm, A., Ikuesan, R. A., Kebande, V. R., Razak, S. A., Grispos, G., Choo, K. K. R., Al-Rimy, B. A. S., & Alsewari, A. A. (2021). Digital Forensics Subdomains: The State of the Art and Future Directions. *IEEE Access*, *9*, 152476–152502. https://doi.org/10.1109/ACCESS.2021.3124262

Aloqaily, M., Bouachir, O., Karray, F., Ridhawi, I. Al, & Saddik, A. El. (2022). Integrating Digital Twin and Advanced Intelligent Technologies to Realize the Metaverse. *IEEE Consumer Electronics Magazine*, 1–7. https://doi.org/10.1109/MCE.2022.3212570

Bulbul, H. I., Yavuzcan, H. G., & Ozel, M. (2013). Digital forensics: An Analytical Crime Scene Procedure Model (ACSPM). *Forensic Science International*, *233*(1–3), 244–256. https://doi.org/10.1016/J.FORSCIINT.2013.09.007

Chow, Y., Susilo, W., Li, Y., Li, N., & Nguyen, C. (2023). *Visualization and Cybersecurity in the Metaverse : A Survey*.

Ellison, D., Ikuesan, R. A., & Venter, H. S. (2019). Ontology for Reactive Techniques in Digital Forensics. *2019 IEEE Conference on Application, Information and Network Security, AINS 2019*, 83–88. https://doi.org/10.1109/AINS47559.2019.8968696

Ghobadi, Mohsen and M.E. Sepasgozar, S. (2020). Smart Cities and Construction Technologies. In *Smart Cities and Construction Technologies*. https://doi.org/10.5772/intechopen.86103

INTERPOL. (2022). *INTERPOL launches first global police Metaverse*. International Criminal Police Organization. https://www.interpol.int/en/News-and-Events/News/2022/INTERPOL-launches-first-global-police-Metaverse

Lagrasse, M., Singh, A., Munkhondya, H., Ikuesan, A., & Venter, H. (2020). Digital forensic readiness framework for software-defined networks using a trigger-based collection mechanism. *Proceedings of the 15th International Conference on Cyber Warfare and Security, ICCWS 2020*, 296–305. https://doi.org/10.34190/ICCWS.20.045

Laukkonen, J. (2022). *How to Connect Meta (Oculus) Quest 2 to a PC Wirelessly*.

LeewayHertz. (2022). Metaverse Use Cases and Benefits. In *LeewayHertz*.

Mathis, F., Williamson, J., Vaniea, K., & Khamis, M. (2020). RubikAuth: Fast and Secure Authentication in Virtual Reality. *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–9. https://doi.org/10.1145/3334480.3382827

Munkhondya, H., Ikuesan, A. R., & Venter, H. S. (2020). A case for a dynamic approach to digital forensic readiness in an sdn platform. *International Conference on Cyber Warfare and Security*, 584--XVIII.

Munkhondya, H., Ikuesan, A., & Venter, H. (2019). Digital Forensic Readiness Approach for Potential Evidence Preservation in Software-Defined Networks. *14th International Conference on Cyber Warfare and Security*, 268–277. https://search.proquest.com/docview/2198531158?accountid=169469

Odeleye, B., Loukas, G., Heartfield, R., Sakellari, G., Panaousis, E., & Spyridonis, F. (2023). Virtually secure: A taxonomic assessment of cybersecurity challenges in virtual reality environments. *Computers and Security*, *124*. https://doi.org/10.1016/j.cose.2022.102951

Qin, H. X., Wang, Y., & Hui, P. (2022). *Identity, Crimes, and Law Enforcement in the Metaverse*. http://arxiv.org/abs/2210.06134

Statista. (2022). Benefits of the metaverse worldwide 2021. *Statista Research Department*. https://www.statista.com/statistics/1285117/metaverse-benefits/

The Outlook of Metaverse Market 2022-2030. (2022). In *GlobalData*.

Trunfio, M., & Rossi, S. (2022). Advances in Metaverse Investigation: Streams of Research and Future Agenda. *Virtual Worlds*, *1*(2), 103–129. https://doi.org/10.3390/virtualworlds1020007

Vondrek, M., Baggili, I., Casey, P., & Mekni, M. (2022). Rise of the Metaverse's Immersive Virtual Reality Malware and the Man-in-the-Room Attack & Defenses. *Computers & Security*, *September*, 102923. https://doi.org/10.1016/j.cose.2022.102923

Wang, Y., Su, Z., Zhang, N., Xing, R., Liu, D., Luan, T. H., & Shen, X. (2022). A Survey on Metaverse: Fundamentals, Security, and Privacy. *IEEE Communications Surveys and Tutorials*, 1–32. https://doi.org/10.1109/COMST.2022.3202047