Forensic Science International: Digital Investigation 47 (2023) 301658

Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

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

Virtual reality forensics: Forensic analysis of Meta Quest 2

Emma Raymer [a], Áine MacDermott [a], Alex Akinbi [b,*]

[a] School of Computer Science and Mathematics, Liverpool John Moores University, Liverpool, UK
[b] Department of Computing and Mathematics, Manchester Metropolitan University, Manchester, UK

ARTICLE INFO

Keywords:
Virtual reality
Meta Quest 2
VR Forensics
Digital forensics

ABSTRACT

The Meta Quest 2 is one of the most popular Virtual Reality (VR) entertainment headsets to date. The headset, developed by Meta Platforms Inc., immerses the user in a completely simulated environment. Some VR environments can be shared over the Internet to allow users to communicate and interact with one another and share their experiences. Unfortunately, the safety of these VR environments cannot always be guaranteed, generating a risk that users may be exposed to illicit online behaviour in the form of online harassment, grooming, and cyberbullying. Therefore, forensic examiners must be able to conduct sound forensic analysis of VR headsets to investigate these criminal investigations. In this study, we conduct digital forensic acquisition and analysis of the Meta Quest 2 VR headset. Analysis of the forensic image exemplified that there were several digital artefacts relating to user activities, device information and stored digital artefacts that can be extracted in a forensically sound manner. The main contributions of this study include a detailed description of the forensic acquisition process, identification of internal file storage locations, and recovery and analysis of digital artefacts that can be used to aid VR forensic investigations.

1. Introduction

Virtual Reality (VR) is described as a simulated experience that can be similar to or completely different from the real world. Thereby creating alternative realities that could allow users to represent themselves as they wish, in just about any format they desire through their avatars. Current virtual reality systems aim to fully immerse users in a simulated environment. To achieve this immersion, VR systems rely on technology that stimulates the senses. Head-mounted VR headsets feature high-resolution displays and motion tracking to visually immerse the user from a first-person perspective. An individual using VR equipment can look through the virtual world, move around in it, and interact with virtual characters or objects. The effect is commonly created by VR headsets consisting of a head-mounted display with a small screen in front of the eyes but can also be created through specially designed rooms with multiple large screens. Virtual reality typically integrates audio and video feedback but may also allow other types of sensory and force feedback through haptic technology. Applications of VR include entertainment (mostly online video games), education (for instance medical, industrial, or military training), business communications (such as virtual meetings) and use in social media. This convergence of VR applications and experiences accessed using VR equipment has been described as the metaverse (Park and Kim, 2022). The market size for VR technology and the metaverse is predicted to reach an estimated $393 billion by 2025 and spread into other diverse domains including Artificial Intelligence (AI), telemedicine and robotics. VR headsets are used to immerse the user into a simulated virtual environment which they can interact with in real time by performing movements and gestures in the real world. This simulated environment may contain a new experience for the user to try or may be used for other entertainment purposes such as gaming, web browsing, video watching and socialising.

Since VR simulates almost real-world experiences, real-world crimes such as virtual assaults, online grooming, virtual groping and rapes, abuse, intimidation, cyberbullying and simulated sexual misconduct with an individual's avatar are being perpetrated and have been reported in several instances (Dugga, 2014; Qamar et al., 2023). A woman recently experienced severe psychological trauma after her avatar was sexually assaulted in the virtual world of Meta's VR platform. The victim felt the full emotional impact of the virtual sexual assault as if it happened in real life. This disturbing incident reveals the potential for realistic virtual experiences to inflict real mental anguish and highlights the need for better safety protections in VR spaces. An undercover researcher posing as a 13-year-old girl witnessed grooming, sexual

* Corresponding author.
E-mail address: a.akinbi@mmu.ac.uk (A. Akinbi).

https://doi.org/10.1016/j.fsidi.2023.301658
Received 10 June 2023; Received in revised form 14 September 2023; Accepted 20 October 2023

material, racist insults, and a rape threat in the virtual reality world called VRChat (Sheera & Kellen B., 2021). Some apps in the virtual reality metaverse have also been described as "dangerous by design" by the UK children's charity, NSPCC (Crawford and Smith, 2022) due to oversight by the app developers. These concerns have facilitated the UK government's consideration to include the metaverse in the proposed online safety legislation (Online Safety Bill, 2023) as there is no specific standard or privacy compliance certificate available for these immersive VR applications (Happa et al., 2021). Currently, investigating online sexual predatory conversations and abuse on social media and gaming platforms is already a daunting task for law enforcement and digital investigators due to the volume, variety and rate of these types of incidents (Akinbi and Ojie, 2021; Ngejane et al., 2021). These challenges are predicted to grow and will create a unique set of challenges when investigating such crimes in VR environments. For forensic examiners, the significant challenges they will face include the identification, collection, preservation, and reporting of digital evidence in these environments.

As of the time of writing, the Meta Quest 2 (also known as the Oculus Quest 2) is the newest generation VR headset developed by Meta Platforms Inc. This generation of VR explores the possibilities of the technology, which enables the user to become immersed and move freely within a simulated environment, without being physically connected to numerous hardware devices. Instead, projection and sensor tracking technology are all contained within the headset itself, which is then used in conjunction with handheld controllers. The 'tether-free' nature of the technology makes the headset much more portable, which is ideal for fully immersing users in a virtualized environment. This also allows the user to easily carry the headset between different locations where it can be used, however, an internet connection is still required to access any online services. Analysis of data artefacts makes it possible to identify the owner of the headset and the previous locations it has been online.

As online-hosted virtual environments for the Meta Quest 2 headset can be accessed by any user, these environments may not always be classified as 'safe' for all users. Several malicious behaviour and communications have been identified across the Meta VR platform, including behaviours such as cyberbullying, grooming, and virtual harassment. For example, research on the popular social application VRChat has identified environments that are full of inappropriate and harmful material, masquerading as child-safe environments (Crawford and Smith, 2022). As a result, VR users may have a deeper and longer-lasting emotional and psychological response to bullying or harassment, which could severely affect users who already suffer from mental health issues. Furthermore, users could become more susceptible to manipulation which could lead to them falling victim to grooming or similar abuse.

When situations like this arise, law enforcement must launch investigations into such incidents. These investigations require evidence which can create a timeline of events and link suspected perpetrators to the crime including the identification of possible victims.

In this paper, the focus and main contributions include the forensic acquisition and analysis of digital artefacts recovered from the Meta Quest 2 VR headset. The study identifies the storage locations where relevant forensic artefacts can be found and data associated with actions carried out by a typical user of the headset. To ensure results from our analysis can be reproduced, we described our analysis methodology which includes the creation of a user profile and a list of actions in our experiment design.

The remainder of this paper is organized as follows. In Section 2 we present background information on the Metaverse and the Meta Quest 2. Section 3 highlights related works in this domain. In Section 4 we outline our investigative methodology and testing parameters and tools. Section 5 details our forensic analysis findings, specifically live data artefacts, backup data artefacts, and internal storage artefacts. Section 6 evaluates our research questions and discusses our results, and we highlight some limitations in Section 7. We conclude our findings and identify avenues for future work in Section 8.

2. Metaverse and the Meta Quest 2

Meta Platforms, Inc. often branded as just Meta, is an information technology company which owns the majority of the most popular social media platforms, including Facebook – 2.934 billion monthly active users, Instagram – 1.386 billion monthly active users, Messenger – 1 billion monthly active users, and WhatsApp – 2 billion monthly active users (Kretzschmar et al., 2020). However, the company recently rebranded from Facebook, Inc. to Meta Platforms, Inc. to reflect its focus on building the metaverse" (Heath, 2021). Meta claims the "metaverse" is "the next evolution in social connection and the successor to the mobile Internet" and consists of a "set of 2D and 3D digital spaces, which you can move seamlessly between" and will allow users to "connect, work, play, learn and shop" (Meta, 2022). The Metaverse will be accessible to everyone via various devices such as a phone, computers or virtual reality devices (Meta, 2022). Meta has begun building their Metaverse by investing in the development of various VR and AR devices, including Meta Quest VR headsets, Meta Portal video calling devices and Smart glasses (Meta, 2022). As of 2022, Meta reportedly invests $10 billion annually into their Metaverse, hoping that their company will lead the "next big computing platform" against their competitors such as Sony (Bezmalinovic, 2022).

Meta's most popular VR headset has recently dominated the VR headset gaming market as reported by online gaming retailer Steam in its October 2022 'Steam Hardware & Software Survey. The survey reported that the Oculus Quest 2 (also known as the Meta Quest 2), makes up 41.49 % of all VR headset models used to play compatible games purchased from the Steam library (Steam, 2022). This headset immerses the user in a simulated environment. The headset contains a Qualcomm Snapdragon XR2 processor, an LCD panel with a per-eye resolution of 1832x1920 and a refresh rate of 120 Hz, an operating system based on Android 10, and 128 GB or 256 GB of internal storage (Meta, 2022).

3. Related works

Previous research studies have focused on forensic analysis of multimedia devices including streaming platforms, gaming consoles (Moore et al., 2014) and gaming platforms (Barr-Smith et al., 2021; Davies et al., 2015; Hadgkiss et al., 2019; Murias et al., 2023; Taylor et al., 2019). However, digital forensic investigation of VR environments and devices is still in the nascent stages with limited research focused on the forensic acquisition and analysis of VR headsets (Casey et al., 2019). conducted preliminary forensic analysis of the HTC Vive and Oculus Rift VR headsets. The researchers developed an open-source plugin called Vivedump for the Volatility Framework used in the analysis of memory dumps of the device's volatile memory. Results from the study showed that the device status data can be reconstructed from artefacts recovered from the volatile memory of the HTC Vive headset. However, since the data recovered resides in volatile memory, the forensic artefacts are non-persistent once the device has been powered off. Moreover, the study was limited to the recovery of VR runtime and global data and did not consider user-related data or artefacts valuable to forensic investigations (Yarramreddy et al., 2018). conducted the forensic analysis of HTC Vive and Oculus Rift VR headsets. The results from the study showed data artefacts and network traffic related to Bigscreen, Steam and Facebook Spaces social applications could be recovered from the device.

Preliminary findings on potential artefacts available from the Oculus Quest 2 virtual reality (VR) were published in a bulletin by DSTL (Defence Science and Technology Laboratory, 2022) to support the UK Government and Law Enforcement Agencies in conducting digital forensics. The report provided a summary of forensic extraction methods including JTAG and chip-off to recover artefacts from the UFS storage chipset. However, both methods showed no relevant forensic data could

be recovered due to the lack of support in existing tools and the inability to access the user data partition on the chip. Overall findings highlighted the best approach to recover data was a combination of several methods including adb, fastboot, sysdump and Media Transfer Protocol (MTP). The extracted data contained the headset's serial number, user account information, a list of installed applications, and some user activity data within each application. This research indicates potential user-related data is stored on the Meta Quest 2 VR headset and provides a starting point for acquisition and analysis in a forensically sound manner.

Moreover, it is imperative that we show a much more detailed forensic methodology and relevance of the artefacts we recovered. Hence, we make the most of the potential investigative impact of our work. To provide practical outcomes and value of our forensic analysis to forensic examiners, we formulate the following research questions (listed below) that our study attempts to answer in return at the end of this study.

3.1. Research questions

1. Can data artefacts be acquired from the Meta Quest 2, in a forensically sound manner?
2. What types of data artefacts can be recovered from the Meta Quest 2?
3. Is it possible to access application database files?
4. How are the recovered data artefacts relevant to a forensic investigation?

4. Methodology

According to (Anglano et al., 2016, 2017), the goal of any forensic analysis is to allow the analyst to obtain the digital evidence generated by the applications or devices under consideration. The methodology used to carry it out must be complete, generalised and can be repeatable to achieve the same results. The main aim of this study is to demonstrate the forensic acquisition of the Meta Quest 2 headset in a forensically sound manner using forensic tools. After the acquisition, the image is then analysed for relevant forensic artefacts related to the device information and user artefacts.

4.1. Testing environment

A Meta Quest 2 headset was used for this experiment. The device model number is *KW4*9CM and has a non-removable 128 GB of internal storage. To set up the headset, the device required pairing with the Meta Quest companion mobile app. We downloaded, installed, and ran the *Meta Quest iOS app v.192.0* (recent version at the time of writing) on an *Apple iPhone 11 running iOS v. 15.6.1*. The app was subsequently paired with the headset.

4.2. Experiment design

The experiment design includes various user activities and actions in VR to simulate real-world headset usage and generate forensic artefacts. This allows us to demonstrate typical user interaction using the VR headset and comprehensively collect relevant forensic traces. A test user account was created with the username *"Bengal_kitten"* with the screen name *"Neo Roberts"*. For each action performed by the test user account, notes were made to record the date and time and other relevant information during this design phase. In Table 1, we present descriptions of actions performed on the Meta Quest 2 VR headset.

4.3. Acquisition and analysis tools

To conduct the forensic acquisition of the Meta Quest 2 headset using forensic software, Android Debug Bridge (adb) must be enabled whilst the headset is connected to the forensic workstation using a USB-C cable (Fig. 1).

Table 1
Experiment concerning actions performed on Meta Quest 2 headset.

Actions	Description
Initial Setup	Factory reset headset to ensure no pre-existing artefacts are present during the forensic acquisition.
Connectivity	The device is connected to the internet via Wi-Fi.
Account Access	Log in with the developer Meta Account.
Application Installation	Installed the following VR applications: YouTube (version 1.43.32), Beat Saber (version 1.26.1), Keep Talking and Nobody Explodes (version 1.9.22), Job Simulator (version 1.4.0.4681).
Web Browsing	Browsed the internet using the proprietary Meta Quest Browser (version 24.4.0). 4 different websites were visited.
Media Viewing	Watched YouTube videos. 4 different YouTube videos were watched.
File Downloads	Downloaded several images (7 copyright-free images from pixabay.com), a document (PDF of the Keep Talking game manual), a video (4 copyright-free videos from videvo.net), and audio files (5 copyright-free audio files from videvo.net).
Game Play	Played Beat Saber (6 solo levels, 2 online levels, 3 screenshots, 2 videos created), Keep Talking (3 levels, 3 screenshots, 2 videos created), and Job Simulator (1 level, 3 screenshots, 2 videos created)
Messaging	Messaged another user. The test user sent 6 messages and received 4 messages.

Fig. 1. The Meta Quest 2 headset is connected via a USB-C cable.

By default, adb is not enabled on the headset and can only be achieved by enabling both Developer Mode and USB debugging (Defence Science and Technology Laboratory, 2022). This was accomplished by upgrading the primary Meta (user) account associated with the device to a 'developer' account via the Meta Quest developer's website (Meta Developer, 2022). We then proceeded to download and install the Meta Quest app on an iPhone from the Apple App Store. Once the app was installed, we logged in using the new developer account. Bluetooth was enabled on the smartphone, and we paired the Meta Quest 2 headset to the app. Once paired, we enabled Developer Mode through the app Menu->Devices -> The Meta Quest 2 headset -> Headset Settings -> Developer Mode -> Toggle Developer Settings on as shown in Fig. 2. With Developer Mode enabled on the headset, we could access data through the developer account.

Once these steps were completed, the headset prompted the forensic

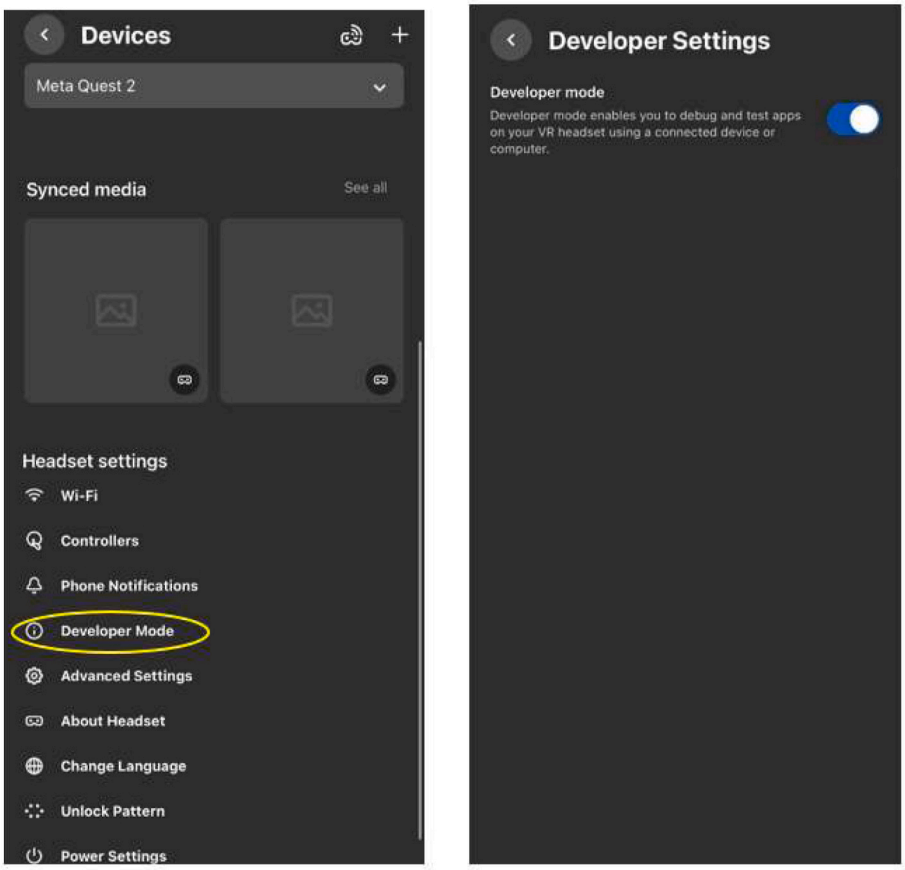

Fig. 2. Enabling Developer Mode on the Meta Quest app.

investigator to enable USB debugging via a toggle switch once connected to the forensic workstation.

We used the forensic software *AXIOM Process v. 6.5.0.32778* (Magnet Forensics, 2022) to acquire an adb backup of the headset and also collect live system data information using its built-in dumpsys utility. The backup obtained was then analysed using the forensic analysis software *Autopsy v. 4.19.3* (Carrier, 2022).

The proximity sensor on the Meta Quest 2 headset can detect when the headset is no longer being worn and turn off the display. This can interrupt the acquisition process and cause a failed attempt. Therefore, it is recommended that the headset be worn throughout the acquisition process to prevent it from going idle. However, this can be temporarily disabled during the forensic acquisition by covering the headset's proximity sensor with a piece of tape or other material so that the display remains active even when the headset is not being worn (Fig. 3).

4.4. Location of forensic artefacts

Once the acquisition is complete, *AXIOM Process* outputs the logical forensic image as a compressed zip file named 'Oculus Quest 2 Quick Image'. Within the forensic image, all data artefacts are stored in two individual compressed files named *'adb-data.tar'* and *'sdcard.tar.gz'*, and one folder named *'Live Data'* as shown in Fig. 4.

The sdcard.tar.gz file was converted to a TAR file using *7-zip,* an open-source file archiver. Both TAR files (sdcard.tar and adb-data.tar) and the Live Data folder (see Table 2), were examined using the software *Autopsy* to find data related to the user activity and device information that could be relevant for forensic examiners.

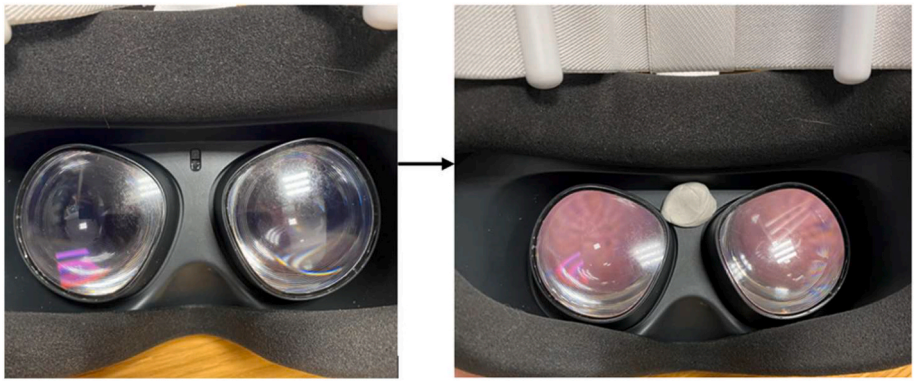

Fig. 3. Covering the proximity sensor which is located between the two eye lenses.

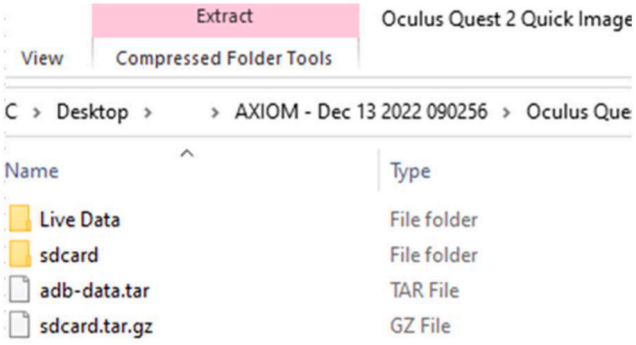

Fig. 4. Forensic artefacts within the 'Oculus Quest 2 Quick Image' zip folder.

Table 2
Summary of Meta Quest 2 artefacts.

File Name	File Type	File contents
adb-data.tar	TAR file	Data for applications stored on the Meta Quest 2.
sdcard.tar.gz	GZ file	Data stored on the internal storage of the Meta Quest 2.
Live Data	Folder	Live data files were obtained using *AXIOM Process* forensic software.

5. Forensic analysis and findings

Each forensic artefact was loaded into Autopsy as logical evidence source files and several ingest modules were selected for evidence processing and analysis. The ingest modules selected for our analysis include File Type Identification, Embedded File Extractor, Picture Analyzer, Email Parser, Encryption Detection, Interesting Files Identifier, PhotoRec Carver, Android Analyzer (aLEAPP), Android Analyzer and GPX Parser. Fortuitously, the relevant forensic artefacts within the evidence source files provide useful information about user data and activities including details of installed user applications. In the following sections, we present a comprehensive analysis of relevant forensic artefacts that can be recovered.

5.1. Live data artefacts

The internal operating system of the Meta Quest 2 VR headset is based on Android OS. The *AXIOM Process* forensic software uses the *Android Debug Bridge (ADB) dumpsys* command line tool to collect and output diagnostics and information about system services running on the VR headset as live data artefacts in individual text files. The live data output is typically verbose. However, from our analysis of the artefacts in the 'Live Data' folder, we found 10 output text files which contain relevant artefacts related to the test user accounts and activities. These files include *account.txt, appops.txt, backup.txt, bluetooth_manager.txt, device_properties.txt, package.txt, trust.txt, usagestats.txt, user.txt and wifi_Stats.txt.*

The *account.txt* (Fig. 5) *and trust.txt* (Fig. 6) files both contain information associated with a primary user account. The *user.txt* (Fig. 7) specifies the primary user account as an admin, or the account name used to initialise the VR headset.

```
User UserInfo{0:Neo Roberts:13}:
  Accounts: 4
    Account {name=Meta, type=com.meta}
    Account {name=Oculus, type=com.oculus}
    Account {name=Facebook, type=com.facebook}
    Account {name=Facebook SSO, type=com.facebook.sso}
```

Fig. 5. Data contained within the file account.txt.,

The file *'appops.txt'* contains a record of the last time an application took exclusive control of headset features (such as volume control and audio focus). Files *'backup.txt'* (Fig. 8), *'package.txt', 'usagestats.txt'* and *'usage_stats.txt'* all contain information related to the installed applications on the headset. The file *'bluetooth_manager.txt'* contains a record of the Bluetooth devices which have connected to the headset. The file *'device_properties.txt'* stores hardware and operating system information. Files *'wifi.txt'* and *'wifi_Stats.txt'* both contain information related to the networks which the headset is associated with.

For example, Fig. 9 shows that the application *Beat Saber*, *version 1.26.1* was first installed on December 5th, 2022, at 18:22, and that it was not updated after this time. It also shows the application was granted access to the network and therefore the Internet.

All these files can be useful in forensic investigations as they can allow investigators to easily identify which applications (and their versions) have been installed on the headset. The files also provide information which would be useful for creating an accurate timeline of user actions on the headset. Furthermore, the package name for each application is prefixed with the developer who created them, e.g., the application *Beat Saber*, package: *com.beatgames.beatsaber*, was developed by Beat Games. This allows investigators to easily identify if applications were developed by Meta (Oculus/Facebook) or third parties. This can direct investigators where to search for additional data artefacts, such as in cloud infrastructure hosted by a third party.

A summary of the relevant live data artefacts is presented in Table 3, with file name, file type, file location, and information associated with the artefact clearly outlined.

5.2. Backup data artefacts

Examining the data artefacts in the '*adb-data.tar*' file, we identified artefacts containing information about installed applications. Some of this information indicates the version of the applications installed, configuration files, file paths of relevant app databases, VR headset device information and user account information relevant to installed apps. Additionally, some of this information indicates how far the user has progressed in gaming applications. This information could be used to create a timeline of user activity as the amount of progress made can infer how long the user has spent playing the game – (the more progression in the game, the more time the user has likely spent playing it). Additionally, this information may be useful in verifying an alibi, if a suspect's alibi is that they were completing a level in one of these games, it is possible to easily disprove it should these files state that the level has not yet been completed. The useful data artefacts for each installed application have been summarised in Table 4.

5.3. Internal storage artefacts

By connecting the Meta Quest 2 headset to any PC (via a USB-C cable), it is possible to view and modify the contents of the internal storage. Since it is possible to easily view and alter the files stored internally, users may use this to store incriminating files. Thankfully, analysis software can identify the MD5 hash value for every file stored, which will allow investigators to look up known MD5 hash values to easily identify any incriminating evidence. Therefore, forensic investigators must identify the Meta Quest 2 VR headset as a possible evidence source during an investigation. However, investigators must also be aware that due to the user having access to the data, its data artefacts may have at some point been modified, which creates uncertainty about the integrity of any evidence found on the internal storage. Despite this, the internal storage may contain some useful data artefacts, about installed applications and user behaviour, which could aid an investigation. These data artefacts have been summarised in Table 5.

Instead of connecting the headset to a PC, users can download files

```
Trust manager state:
 User "Neo Roberts" (id=0, flags=0x13) (current): trusted=0, trustManaged=0, deviceLocked=0, strongAuthRequired=0x0
   Enabled agents:
   Events:
```

Fig. 6. Data contained within the file trust.txt.

```
Users:
  UserInfo{0:Neo Roberts:13} serialNo=0 isPrimary=true
    Flags: 19 (ADMIN|INITIALIZED|PRIMARY)
```

Fig. 7. Data contained within the file user.txt.

from an online source to store them on the internal storage of the headset. These downloaded files are stored in the 'Download' directory. Using analysis software, it was possible to identify when these files were downloaded (modified time in Fig. 10), as well as their file size (in bytes) and MD5 hash values. This aids investigations by ensuring the integrity and completeness of evidence.

5.4. Cloud data artefacts

It was possible to view and download the user data from the registered user account associated with the headset from the Oculus cloud account once logged in. Under the Privacy Centre tab in the Settings section, we downloaded the zip file *"my-data"* for the Neo Roberts user account to the forensic workstation. Fig. 11 details the contents of the downloaded file.

From the analysis, relevant forensic artefacts associated with the Meta user account and headset were found in a ***data.json*** file, ***data*** and ***files*** folders. The ***data*** folder contains an '*index.html*' file that includes information associated with the user's personal account information (full name, email address and date of birth), account settings and profile settings information and device information (device type, serial number, account location and login history). The file also contains a record of apps installed on the headset, recently viewed apps and achievements across gaming apps we installed. Several html files were also stored in this folder with each file containing information (app name, app installation time, app status and last used time) for each app installed on the headset. The ***data.json*** file contains the same information as the *index.html*, but the data is stored in JSON format. The ***files*** folder contains an image associated with the Meta user account's avatar.

6. Evaluation of research questions and discussion

In this section, we will discuss the implications of our findings for relevant forensics questions.

Research Question 1: Can data artefacts be acquired from the Meta Quest 2, in a forensically sound manner?

A "forensically sound" data acquisition protects the integrity of obtained data artefacts and their metadata by ensuring they have not been altered or destroyed within the acquisition process.

At the very start of the acquisition process, the headset was powered on and used to disable wireless connections. No other applications were launched. Once the headset had been physically connected to the PC, the only user input was to enable USB debugging and respond to any prompts generated by the acquisition software.

The acquisition software used was a certified digital forensics software, *AXIOM Process*, which created a 'Quick Image' of the Meta Quest 2 headset. This extracted the data artefacts stored across the headset, including live data, and persistent data stored on the embedded internal SD card. It also triggered the device to begin a backup so that the data artefacts contained within the backup file could also be extracted. All extracted data artefacts were then stored in appropriately named files, which were compressed into one zip file.

This zip file included 3 files which contain the acquired data artefacts from the different storage mediums of the headset:

- 'sdcard.tar.gz' – compressed file which stored data artefacts from the SD card.

```
Full backup queue:10
    0 : com.android.webview
    1670260719208 : com.oculus.environment.prod.adobe
    1670260742865 : com.oculus.tv
    1670260748756 : com.facebook.arvr.quillplayer
    1670260767782 : com.oculus.mobile_mrc_setup
    1670260773199 : com.oculus.helpcenter
    1670263308496 : com.google.android.apps.youtube.vr.oculus
    1670263367482 : com.steelcrategames.keeptalkingandnobodyexplodes
    1670263734713 : com.owlchemylabs.jobsimulator
    1670264659799 : com.beatgames.beatsaber
```

Fig. 8. Data contained within the file backup.txt.

```
Package [com.beatgames.beatsaber] (ca68729):
  userId=10086
  pkg=Package{2cc3aae com.beatgames.beatsaber}
  versionName=1.26.1
  firstInstallTime=2022-12-05 18:22:13
  lastUpdateTime=2022-12-05 18:22:13
  install permissions:
    android.permission.INTERNET: granted=true
    android.permission.ACCESS_NETWORK_STATE: granted=true
```

Fig. 9. Data contained within the files Package.txt, Usagestats.txt and 'Usage_Stats.txt.

Table 3
Summary of live data artefacts.

File Name	File Type	File Location	Information within the artefact
account.txt	TXT	/Live Data/Dumpsys Data/account.txt	Shows user accounts on the headset as well as the user's name.
appops.txt	TXT	/Live Data/Dumpsys Data/appops.txt	Shows the last date and time an application took control of audio focus, volume control and wake lock.
backup.txt	TXT	/Live Data/Dumpsys Data/backup.txt	List of all applications installed on the headset.
bluetooth_manager.txt	TXT	/Live Data/Dumpsys Data/bluetooth_manager.txt	Shows the ID of connected Bluetooth devices.
device_properties.txt	TXT	/Live Data/device_properties.txt	Device model, OS version, local region, and time zone.
package.txt	TXT	/Live Data/Dumpsys Data/package.txt	The version of installed applications, their permissions, and the installation and latest update timestamps.
trust.txt	TXT	/Live Data/Dumpsys Data/trust.txt	Name associated with the user account.
uage_Stats.txt & usagestats.txt	TXT	/Live Data/usage_stats.txt & Live Data/Dumpsys Data/usagestats.txt	Application usage history, including the number of times it is launched, the total time it is used, and when it was last used.
user.txt	TXT	/Live Data/Dumpsys Data/user.txt	User accounts on the headset. Specifies if an account is an admin or primary user.
wifi.txt & wifi_Stats.txt	TXT	/Live Data/Dumpsys Data/wifi.txt & /Live Data/wifi_stats.txt	SSIDs the headset has associated with, alongside the number of associations.

- 'adb-data.tar' – compressed file, which stored data artefacts related to installed applications, obtained by the device back-up.
- 'Live Data' – the folder which stores live data artefacts on the device.

All compression methods (*.zip, .tar, .gz*) use lossless compression and thereby do not alter or delete any of the collected data artefacts. Furthermore, *AXIOM Process* did not alter the data artefacts at any point. The entire acquisition process has been thoroughly documented in *Section 3.3* so that it is both reliable and repeatable. During the forensic acquisition, we observed no changes to the user data when developer mode was enabled. When conducting forensic acquisition on Meta Quest 2 headsets, investigators will need to create a secondary developer account and pair it with the headset to enable Developer Mode and USB debugging. As we were limited to using the primary user account to enable developer mode in this study, we were unable to confirm if there would be any changes to the original user's data by connecting a secondary developer account via the method outlined in Section 3.3.

Research Question 2: What types of data artefacts can be recovered from the Meta Quest 2?

Numerous data artefacts were acquired from the Meta Quest 2 headset. These artefacts originated from the live data, backup file and internal SD card.

The useful data artefacts from the **Live Data** medium consisted of numerous text (.TXT) files.

- Files *'account.txt'*, *'trust.txt'* and *'user.txt'* contain the name of the user account on the headset.
- The file *'appops.txt'* contains a record of the last time an application took exclusive control of headset features (such as volume control and audio focus).
- Files *'backup.txt', 'package.txt', 'usagestats.txt' and 'usage_stats.txt'* all contain information related to the installed applications on the headset.
- The file *'bluetooth_manager.txt'* contains a record of the Bluetooth devices which have connected to the headset.
- The file *'device_properties.txt'* stores hardware and operating system information.

Table 5
Summary of internal storage artefacts.

File Name	File Type	File Location	Information Within the Artefact
obb	DIRECTORY	/sdcard.tar/sdcard/Android/obb	Folders containing data artefacts for installed applications.
Download	DIRECTORY	/sdcard.tar/sdcard/Download	Files downloaded by the user. All file types including.PDF, .JPG, .MP3, .MP4, .MOV
Movies	DIRECTORY	/sdcard.tar/sdcard/Movies	Thumbnails of screen recordings.
Pictures	DIRECTORY	/sdcard.tar/sdcard/Pictures	Thumbnails of screenshots.
Screenshots	DIRECTORY	/sdcard.tar/sdcard/Oculus/Screenshots	Screenshots stored as. JPG files.
Videoshots	DIRECTORY	/sdcard.tar/sdcard/Oculus/VideoShots	Screen recordings are stored as.MP4 files.

Table 4
Summary of artefacts from installed user apps.

File Name	App	File Type	File Location	Information Within the Artefact
PlayerData.dat	Beat Saber	DAT	/adb-data.tar/apps/com.beatgames.beatsaber/ef/PlayerData.dat	Game Settings, Game progress and if the user has agreed to the multiplayer disclaimer.
com.owlchemylabs.jobsimulator.v2.playerprefs.xml	Job Simulator	XML	/adb-data.tar/apps/com.owlchemylabs.jobsimulator/sp/com.owlchemylabs.jobsimulator.v2.playerprefs.xml	Game Level Progression.
best_times.xml	Keep Talking and Nobody Explodes	XML	/adb-data.tar/apps/com.steelcrategames.keeptalkingandnobodyexplodes/ef/best_times.xml	Best Time's for a user progressing on each Level.
youtube.xml	YouTube	XML	/adb-data.tar/apps/com.google.android.apps.youtube.vr.oculus/sp/youtube.xml	Device model and visitor ID it has been assigned by YouTube.
app	YouTube	–	adb-data.tar/apps/com.google.android.apps.youtube.vr.oculus/f/.com.google.firebase.crashlytics.files.v1/open-sessions/639871E402E600010C2D9D02BF22DCEC/native/app.	Installed Application Version.

Name	Modified Time	MIME Type	Extension	Size	MD5 Hash
210329_01B_Bali_1080p_027.mp4	2022-12-09 19:15:39 GMT	video/mp4	mp4	221063928	47d729aea3c940c1c0ee4ff2bcb3bb9b
210329_01B_Bali_1080p_028.mp4	2022-12-09 19:14:20 GMT	video/mp4	mp4	215106949	882d3c4477e0dbdf4d55e235b0cb4335
210329_06B_Bali_1080p_007.mp4	2022-12-09 19:14:17 GMT	video/mp4	mp4	224694247	ecdb08d56143b9eaebc0495b45b0ab0e
210329_06B_Bali_1080p_013.mp4	2022-12-09 19:13:50 GMT	video/mp4	mp4	224749240	13e99c92c0d415d742fe57e9c740fa64
_import_61516692993d77.04238324.mov	2022-12-09 19:14:13 GMT	video/quicktime	mov	1174479343	45d3a56daed678b795ce2c94fa9c9756
christmas-tree-g38fa967be_1920.jpg	2022-12-09 19:10:53 GMT	image/jpeg	jpg	199659	63442877b9662acb6026a361f26eec58
Death Grips - Beware.mp3	2022-12-09 19:17:16 GMT	audio/mpeg	mp3	5642924	82ae3ea55dc5d36190eab00aaca6a21f
Death Grips - Blackjack.mp3	2022-12-09 19:17:17 GMT	audio/mpeg	mp3	2274189	2aaebfb587fbedd0a4a1a9f1f6b99621
Death Grips - I've Seen Footage.mp3	2022-12-09 19:17:31 GMT	audio/mpeg	mp3	3247632	c08178a587682ac10228dfc7c59cb3e6
Death Grips - No Love.mp3	2022-12-09 19:17:13 GMT	audio/mpeg	mp3	4864281	285f97661047a5e4c6b930674b4f34c5
KeepTalkingAndNobodyExplodes-BombDefusalManual-v1	2022-12-09 19:06:46 GMT	application/pdf	pdf	813425	1f68406d0d6d2241b5c47b9e4db27337
ladybug-ga25a9cb84_1280.jpg	2022-12-09 19:09:57 GMT	image/jpeg	jpg	157433	27bf18ab630708bd5652375467991f83
ladybug-gce0a9d4df_1920.jpg	2022-12-09 19:10:16 GMT	image/jpeg	jpg	679779	47618c99acc8ac4cd9d1b522a5739b05
middle-spotted-woodpecker-g374dbb14d_1920.jpg	2022-12-09 19:08:06 GMT	image/jpeg	jpg	834240	60a18431e7e958794e4a6856a3dcb3f4
Nils Frahm - You.mp3	2022-12-09 19:17:22 GMT	audio/mpeg	mp3	3021051	392524562e613ec14545532285f4fb5b
sea-ga9174cb75_1280.jpg	2022-12-09 19:11:38 GMT	image/jpeg	jpg	371807	8a9e697c489ae34a6080cc76c8ab6852
sunrise-g1e272d678_1920.jpg	2022-12-09 19:11:28 GMT	image/jpeg	jpg	266079	73159e5cb32c3b9367eb87a06817b7af
tree-ga1fca903f_1280.jpg	2022-12-09 19:11:13 GMT	image/jpeg	jpg	185491	d1933b7b567fce679b70120bba7bdb1d

Fig. 10. Files stored in the 'Download' directory in the internal storage.

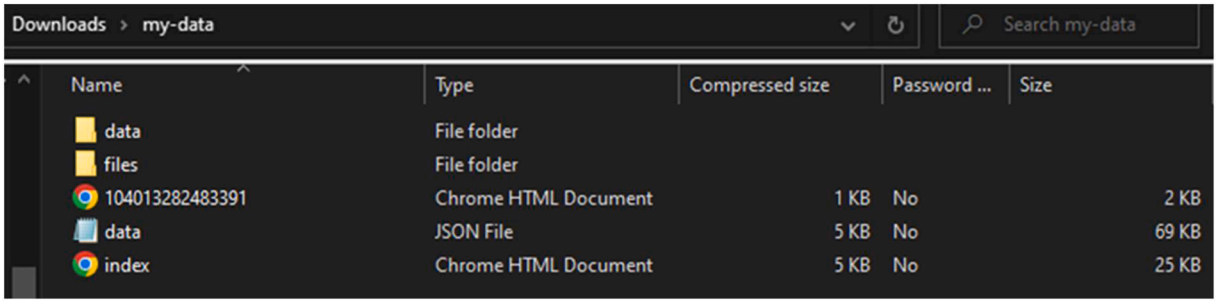

Fig. 11. Contents of the downloaded zip file.

- Files *'wifi.txt'* and *'wifi_stats.txt'* both contain information related to the networks which the headset is associated with.

The **Backup Data** contained useful data artefacts associated with the installed applications on the headset.

For gaming applications, these artefacts contained game files which stored the user's progress throughout the game. Some files even stored the installed version of the game as well as statistics for the user activity within the game itself.

Some files referred to database files which were unobtainable by the logical acquisition process, due to the operating system of the headset having been unrooted.

Due to the extensive storage capability of the **internal storage**, this medium contained the largest variety of data artefacts. Directories 'Movies', 'Pictures', 'Videoshots' and 'Screenshots' all contained image (.jpg) or video (.mp4) files. The contents of these files are all related to videoshots of screenshots of user activity, captured by the user, on the headset itself. The Directory 'obb' contains the same data artefacts which are present in the **Backup** files. Therefore, all these files relate to the installed applications and the user's activity within the application.

The Directory 'Download' contained the most unique and interesting data artefacts, as this directory contains all user files that have been downloaded onto the headset. The directory was even able to store files of types that are unsupported by the headset, such as.pdf or.mov files.

Research Question 3: Is it possible to access user application data?

No. To access and extract user application data, a physical acquisition of the device would be required via rooting. Future work should focus on finding a successful method to root the Meta Quest 2 to gain access to user application data which will include application databases that could contain relevant forensic artefacts.

Research Question 4: How are the recovered data artefacts relevant to a forensic investigation?

The data artefacts in the **Live Data** are relevant to forensic investigations as they provide evidence that can link the headset to its owner, identify where the headset has been, and what it has been used for. Recovered system information also highlights the version of applications installed, SSIDs of established internet connections, as well as the configured time zone and region of the headset. The data artefacts in the **Backup Data** provide information related to installed applications. Gaming applications contain files that indicate the user's progress, which may facilitate the creation of a timeline of user activity. Furthermore, the information contained within these files may provide evidence for proving or disproving a user's alibi. As the **device's internal storage** within the headset functions as a regular SD card, the data artefacts it contains are highly relevant to forensic investigations. This is because users can store their files on the storage medium. There is no limitation to which file types can be stored on the SD card, as it stores file types which are not supported by the headset itself. The SD card can be populated by downloading files directly using the headset, or by connecting the headset to a PC and using file management software, such as Windows File Explorer, to view and alter the stored files. This functionality makes it possible for users to store malicious or

incriminating files on the Meta Quest 2. However, forensic investigators must be aware that this functionality generates uncertainty about the integrity of any evidence it contains, as users can manually modify files.

Cloud data including the data.json file, data folder and files folder contained on the Meta headset provide valuable information for forensic investigators about the device user and their activity. Specifically, the data folder contains detailed records of apps installed on the device including name, install time, status and last usage. The data.json and index.html files in the data folder contain personal account details of the user like name, email, date of birth as well as device information like serial number and login history. The files folder contains images linked to the user's avatar. Taken together, these artefacts allow investigators to identify the device owner, understand their app usage and activity, and potentially tie the device to specific actions or events under investigation. The files provide insight into user behaviour and actions on the device.

7. Limitations

The Meta Quest 2 runs an operating system based on Android version 10, which isolates and protects sensitive application files, such as databases, by limiting the privileges the user has on the device (they have no root access). However, this means that forensic acquisition tools including *AXIOM Process* are also unable to gain root access to acquire a physical image limiting user and application data that could contain user-related data stored in databases. To acquire such files, the Meta Quest 2 headset will need to be rooted before the acquisition takes place. At the time of writing, there are no established methods to successfully root the Meta Quest 2 headset and our findings confirm conclusions in related works (Defence Science and Technology Laboratory, 2022), that most of the useful application files and locations require root privileges for a complete forensic acquisition. Moreover, our study did not consider JTAG and chip-off forensic acquisition methods. This is because Android 10 enables file-based encryption and the lack of support on existing JTAG tools prevents accessing the internal memory for the Qualcomm XR2 chipset used in Meta Quest 2 headsets as described in previous works. We were also unable to recover associated user contacts including chat logs and messages sent and received directly from the headset. Previous studies show that user communication data are stored within the databases on Facebook messenger app installed on companion iOS or Android devices paired with the user's headset (Defence Science and Technology Laboratory, 2022).

8. Conclusion and future work

The acquisition and analysis of forensic data from VR headsets is relatively novel. This research has defined a new successful methodology for acquiring data artefacts from the Meta Quest 2 in a forensically sound manner, as well as identifying its forensic capabilities. This methodology may apply to other VR headsets which have been manufactured by different companies, and so may be followed by law enforcement to acquire digital evidence from VR headsets, for use in criminal investigations. This is extremely beneficial as there has been a significant rise in criminal behaviour amongst VR users, which has been facilitated by the rise in unsafe VR environments.

The digital evidence acquired from the logical acquisition can link the headset to its owner, identify where the headset has been, what applications are installed, and how the user has interacted with these applications. The most interesting data artefacts were stored on the internal storage, which allows users to store their files. There is no limitation to what file types can be stored, which means the internal storage can contain a large variety of digital evidence. Therefore, it is imperative that Meta Quest 2 is not overlooked as a data source during a criminal investigation. Further research should be conducted to identify further data artefacts from the Meta Quest 2, and other headsets, which may provide evidence in criminal investigations. To obtain such evidence, it may be necessary to devise a successful methodology to root VR devices.

Declaration of competing interest

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

Data availability

Data will be made available on request.

Acknowledgements

This work was supported by the School of Computer Science and Mathematics, Liverpool John Moores University, U.K.

References

Akinbi, A., Ojie, E., 2021. Forensic analysis of open-source XMPP multi-client social networking apps on iOS devices. Forensic Sci. Int.: Digit. Invest. 36, 301122 https://doi.org/10.1016/j.fsidi.2021.301122.

Anglano, C., Canonico, M., Guazzone, M., 2016. Forensic analysis of the ChatSecure instant messaging application on android smartphones. Digit. Invest. 19, 44–59. https://doi.org/10.1016/j.diin.2016.10.001.

Anglano, C., Canonico, M., Guazzone, M., 2017. Forensic analysis of telegram messenger on android smartphones. Digit. Invest. 23, 31–49. https://doi.org/10.1016/j.diin.2017.09.002.

Barr-Smith, F., Farrant, T., Leonard-Lagarde, B., Rigby, D., Rigby, S., Sibley-Calder, F., 2021. Dead man's switch: forensic autopsy of the nintendo switch. Forensic Sci. Int.: Digit. Invest. 36, 301110 https://doi.org/10.1016/j.fsidi.2021.301110.

Bezmalinovic, T., 2022. This Is How Much Meta Is Investing in VR, AR and Horizon. https://mixed-news.com/en/this-is-how-much-meta-is-investing-in-vr-ar-and-horizon/.

Carrier, B., 2022. Autopsy (4.19.3. https://www.autopsy.com/.

Casey, P., Lindsay-Decusati, R., Baggili, I., Breitinger, F., 2019. Inception: virtual space in memory space in real space – memory forensics of immersive virtual reality with the HTC vive. Digit. Invest. 29, S13–S21. https://doi.org/10.1016/j.diin.2019.04.007.

Crawford, A., Smith, T., 2022. Metaverse App Allows Kids into Virtual Strip Clubs. BBC News. https://www.bbc.co.uk/news/technology-60415317.

Davies, M., Read, H., Xynos, K., Sutherland, I., 2015. Forensic analysis of a Sony PlayStation 4: a first look. Digit. Invest. 12, S81–S89. https://doi.org/10.1016/j.diin.2015.01.013.

Defence Science and Technology Laboratory, 2022. *Oculus Quest 2*. Digital Forensics Bulletin. https://us5.campaign-archive.com/?u=a5a2a1131e612711f02b96e2c&id=68da1dc52c.

Developer, Meta, 2022. Oculus Developer Center. https://developer.oculus.com/.

Dugga, M., 2014. *Online Harassment*. Pew Research Center. https://www.pewresearch.org/internet/2014/10/22/online-harassment/.

Hadgkiss, M., Morris, S., Paget, S., 2019. Sifting through the ashes: amazon Fire TV stick acquisition and analysis. Digit. Invest. 28, 112–118. https://doi.org/10.1016/j.diin.2019.01.003.

Happa, J., Steed, A., Glencross, M., 2021. Privacy-certification standards for extended-reality devices and services. In: 2021 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops. VRW). https://doi.org/10.1109/VRW52623.2021.00085, 397–398.

Heath, A., 2021. Facebook is planning to rebrand the company with a new name. Verge. https://www.theverge.com/2021/10/19/22735612/facebook-change-company-name-metaverse.

Kretzschmar, M.E., Rozhnova, G., Bootsma, M., Boven, M. E. van, Wijgert, J. van de, Bonten, M., 2020. Time is of the essence: impact of delays on effectiveness of contact tracing for COVID-19. medRxiv. https://doi.org/10.1101/2020.05.09.20096289.

Magnet Forensics, 2022. *Magnet Process* (6.5.0.32778. https://www.magnetforensics.com/.

Meta, 2022. Meta – VR Headsets, Smart Displays and AR Glasses. https://www.meta.com/gb/?utm_content=31202.

Moore, J., Baggili, I., Marrington, A., Rodrigues, A., 2014. Preliminary forensic analysis of the xbox one. Digit. Invest. 11, S57–S65. https://doi.org/10.1016/j.diin.2014.05.014.

Murias, J.G., Levick, D., McKeown, S., 2023. A forensic analysis of streaming platforms on Android OS. Forensic Sci. Int.: Digit. Invest. 44, 301485 https://doi.org/10.1016/j.fsidi.2022.301485.

Ngejane, C.H., Eloff, J.H.P., Sefara, T.J., Marivate, V.N., 2021. Digital forensics supported by machine learning for the detection of online sexual predatory chats. Forensic Sci. Int.: Digit. Invest. 36 https://doi.org/10.1016/j.fsidi.2021.301109.

Online Safety Bill, 2023 (testimony of UK Parliament). https://bills.parliament.uk/publications/49376/documents/2822.

Park, S.-M., Kim, Y.-G., 2022. A metaverse: taxonomy, components, applications, and open challenges. IEEE Access 10, 4209–4251. https://doi.org/10.1109/ACCESS.2021.3140175.

Qamar, S., Anwar, Z., Afzal, M., 2023. A systematic threat analysis and defense strategies for the metaverse and extended reality systems. Comput. Secur. 128, 103127 https://doi.org/10.1016/j.cose.2023.103127.

Sheera, F., Kellen, B., 2021. The Metaverse's Dark Side: Here Come Harassment and Assaults. The New York Times. https://www.nytimes.com/2021/12/30/technology/metaverse-harassment-assaults.html.

Steam, 2022. Steam Hardware & Software Survey. https://store.steampowered.com/hwsurvey/Steam-Hardware-Software-Survey-Welcome-to-Steam.

Taylor, D., Mwiki, H., Dehghantanha, A., Akibini, A., Choo, K.K.R., Hammoudeh, M., Parizi, R., 2019. Forensic investigation of cross platform massively multiplayer online games: minecraft as a case study. Sci. Justice 59 (3), 337–348. https://doi.org/10.1016/j.scijus.2019.01.005.

Yarramreddy, A., Gromkowski, P., Baggili, I., 2018. Forensic analysis of immersive virtual reality social applications: a primary account. In: 2018 IEEE Security and Privacy Workshops (SPW), pp. 186–196. https://doi.org/10.1109/SPW.2018.00034.