The Development of an IoT-Focused Investigative Methodology:

The Case of a Pico 4 Headset

Luke Yates
Dept. of Computing
Buckinghamshire New University
High Wycombe, Buckinghamshire
email: luke.yates@bucks.ac.uk

Professor Ian Fergusson
Dept. of Cybersecurity and Computing
Abertay University
Dundee, Scotland
email: i.ferguson@abertay.ac.uk

Dr Karl van der Schyff
Dept. of Cybersecurity and Computing
Abertay University
Dundee, Scotland
email: k.vanderschyff@abertay.ac.uk

***Abstract*—The paper is submitted to the conference as it is relevant to Internet of Things and Forensics in Constrained Environments. The rapid proliferation of Internet-of-Things (IoT) devices, including Virtual Reality (VR) headsets, has introduced new opportunities and challenges for digital forensics. This study focuses on the Pico 4 VR headset, a next-generation Android-based device, to explore forensic methodologies for extracting and analyzing digital artifacts. Crimes involving VR, such as harassment, fraud, and illegal content distribution, highlight the urgency for specialized investigative approaches. Using the Android Debug Bridge (ADB) suite to capture device data, we developed a forensic methodology that ensures data integrity while navigating the limitations of non-rooted devices. Our investigation reaffirms the potential of ADB commands, including backup and dumpsys, to collect system information, application data, and user-generated content from the Pico 4 in a forensically sound manner. This paper focuses on the most significant aspect of this research, where a custom module for Autopsy facilitated efficient web browser data processing. However, the challenges posed by device security, inaccessible storage areas, and encrypted communications underscore the need for adaptable and innovative forensic techniques. The research describe here contributes to the field by presenting the first digital forensic approach tailored to the Pico 4. The findings emphasize the importance of combining traditional forensic tools with bespoke methodologies to address emerging IoT devices. Our work provides a foundation for future studies on VR-related crime investigations, offering practical insights for digital forensic practitioners navigating the evolving landscape of IoT technologies.**

Keywords–IoT; forensics; Pico 4; Digital forensics; Android devices; VR forensics; Digital forensic methodology.

I. INTRODUCTION

An exponential growth of the Internet of Things (IoT) [1] means that more people are using non-traditional computing devices to access the internet, for legal and non-legal purposes. This includes the use of Virtual Reality (VR) headsets to commit fraud, harassment, identity theft and most seriously, access and distribution of illegal images of children [2]. Utilising modern VR devices to carry out these and potential new types of crime creates the potential to hide evidence from outdated digital forensics methodologies. It is therefore imperative that the science of Digital Forensics is mindful of the challenges VR technology presents, when conducting investigations. Digital forensics experts are required to carry out their investigations in a "forensically sound" manner that seeks to protect the integrity of data obtained from devices, as well as ensuring that no harm comes to devices procured in an investigation. They must also adopt techniques that consider the security restrictions on Android systems such as those on VR headsets and be mindful that there are often restrictions on what can be obtained.

The Pico 4 released in October 2022 [3] by ByteDance headset is an example of a newer Android-based VR device. A range of apps and games are available, both standalone on the device and via connection to a computer or phone. Whilst a considerable amount of research has been carried out on IoT and VR devices, the Pico 4 is relatively new technology and hence it is not known what useful digital forensic data may be stored on it. If investigators are unclear with regards to the digital forensic techniques to use on such a device, inadequate amounts of evidence will likely be collected, negatively impacting the effectiveness of an investigation or even resulting in evidence being excluded from court, which could have disastrous consequences for the case to be made.

This leads to the formulation of two research questions:

RQ1. What type of digital artefacts are typically acquired in a VR-focused digital forensic investigation, and how could these be extracted in a forensically sound manner? To develop a sound investigative methodology, it is important to know which type of artefacts are likely to be encountered and where to locate them. Handling such artefacts in an appropriate manner may require additional understanding – all of which could aid investigators faced with VR-focused investigations.

RQ2. Which techniques are suitable to aid investigators in identifying and reporting relevant digital forensic artefacts as evidence (in a forensically sound manner) when considering Android-based IoT devices like the Pico 4 VR headset? In addition to the type and location of the artefacts, it is also crucial to understand the techniques required to

generate useful information in reporting these findings and their relationship to the case being investigated. Some existing techniques may prove useful – yet others may have to be adapted (erg., Autopsy modules).

Our study is structured as follows: We first present readers with a review of related literature in Section II before providing a complete outline of our methodological approach in Section III. This is followed by the results of our evaluation in Section IV and an associated discussion, including the theoretical and practical implications in Sections V and VI. The study concludes with a brief discussion of the limitations and areas of future research in Section VII and a final conclusion in Section VIII.

II. LITERATURE

Guided by our first research question, the review will first provide readers with an outline of how digital forensic data should be acquired, followed by specifics as to how this relates to Android-based (thus Pico 4 related) devices

A. Acquiring digital forensic data from IoT devices

Regarding digital forensics, Alazab et.al. [4] states that IoT forensics requires a more specialised approach but has the potential to yield highly useful information that traditional computing lacks, such as motion sensor, GPS, camera, and microphone data. However, issues with IoT forensics are also considered, such as "inappropriate handling of data, securing the chain of custody and lack of standardisation". In addition, the concept of "cloud jurisdiction" is discussed. This is where data on the cloud from an IoT device may be stored in other countries, and hence subject to different rules and regulations regarding privacy and data protection, creating new obstacles for digital forensic investigations.

Research carried out on a SteamDeck handheld console systematically identified forensically relevant artefacts [5]. This device is not a typical IoT device and runs a Linux-based "SteamOS" operating system, however the differential forensic analysis approach used in the research holds value for IoT digital forensics. This is where "before and after" snapshots of the device data are taken, to see what has changed. This narrows the search down and expedite the locating of relevant forensic data. The data identified by this research as relevant, included device information, Wi-Fi connections, user accounts, games and apps, screenshots and images taken or downloaded to the device, friends (connections to other users) and financial transactions.

Raymer et.al. identify the importance of forensic techniques on VR devices in regard to the potential for crime, such as online harassment, grooming and cyberbullying [6]. A forensic analysis on a Meta Quest 2 device was performed, providing helpful and relevant information for when tackling VR headsets – specifically Android-based devices. Their research [6] confirmed that data can be retrieved from such a device using forensically sound practice, as well as describing locations and types of useful forensics data (live user activity, user files and live device data). Raymer et.al. [6] described their solution for a formal acquisition process, in which they identified storage types and locations on the device, then recover and analyse digital artifacts pertaining to a digital forensic investigation.

The three main areas investigated were user data, application data and live system data. Raymer et.al. [6] note that a limitation when working with the Quest 2 VR device as with all Android-based devices, is the restriction imposed on access to certain parts of storage, such as system files, and the only way to overcome this being to root the device being examined.

B. Investigating Android-based IoT devices

Taylor et. al. [7] examined the process of investigating mobile apps, as well as issues relating to obtaining digital evidence from such devices. Of particular interest is their research on Android apps and security. The research identified that each Android application runs as a unique user identity, which enhances security, and, consequently, makes acquiring data for digital forensics from such devices, more challenging. Additionally, this research identified the range of crimes that may be carried out by utilising digital devices, such as fraud, theft, money laundering, copyright infringement, and the possession and/or distribution of indecent images.

When considering digital forensics, the advantage of acquiring a rooted device is that it is possible to make physical images of the storage and data on that device, rather than just logical (files and folders) level copies. This allows retrieval of files and folders which have been deleted, as well as all applications and data. However, Android devices are not released in a rooted state [8], and obtaining an IoT Android device that is rooted is not always possible. This is because rooting such a device is extremely difficult to carry out on a new device, and introduces the risk of the evidence being no longer forensically sound. For the owner of the device, there is a risk of compromised security, voided warranty, unavailable services (such as online purchasing and banking), device instability, and in the worst case, the damage or destruction of an expensive piece of hardware. With new devices, such as the Pico 4, manufacturers will lock the boot-loader to discourage rooting attempts, and as rooting usually requires the exploitation of a vulnerability, a methodology may not exist at all to unlock the hardware in this way.

Kara [9] performed specific research on extracting Discord data from an Android device, and whilst successful in retrieving artifacts, such as contacts, messages, and deleted items, as well as understanding the data structure of Discord, this methodology relies on rooting or jail-breaking [10] the Android device, something that is either impossible or at least highly risky when dealing with newly released Android devices. Additionally, this approach copies files to the laboratory computer; files copied to another device will have their dates/times altered, harming their integrity as evidence. Kara [9] also observes that any security measures put into place on the suspect Android device, such as

biometrics or PINs, could make retrieving data a far more complex process.

It is worth observing that whilst Android employs strong mechanisms in its design which can protect privacy, but interfere with digital forensics investigations, user naivety over security and privacy settings can sometimes compromise this and could work in the favour of a digital forensics investigation. The research by Neisse et.al. [11] considers this and notes that the complexity of the permission-granting mechanism in Android devices means that users often fail to understand the privacy implications of granting apps permission to sensitive resources.

C. *The role of the Android Debug Bridge*

Easttom & Chuck [12] describe a methodology for SMART TV forensics in which they justify and then use the Android Debug Bridge (or ADB). Importantly, and as evidenced in their work, this tool is recognised as a means to extract artefacts in a forensically sound manner and therefore features in our methodology.

III. METHODOLOGICAL APPROACH

This section provides an outline of our methodological approach and investigative methodology in particular regard to the artifact developed for Autopsy. We start by first describing the methods used to prepare the hardware and software used. This is followed by details of how the initial data was captured from the Pico 4 headset, after which an explanation is provided of the test apps (and data) used. This section concludes with a detailed outline of the data acquisition process as well as the methods used for searching and data analysis. Note that this study received full ethical clearance from the primary author's university (ref: EMS8927).

Using the techniques identified in the literature study, images of the data were captured from the Pico 4 using ADB's "Android Backup", thus maximising integrity of data and forensic soundness. The first image was taken immediately after a factory reset of the Pico device and resulted in 49.38MB of data stored in the device's "apps" and "shared" folders (also known as the /sdcard folder on Android devices). The device was then used in a variety of common ways as it might be used by a typical user, including installing and using the Wolvic browser to visit websites and download 10 image files (done using the browser's "Save Image As" feature). A second image of the "apps" and "shared" folder data was then captured, this resulted in a file size of 13.38GB. Differential analysis was used to identify new or changed files in this second backup, leading to the identification of the database files relating to web browsing history. The analysis was done using a comparison of MD5 file hashes, to ensure identical files from both images could be safely ignored.

Investigating the browser history has not only become commonplace, but also crucial when trying to establish intent and was hence the main focus of this research. Given our use of the Wolvic browser, we were able to identify an SQLite database file (places.sqlite). The analysis of this database was automated by writing a module for Autopsy, a well-known open-source tool used for digital forensics. Autopsy uses a Jython parser, allowing Python code to interface with the Java-based Autopsy. A code template (for developing Autopsy modules) was acquired from GitHub [13] and rewritten to work with the data extracted from the Wolvic browser. The bespoke code connects to the web browser database file, and reads off rows in the web history table. It then creates an event for each visit to a website URL. It then creates an Autopsy "blackboard" artifact containing retrieved information about the website URL, web page title and date/time visited, and places this new artifact in Autopsy's "Web History" container. The flowchart for this algorithm is presented here:

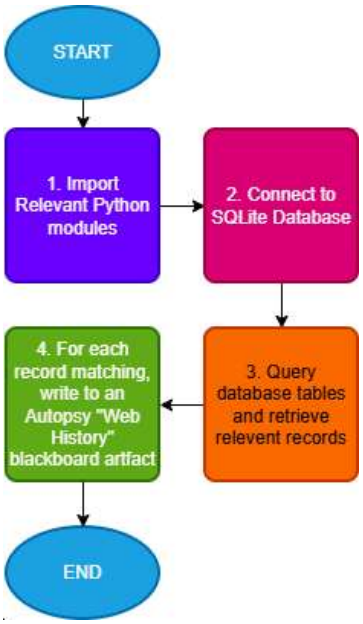

Figure 1. Flowchart for Web Browser DataRetrieval

Additionally, the relevant excerpt of the Python code to read the database and create Autopsy artifacts is shown here:

```
# Code to connect to database and extract browser history items

        # Query the browser history tables in the database and get
necessary columns.
        # we need URL, Title and Visit Date
        try:
            stmt = dbConn.createStatement()
            resultSet = stmt.executeQuery("SELECT moz_places.url as
'URL', moz_places.title as 'Website Title', moz_historyvisits.visit_date as
'Visit Date' FROM moz_places  INNER JOIN moz_historyvisits ON
(moz_historyvisits.place_id = moz_places.id) ORDER BY 'Visit Date'")
        except SQLException as e:
            self.log(Level.INFO, "Error querying database for browser
history tables (" + e.getMessage() + ")")
            return IngestModule.ProcessResult.OK
```

```
        # Cycle through each row and create artifacts
        while resultSet.next():
            try:
                url  = resultSet.getString("URL")
                title = resultSet.getString("Website Title")
                visit_date_local = int(resultSet.getString("Visit Date"))/1000
# UNIX Timestamp is stored in db as milliseconds - needs to be in
seconds!
            except SQLException as e:
                self.log(Level.INFO, "Error getting values from browser
history tables (" + e.getMessage() + ")")


            # Make an artifact on the blackboard, TSK_WEB_HISTORY
and give it attributes for each of the fields
            art =
file.newDataArtifact(BlackboardArtifact.Type.TSK_WEB_HISTORY,
Arrays.asList(
                BlackboardAttribute(BlackboardAttribute.Type.TSK_URL,

WebHistoryDbIngestModuleFactory.moduleName, url),
                BlackboardAttribute(BlackboardAttribute.Type.TSK_TITLE,

WebHistoryDbIngestModuleFactory.moduleName, title),

BlackboardAttribute(BlackboardAttribute.Type.TSK_DATETIME_ACC
ESSED,

WebHistoryDbIngestModuleFactory.moduleName, visit_date_local)
            ))

            try:
                blackboard.postArtifact(art,
WebHistoryDbIngestModuleFactory.moduleName,
self.context.getJobId())
                recordCount +=1
            except Blackboard.BlackboardException as e:
                self.log(Level.SEVERE, "Error indexing artifact " +
art.getDisplayName())

        # Clean up
        stmt.close()
        dbConn.close()
        os.remove(lclDbPath)

    # Feedback to user how many database files were found.
    message =
IngestMessage.createMessage(IngestMessage.MessageType.DATA,
        "Wolvic VR Browser History Analyzer", "Found %d matching
database files" % fileCount)
    IngestServices.getInstance().postMessage(message)

    # feedback to user how many database records were turned into
Autopsy browser history artifacts.
    message =
IngestMessage.createMessage(IngestMessage.MessageType.DATA,
        "Wolvic VR Browser History Analyzer", "Processed %d browser
history artifacts" % recordCount)
    IngestServices.getInstance().postMessage(message)

    return IngestModule.ProcessResult.OK
```

IV. Evaluation of Results

The digital forensics methodology devised and used in this research managed to retrieve a significant yield of files relevant to a forensics investigation, in a forensically sound manner, making them admissible as evidence in a legal case.

A combination of the techniques described in the literature review, as well as the usage of the popular open source forensics application, Autopy as described in section IV, yielded 293 image files, 8 videos, and of particular interest to this paper, 33 database files. System and application log files were also discovered containing details of user accounts created and used on the device – these matched ones created for test purposes during the methodology phase both in name and in creation date and time. Of additional interest were username and password credentials which were not created by test users accounts, coded into several web.cfg files. This information disclosure could pose a security risk.

From these database files, it was possible to retrieve digital artefacts, such as browser history, user input and cookie data from the Wolvic web browser. One of the related SQLite databases named places.SQLlite contained a table called moz_places which held information about every unique website visited, along with the date and time of the most recent visit (held in a UNIX timestamp). Where these websites had been visited more frequently, we found corresponding entries in another database table called moz_historyvisits. This latter table linked to the moz_places table and held access dates and times in UNIX timestamps.

Overall, the bespoke Autopsy module developed during this research, found 100 web history artifacts, including the title, URL and access date/time of every website accessed using Wolvic browser as well as the 10 images downloaded intentionally during the data creation stage. The data revealed by the Autopsy plugin was able to be cross-referenced successfully with the URLs, titles and dates of the sites visited, and datetime file stamps on the image files themselves also corresponded with site visit dates and times, further enhancing the credibility of this evidence.

V. Discussion

This study aimed to develop a digital forensic methodology that could be used to investigate Pico 4 VR headsets. We argue that although similar methodologies have been developed for other VR headsets (erg., Meta Quest), our approach contributes to the field of digital forensics as the first to methodically focus on the Pico 4 as well as showing that existing technology, such as Autopsy can be utilized for newer devices with the help of custom plugins.

Two research questions were posed and addressed in this research:

A. Addressing RQ1: Types of artifacts identified

The investigation of the Pico 4 headset showed that analysis of web browser activity, done in this instance using a bespoke coded plugin solution for Autopsy, can be extremely lucrative for uncovering highly useful artifacts. This can then be used to create a timeline of a suspect's online activities. The evidence is forensically sound as the times and dates discovered by the plugin, were shown to be consistent with actions taken to initially create the artifacts.

B. *Addressing RQ2 – techniques used:*

Once web browser database files have been acquired in a forensically sound manner using the techniques discussed in the literature review and in the methodology, these can be passed to an automated digital forensics application, such as Autopsy, making the process of identification of relevant artifacts less technical, and hence easier. This aids in maintaining the integrity of evidence. Problems exist with tools, such as Autopsy, when using it to analyse new devices, such as the Pico 4, as they will miss certain types of data.

However, it is possible to write modules for Autopsy that can work specifically with newer devices and the data created and stored by their applications. These modules are written in scripting languages, such as Python, and once implemented, can allow Autopsy to scan and detect new artifacts, add them to its catalog and include them in its excellent reporting systems, such as timelines.

VI. THEORETICAL AND PRACTICAL IMPLICATIONS

The research showed that due to the nature of the file and security structure of Android devices, coupled with the freedom for developers to create and store data anywhere on the device, limits what data can be recovered, and means there is potential for misuse by criminals. Various Android apps allow encrypted, private conversations to take place, and the data for these cannot be retrieved or analysed. Whilst this may be reassuring to many users, it creates issues for digital forensic investigators, who may be unable to capture this information for their evidence files. This secrecy afforded on non-rooted devices could enable computer-based crimes, such as harassment, abuse and fraud, as well as aiding communication and planning of non-computer-based crimes which could have even more dire consequences. These limitations mean that there are areas of research into the Pico 4 (and other IoT devices) that lack clarity.

Web browsers, such as the Wolvic browser which can be installed from the Pico app store, successfully yield all of their browser history, cookies, user input and downloaded files. This information is contained within database files, which can be easily read and processed by suitable coded modules for forensic apps, such as Autopsy.

This research provides an example of such scripting using Python coding, and this could be drawn on as a starting place to develop similar scripts for future IoT and VR devices.

VII. LIMITATIONS AND FUTURE RESEARCH

While this study provides a foundational forensic methodology for investigating the Pico 4 VR headset, several limitations remain.

The experimental design involved artificially generating test data on the Pico 4 rather than analyzing real-world forensic case data. While this method ensures controlled conditions for evaluating forensic techniques, it does not account for the complexity of real investigations where data may be deliberately hidden, fragmented, or manipulated. Future studies should seek to apply the methodology in real investigative contexts, analyzing seized VR devices from actual cases to assess the practical challenges and effectiveness of the proposed techniques in more complex scenarios.

A comparative study evaluating forensic techniques across multiple VR headsets, such as the Meta Quest 2 and HTC Vive, could provide a broader understanding of forensic methodologies applicable to different hardware and software ecosystems.

One area requiring further research is the role of forensic automation and artificial intelligence in VR investigations. While this study successfully integrated Autopsy for data analysis, the development of custom forensic modules was not fully explored. Automated techniques, including machine learning-driven artifact classification, could enhance the efficiency of forensic investigations by reducing manual effort and improving the detection of relevant artifacts. Additionally, exploring the use of AI-driven analysis in VR-specific forensics, such as behavioral pattern recognition within virtual environments, could open new avenues for detecting criminal activity within immersive platforms.

VIII. CONCLUSION

The objective of this study was to develop a forensic methodology tailored to the Pico 4 VR headset – with this paper focusing primarily on the Autopsy plugin developed. Our findings indicate that it is indeed possible to use open source techniques to forensically investigate the Pico 4 headset without having to root it. These findings, and our methodology, provide investigators with a practice-oriented approach they could use to investigate VR-based devices. Together with the Autopsy plugin we developed, this study contributes on three fronts. First, it establishes a structured digital forensic methodology tailored for the Pico 4 VR headset. Second, it provides a detailed analysis of artifact extraction techniques and their forensic significance, serving as a practical reference for investigators in the field. Third, it practically demonstrates how investigators could extract evidence from Android-based IoT devices without the need to perform low-level modifications (i.e., rooting) yet still maintain evidence integrity. We argue that, together, these contributions not only advances our theoretical understanding of VR-based evidence but also enables investigator to extract it.

ACKNOWLEDGMENT

The author wishes to thank Professors Karl van der Schyff and Ian Fergusson for their invaluable support and guidance throughout the development of this work.

REFERENCES

[1] Statista, “IoT connections worldwide 2022-2033,” [Internet], 2022. Available from: https://www.statista.com/statistics/1183457/iot- [retrieved: March, 2026].

[2] A. Crawford. “Child abuse material found on VR headsets, police data shows,” BBC News [Internet], 2023. Available from: https://bbc.co.uk/news/uk-64734308 [retrieved: March, 2026].

[3] A. Gutierrez. “Pico 4: features, price and specifications of the new VR headset,” Ludusglobal.com [Internet], LUDUS TECH SL, 2023. Available from: https://www.ludusglobal.com/en/blog/pico-4-features-price-specifications-vr-headset [retrieved: March, 2026].

[4] A. Alazab, A. Khraisat, and S. Singh. “A Review on the Internet of Things (IoT) Forensics: Challenges, Techniques, and Evaluation of Digital Forensic Tools,” IntechOpen [Internet], 2023. Available from: https://www.intechopen.com/online-first/86010 [retrieved: March, 2026].

[5] M. Eichhorn, J. Schneider, and G. Pugliese. “Well Played, Suspect! – Forensic examination of the handheld gaming console ‘Steam Deck’,” Forensic Science International: Digital Investigation, vol. 48, p. 301688, Mar 1, 2024.

[6] E. Raymer, A. MacDermott, and A. Akinbi. “Virtual reality forensics: Forensic analysis of Meta Quest 2,” Forensic Science International: Digital Investigation, vol. 47, p. 301658, Dec 1, 2023. [retrieved: March, 2026].

[7] M. Taylor, G. Hughes, J. Haggerty, D. Gresty, and P. Almond. “Digital evidence from mobile telephone applications,” Computer Law & Security Review, vol. 28, no. 3, pp. 335–339, Jun 1, 2012. [retrieved: March, 2026].

[8] A. Arslan. “Why Doesn’t Android Come Rooted?” MUO [Internet], 2013. Available from: https://www.makeuseof.com/tag/why-doesnt-android-come-rooted [retrieved: March, 2026].

[9] İ. Kara. “Digital Forensic Analysis of Discord Mobile Application on Android Based Smartphones,” Acta Infologica, vol. 0, no. 0, Oct 31, 2022.

[10] K. Gupta, P. Lanka, and V. Cihan. “A holistic digital forensic analysis of Discord – Storage, memory, and network perspectives,” Journal of Forensic Sciences, vol. 69, no. 4, pp. 1320–1333, May 28, 2024.

[11] R. Neisse, G. Steri, D. Geneiatakis, and I. N. Fovino. “A privacy enforcing framework for Android applications,” Computers & Security, vol. 62, pp. 257–277, Sep 2016.

[12] ProQuest. “A Methodology for Smart TV Forensics,” Proquest.com [Internet], 2021. Available from: https://www.proquest.com/docview/2505730094 [retrieved: March, 2026].

[13] M. McKinnon. “Data Source Ingest Module Template,” [Online], 2022. Available from: https://github.com/sleuthkit/autopsy/blob/develop/pythonExamples/dataSourceIngestModule [retrieved: March, 2026].