The Development of an IoT-Focused Investigative Methodology:

The Case of a Pico 4 Headset

Presented by:
Luke Yates, Abertay University, Dundee (l.yates@abertay.ac.uk)

Authors:
Luke Yates, Abertay University, Dundee (l.yates@abertay.ac.uk)
Prof. Ian Ferguson – Abertay University, Dundee (i.ferguson@abertay.ac.uk)
(Dr. Karl van der Schyff Abertay University, Dundee (k.vanderschyff@abertay.ac.uk)

About the presenter

Luke Yates

I am from Kent, UK and studied Msc Cybersecurity and Ethical Hacking at Abertay from 2002 to 2004 achieving a Distinction. The paper I have presented to this conference was written during that time.

I have worked in education for 13 years, at Secondary, Further and then Higher Level. Prior to this I worked in the computing industry in several roles, including a software and website developer.

I am currently working at Buckinghamshire New University as a Graduate Teaching Associate, and about to embark on my PhD, which will consider cybersecurity and human engineering aspects.
I am also still working for Abertay University as an online lecturer.

When I am not working, I play guitar in a punk band, am a semi-professional photographer and also enjoy long distance running, including marathon-distance races.

Introduction & Research Motivation

- The rapid growth of IoT devices introduces new digital forensic challenges.
- VR headsets increasingly used for crimes like fraud, harassment, and identity theft
- The Pico 4 (released Oct 2022) is an Android-based VR device
- Outdated forensic methodologies may fail to capture evidence from modern VR hardware.
- Lack of clear techniques can lead to evidence being excluded from legal proceedings.
- The study presents the first tailored digital forensic approach for the Pico 4.

Research Questions (RQs)

RQ1: What digital artifacts are acquired in VR-focused investigations?

RQ2: How can these artifacts be extracted in a forensically sound manner?

- Investigation prioritised maintaining data integrity without compromising hardware.
- Special emphasis was placed on navigating the security of non-rooted devices
- The research explored using both existing tools and bespoke software adaptations – the paper presented focuses on the latter.

Challenges in Android & IoT Forensics

- IoT forensics requires specialized approaches for GPS, sensors, and cameras.
- "Cloud jurisdiction" creates obstacles when data is stored in different countries
- Android’s security model assigns unique user IDs to apps, complicating data acquisition
- Rooting a device is risky, potentially voiding warranties or destroying evidence
- Manufacturers lock boot-loaders on new devices to discourage rooting attempts
- Encrypted communications in many apps remain inaccessible on non-rooted devices

Methodology & Data Acquisition

- The study used the Android Debug Bridge (ADB) suite for data capture
- ADB commands like "backup" and "dumpsys" helped ensure data remained forensically sound
- Differential analysis was performed using "before and after" device snapshots
- Initial state: 49.38MB; after user activity, data grew to 13.38GB
- MD5 file hashes were used to identify new or modified files effectively, reducing manual workload considerably.
- (Ethical clearance for the methodology was granted by the primary university)

Custom Autopsy Module Development

- A bespoke module was written for Autopsy to automate browser data analysis
- The module used a Jython parser to interface Python with Java-based Autopsy
- It targeted the "places.sqlite" database from the Wolvic VR web browser
- The script extracted URL, website title, and access date/time information
- Data converted from UNIX milliseconds to seconds for proper timestamping (also handled by module)
- Retrieved artifacts are automatically placed in Autopsy’s "Web History" container along with any other artifacts

Key Findings & Evaluation

- The entire methodology retrieved 293 images, 8 videos, and 33 database files
- System logs revealed user account details matching the experimental test data
- A security risk was identified: usernames and plain text passwords found in "web.cfg" files
- The custom Jpython-based plugin specifically identified 100 web history artifacts from the Wolvic browser
- Artifacts were cross-referenced with file timestamps to ensure credibility
- The process demonstrated significant data is accessible without needing to root.

Implications & Future Research

- Theoretical: Android's structure limits recovery but user naivety can aid investigations
- Practical: The Python script serves as a template for future IoT/VR devices.
- Limitation: Test data was artificially generated rather than from real-world cases
- Future Work: Apply this methodology to real-world criminal investigation data.
- Future Work: Comparative studies across other headsets – such as Meta Quest and HTC headsets
- Innovation: Exploring AI and machine learning for automated artifact classification

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. [retrieved: March, 2026].

[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