Several challenges were encountered during the recovery process, highlighting the need for customized approaches to handle Flipper Zero's unique file types:

Extra Bytes (Padding): PhotoRec recovered files with trailing padding bytes (\x00 sequences), which made the recovered data longer than the original files. This issue caused discrepancies in file size and posed challenges in validating the integrity of the recovered files. To address this, a Python script was developed to detect and truncate these padding sequences, ensuring that the recovered files matched their original size.

Signature Ambiguities: Some file types, such as BadUSB scripts, lacked consistent binary patterns, complicating the creation of custom signatures. Default recovery methods struggled to correctly identify these files, resulting in a high mismatch rate. This challenge was overcome by developing a custom signatures dictionary based on mapped command sets from Flipper Zero documentation, significantly improving recognition accuracy.

BadUSB False Positive Issue: The BadUSB false positive issue arose due to an interaction with PhotoRec's default configuration, which already recognized certain files as .txt based on their structure, even though they contained data matching BadUSB patterns. Two files from the dataset were not recovered using custom signatures but were correctly identified by the default PhotoRec settings, which support general .txt files. The issue occurred because these files started with a *, used for comments, which was not included in the custom dictionary, as the documented command set for BadUSB files did not mention * as a valid pattern. When the file extension was temporarily changed to .badusb, the custom signature successfully identified 38 out of 40 BadUSB files, while the remaining two files continued to be identified as .txt. This explains the difference between the Identification Rate (I) and Recovery Rate (R) in the improved results: Fidentify recognized all 40 BadUSB files, but PhotoRec only recovered 38, indicating that two files were false positives, misidentified as .txt by PhotoRec. Hence, the discrepancy between Fidentify's 100% identification and PhotoRec's 95% recovery rate was due to the default configuration's recognition of .txt files. This highlights the need to update the custom dictionary to account for the * character and to conduct further testing to identify other undocumented patterns. While custom signatures are effective, they require comprehensive documentation and rigorous testing to address edge cases, and manual verification remains critical when dealing with incomplete or evolving specifications.

The study also revealed several unique issues related to the recovery of Flipper Zero files:

Limited Support for Flipper Zero-Specific Formats: Many forensic tools lack built-in support for file types such as .ir, .rfid, .nfc, .sub, and .ibtn, which are unique to Flipper Zero. To overcome this limitation, custom signatures were developed to enable accurate recognition and recovery of these file types.

Proprietary Patterns and Unconventional Data Structures: Certain file types, like iButton, use unique patterns and data structures that are not easily detectable by general-purpose recovery tools. Manual pattern analysis and creating custom signatures were crucial to effectively addressing this challenge.

V. Conclusion

Implementing custom signatures significantly enhanced the identification and recovery rates for specialized file types, such as Infrared, RFID, NFC, Sub-GHz, and iButton, achieving 100% accuracy in identification (I) and recovery (R). This approach effectively addressed the limitations of the default PhotoRec configuration, particularly for file types with unique characteristics like Flipper Zero's proprietary formats. However, challenges like trailing padding bytes and needing specialized custom dictionaries were encountered, particularly with file types such as BadUSB scripts requiring further refinement. Despite these challenges, custom signatures improved considerably over default settings, underscoring the importance of tailored recovery methods and thorough testing for handling unique file formats. Manual verification and continuous updates to the custom dictionary remain essential for handling evolving or undocumented file types and ensuring the accuracy of recovery processes.

References

[1] Flipper Zero, "Flipper Zero," 2024. [Online]. Available: https://flipperzero.one/.

[2] Flipper Devices, Flipper Zero Documentation. [Online]. Available: https://docs.flipper.net/.

[3] A. S. Thakur and R. Singh, "Navigating the Flipper Zero: A comprehensive tool for cybersecurity professionals," International Journal of Research Publication and Reviews, vol. 5, no. 6, pp. 551–554, Jun. 2024.

[4] Pava, Robert & Martin, Reese & Mishra, Sushma. (2024). Unveiling exploitation potential: a comparative analysis of flipper zero and rubber ducky. Issues in Information Systems. 25. 84-95.

[5] Sourabh, S., Chauhan, M. (2021). Computer File Signature Analysis Through Hexadecimal Editor Software. In: Abraham, A., Castillo, O., Virmani, D. (eds) Proceedings of 3rd International Conference on Computing Informatics and Networks. Lecture Notes in Networks and Systems, vol 167. Springer, Singapore. https://doi.org/10.1007/978-981-15-9712-1_9

[6] Suryadithia, R., Endah Pangesti, W., Faisal, M., Nurrohman, A., & Syah Putra, A. (2022). FTK Image For Forensic Data Processing In Forensic Tools. International Journal of Information System & Technology Akreditasi, 5(158).

[7] Pratama, I. P. A. E. (2021). Computer Forensic Using Photorec for Secure Data Recovery Between Storage Media: a Proof of Concept. International Journal of Science, Technology & Management, 2(4). https://doi.org/10.46729/ijstm.v2i4.256

[8] Vayadande, K., Mandhana, R., Paralkar, K., Pawal, D., Deshpande, S., & Sonkusale, V. (2022). Pattern Matching in File System. International Journal of Computer Applications, 183(52). https://doi.org/10.5120/ijca2022921936

[9] Exterro, "FTK Imager," 2024. [Online]. Available: https://www.exterro.com/digital-forensics-software/ftk-imager.

[10] TestDisk and PhotoRec, "TestDisk," 2024. [Online]. Available: https://www.cgsecurity.org/.

[11] Bosnjak, L., Sres, J., & Brumen, B. (2018). Brute-force and dictionary attack on hashed real-world passwords. 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2018 - Proceedings. https://doi.org/10.23919/MIPRO.2018.8400211

[12] Flipper Devices, "Flipper Zero Firmware," GitHub repository, 2024. [Online]. Available: https://github.com/flipperdevices/flipperzero-firmware