File Signature Identification of Flipper Zero Device to Support File Recovery

1st Maxwealth Fereli
School of Computing, Telkom University
Bandung, Indonesia
kuraishishi@student.telkomuniversity.ac.id

2nd Niken Dwi Wahyu Cahyani
School of Computing, Telkom University
Bandung, Indonesia
nikencahyani@telkomuniversity.ac.id

3rd Muhammad Irsan
School of Computing, Telkom University
Bandung, Indonesia
irsanfaiz@telkomuniversity.ac.id

***Abstract*—The Flipper Zero is a versatile tool popular in cybersecurity and hardware hacking. This study bridges the gap by developing custom file signatures tailored for PhotoRec, enabling accurate identification and recovery of Flipper Zero-specific file types such as Infrared, RFID, NFC, Sub-GHz, and iButton. Using a pattern-matching and dictionary-based approach, the research achieved a 100% recovery rate for these specialized file types, significantly surpassing default PhotoRec configurations, which only identified a fraction of these file types. Additionally, while challenges were encountered in recovering general file types like BadUSB due to inconsistent or undocumented patterns, the custom signatures resulted in a notable improvement in recovery accuracy. These findings demonstrate the enhanced capability of custom signatures in adapting forensic investigations to emerging technologies, underscoring their potential for improving recovery tools in handling proprietary formats.**

Keywords— Flipper Zero, file recovery, digital forensics, custom signatures, PhotoRec

I. Introduction

Flipper Zero is a portable, multi-functional tool that has gained widespread attention in the field of penetration testing. It is particularly valuable for interacting with access control systems, RFID, NFC, and digital radio protocols. This versatility makes it an excellent choice for forensic applications, where diverse data recovery scenarios often arise. With its open-source design, robust customization options, and the ability to store and emulate various signal types on MicroSD cards, Flipper Zero has become an indispensable resource in investigating unauthorized access and exploiting vulnerabilities in hardware systems within cybersecurity contexts [1][2].

The utility of Flipper Zero in these areas has been well-documented in the research literature. Studies such as those by Thakur and Singh (2024) [3], in "Navigating The Flipper Zero, A Comprehensive Tool for Cybersecurity Professionals", explored the versatile applications of Flipper Zero's attack methods and evaluated their effectiveness across various cybersecurity scenarios. Similarly Pava et al. (2024) [4], in "Unveiling Exploitation Potential: A Comparative Analysis of Flipper Zero and Rubber Ducky", conducted a comparative analysis, highlighting Flipper Zero's exploitation potential relative to the Rubber Ducky. Both studies have demonstrated its adaptability and robust functionality in penetration testing. Despite its strengths, one area that has been less explored is the challenge of recovering data from Flipper Zero during forensic investigations. As digital forensics continues to evolve, there is a growing need to enhance data recovery capabilities from such devices.

In their study, Sourabh and Chauhan (2021) [5], discussed the concept of file signature analysis, focusing on its role in identifying and verifying file types. A file signature is a unique hexadecimal value stored in the header of a file, which acts as an identifying feature for the file format. This value is crucial for detecting tampered files, particularly when the file extension is manipulated to disguise its true nature. The authors highlight how file signatures, which consist of a combination of hexadecimal values ranging from '0' to '9' and 'A' to 'F', are embedded in both the header and footer of a file. These signatures remain unchanged even if the file extension is altered. By using hexadecimal editor software such as HxD, investigators can access and examine the file signature to identify the true format of a file. This method is vital in forensic analysis, as it allows analysts to recover hidden information by comparing the extracted file signature with a known database of signatures, thus ensuring the correct file extension is restored and tampered data is exposed.

This concept of file signature analysis directly relates to this paper, where the same technique is applied to identify and recover files from the Flipper Zero device. The Flipper Zero, like other devices, stores data in various file formats. By leveraging file signature identification, the paper explores how signature analysis can be used to accurately identify the format of files extracted from the device, even if the file extensions are manipulated. This reinforces the importance of file signature analysis in digital forensics, particularly in the context of recovering files from devices like the Flipper Zero.

Previous research has focused mainly on the exploitation and functionality of Flipper Zero but has overlooked data recovery techniques. Tools like PhotoRec, widely used for file carving, lack optimized support for Flipper Zero-specific file types. This study aims to address this gap by focusing on improving PhotoRec by creating and implementing custom file signatures tailored to Flipper Zero's data types. Digital forensic investigations often require acquiring and analyzing data from various storage media to uncover and interpret electronic evidence. Previous studies have highlighted the importance of reliable tools in digital forensic investigations. Suryadithia et al. (2022) [6] demonstrated the effectiveness of FTK Imager in creating forensically sound images of storage devices, emphasizing its role as a trusted solution for acquiring and preserving digital evidence. Similarly, Pratama (2021) [7] explored the capabilities of PhotoRec, showcasing its ability to recover files across various formats and storage media. This research underscored PhotoRec's practicality in scenarios requiring secure data recovery, highlighting its application in forensic workflows. These foundational studies provide essential insights into the capabilities of existing tools and set the stage for further advancements, such as the development of custom file signatures tailored to specific

devices like the Flipper Zero.Tools like FTK Imager have become staples in the forensic community due to their reliability in creating forensically sound images of storage devices [6]. Likewise, data recovery tools such as PhotoRec have proven effective in retrieving files across various formats and storage media [7]. This paper builds on these foundational tools by exploring the deliberate embedding of data into a Flipper Zero device, imaging the storage media, and evaluating the impact of custom file signatures obtained through pattern matching and dictionary-based approach on data recovery and carving processes.

In this context, Vayadande et al. (2022) [8], describe the Naive algorithm for pattern matching, emphasizing its straightforward approach of individually sliding the pattern over the text. In integrating this algorithm within the file system, we leveraged its simplicity and effectiveness for detecting file signatures, particularly in identifying common binary patterns across files with uniform structures. This Naive approach was chosen due to its low computational overhead and suitability for short patterns, such as file headers, making it an optimal choice for our signature identification task.

Through this research, we aim to contribute to the field of digital forensics by enhancing the ability to recover and analyze data from Flipper Zero devices, offering new insights into how forensic investigations can adapt to emerging technologies.

II. Environment And Experimental Setup

A. Environment

- Device: Flipper Zero
- Firmware: Version 1.1.2
- Storage: SanDisk 32GB microSD (FAT32)

B. Tools Specifications

- qFlipper is a Windows, macOS, and Linux desktop application that allows users to update Flipper Zero firmware and databases, manage microSD card files, repair corrupted firmware, and report issues [2].
- FTK Imager: FTK Imager is a data preview and imaging tool used to acquire electronic evidence in a forensically sound [9].
- PhotoRec: PhotoRec is a free, open-source data recovery tool designed to recover lost files like photos, videos, and documents by identifying file signatures. It works across various platforms, including Windows, macOS, and Linux [10].
- Fidentify: Fidentify is a tool that uses the same database as PhotoRec to identify a file's type or extension. It also uses the same signatures as PhotoRec to check files in a directory, helping verify whether PhotoRec can recover specific file formats or extensions [10].
- Python 3: a programming language used for many purposes, including custom scripts for processing.

C. Dataset

Flipper Zero natively supports these file types, showcasing its broad capabilities. The device's ability to store, emulate, and interact with these data types highlights its utility in recovering and analyzing device-specific data in forensic scenarios. The six file types were selected to comprehensively evaluate data recovery methods, encompassing text-based scripts, signal protocols, and hardware authentication data. This variety helps demonstrate the effectiveness of the custom signatures developed in this study across different data structures. As shown in TABLE I, Planted data encompass six Flipper Zero file types [1][2]. The BadUSB (.txt) files are frequently used in cybersecurity experiments to simulate malicious USB attacks, such as keystroke injection and malware payloads that can infect connected systems. Forensically recovering these files aids in identifying the misuse of USB devices in cybercrime, including unauthorized access and data exfiltration. In this study, BadUSB files were employed to simulate typical USB-based attack scenarios, which are crucial for evaluating how forensic tools handle and recover such data. Additionally, the Infrared (.ir), RFID (.rfid), NFC (.nfc), Sub-GHz (.sub), and iButton (.ibtn) file types represent data from various technologies used for device control, access systems, and communication. These file types are essential for understanding how forensic tools can recover data from different signal-based systems, including RFID access cards, NFC payment systems, and Sub-GHz IoT devices. The inclusion of these data types in the dataset helps assess the tool's ability to handle proprietary or non-standard formats, which may be subject to misuse in unauthorized access or signal interception scenarios.

TABLE I. Flipper Zero file types

No	Flipper Zero file types		
	Data Type	***Extension***	***Count***
1	BadUSB	.txt	40
2	Infrared (IR)	.ir	40
3	RFID	.rfid	40
4	NFC	.nfc	40
5	Sub-GHz	.sub	40
6	iButton	.ibtn	40

- BadUSB (.txt): BadUSB scripts are commonly used in cybersecurity experiments to simulate malicious USB attacks. Forensically recovering these files helps identify potential misuse of USB devices in cybercrime.
- Infrared (.ir): Infrared signals are widely used in consumer electronics like TVs and air conditioners. Forensics on these files could aid in reconstructing signal misuse or testing signal recovery for device control.
- RFID (.rfid): RFID files represent access control systems vulnerable to cloning or unauthorized access. Recovering these files is essential for investigating breaches in physical security systems.
- NFC (.nfc): NFC is critical in modern smart cards and payment systems. Forensic recovery of NFC data can provide insights into unauthorized transactions or data tampering.
- Sub-GHz (.sub): Sub-GHz frequencies are used in IoT devices, garage door remotes, and wireless sensors. Recovering these files supports forensic analysis of