Weaponized IoT: A Comprehensive Comparative Forensic Analysis of Hacker Raspberry Pi and PC Kali Linux Machine

Mohamed Chahine Ghanem * , Eduardo Almeida Palmieri , Wiktor Sowinski-Mydlarz , Dipo Dunsin , Sahar Al-Sudani

Posted Date: 10 February 2025

doi: 10.20944/preprints202501.0203.v3

Keywords: IoT Forensics; Raspberry Pi; Single-Board-Computers; CyberCrime; Digital Forensics; Linux; Kali; Hacking; Digital investigation; Weaponized IoT; Exterro FTK; Volatility; Magnet AXIOM

 doi:10.20944/preprints202501.0203.v3

Article

Weaponized IoT: A Comprehensive Comparative Forensic Analysis of Hacker Raspberry Pi and PC Kali Linux Machine

Mohamed Chahine Ghanem *, Eduardo Almeida Palmieri, Wiktor Sowinski-Mydlarz, Dipo Dunsin and Sahar Al-Sudani

Cyber Security Research Centre, London Metropolitan University, London, UK
* Correspondence: m.ghanem@londonmet.ac.uk

Abstract: The proliferation of Internet of Things (IoT) devices has introduced new challenges for digital forensic investigators due to their diverse architectures, communication protocols, and security vulnerabilities. This research paper presents a case study focusing on the forensic investigation of an IoT device, specifically a Raspberry Pi configured with Kali Linux as a hacker machine. The study aims to highlight differences and challenges in investigating weaponised IoT as well as establish a comprehensive methodology for analysing IoT devices involved in cyber incidents. The investigation begins with the acquisition of digital evidence from the Raspberry Pi device, including volatile memory and disc images. Various forensic tools and utilities are utilised to extract and analyse data, such as Exterro FTK and Magnet AXIOM, as well as open-source tools like Volatility, Wireshark, and Autopsy. The analysis involves examining system artefacts, logfiles, installed applications, and network connections to reconstruct the device's activity and identify potential evidence proving that the user perpetrated security breaches or malicious activities. The research results help improve IoT forensics by showing the best ways to look at IoT devices, especially those that are set up to be hacker machines. The case study demonstrates how the research results are helping to improve IoT forensic capabilities by showing the best ways to look at IoT devices, especially those that have been set up as hacker machines. The case study shows how forensic methods can be applied in IoT settings. It helps in creating guidelines, standards, and training for those who work as IoT forensic investigators. In the end, improving forensic readiness in IoT deployments is needed to keep essentials safe from cyber threats, keep digital evidence safe, and keep IoT ecosystems running smoothly, which protects the integrity of IoT ecosystems.

Keywords: IoT Forensics; Raspberry Pi; Single-Board-Computers; CyberCrime; digital forensics; Linux; Kali; hacking; digital investigation; weaponized IoT; Exterro FTK; volatility; Magnet AXIOM

1. Introduction

IoT devices continue to proliferate at an unprecedented rate, and it is forecasted that by 2025, they will make up more than two-thirds of an estimated 41.6 billion internet-connected devices [1]. These devices, ranging from smart home gadgets to complex industrial systems, form a core part of modern ecosystems but also pose new challenges for cybersecurity and forensic investigations. Compact, low-cost single-board computers, such as the Raspberry Pi, exemplify this duality. While these devices are in general deployed as central components in IoT environments for the collection, control, and analysis of sensor data, praised for their high processing power, low price, and user-friendliness, they can easily be utilized by cyber-criminals when loaded with tools like Kali Linux as machines for hacking. This dual-purpose nature underscores the requirement for specialist IoT forensic techniques.

IoT forensics is a relevant and relatively new area, adding new dimensions in cybercrime that present challenges for digital forensics. IoT forensics refers to the identification, collection, and preservation and analysis of digital evidence from IoT devices. Its importance lies in providing insights

 doi:10.20944/preprints202501.0203.v3

into how devices communicate with each other, their network behavior, and user activities—the key elements that can be used to solve incidents such as data breaches, cyberattacks, or even physical crimes. IoT ecosystems generate vast volumes of data, and as the systems become ubiquitous, it will only increase the necessity for robust forensic methodologies in place [2].

IoT forensics includes several important subdomains: device, live, network, and cloud forensics. IoT devices—often, though not always, called "things"—pose challenges to forensics. Some bear permanent storage with recognizable file systems and formats, so traditional forensics works. Yet, others are based on proprietary file systems or do not have permanent memory at all, which complicates evidence collection. Power supply limitations, low RAM, and real-time data transfer worsen the situation for live forensics. The data transferred over the networks can be encrypted. Moreover, IoT data, when processed in cloud environments, often resides at remote and sometimes unknown geographical locations, making retrieval and analysis even more complicated [3].

Forensic investigations of IoT devices are further complicated by the volatility of IoT data, the intricate architectures of IoT ecosystems, and the integration of these devices into larger network infrastructures. There are also legal and ethical issues to contend with, including privacy and ensuring a proper chain of custody.

Figure 1 shows the sub-components of IoT forensics and corresponding sources of artefacts, which include:

- Criminal-operated Linux systems (e.g., command-and-control servers).
- Abused or misused Linux systems (e.g., by suspect users)
- Imaged systems (e.g., dead disks)
- Standalone artefacts from Linux distributions
- Raspberry Pi devices running Kali Linux
- Metapackages from other platforms

The uniqueness of IoT forensic investigations demands specialized techniques and tools tailored to the constraints and complexities of these environments. The diversities of the evidence sources are depicted in Figure 1, showing diversity and complexity, which need to be handled with care to analyze the artefacts for accurate and reliable output [4].

 doi:10.20944/preprints202501.0203.v3

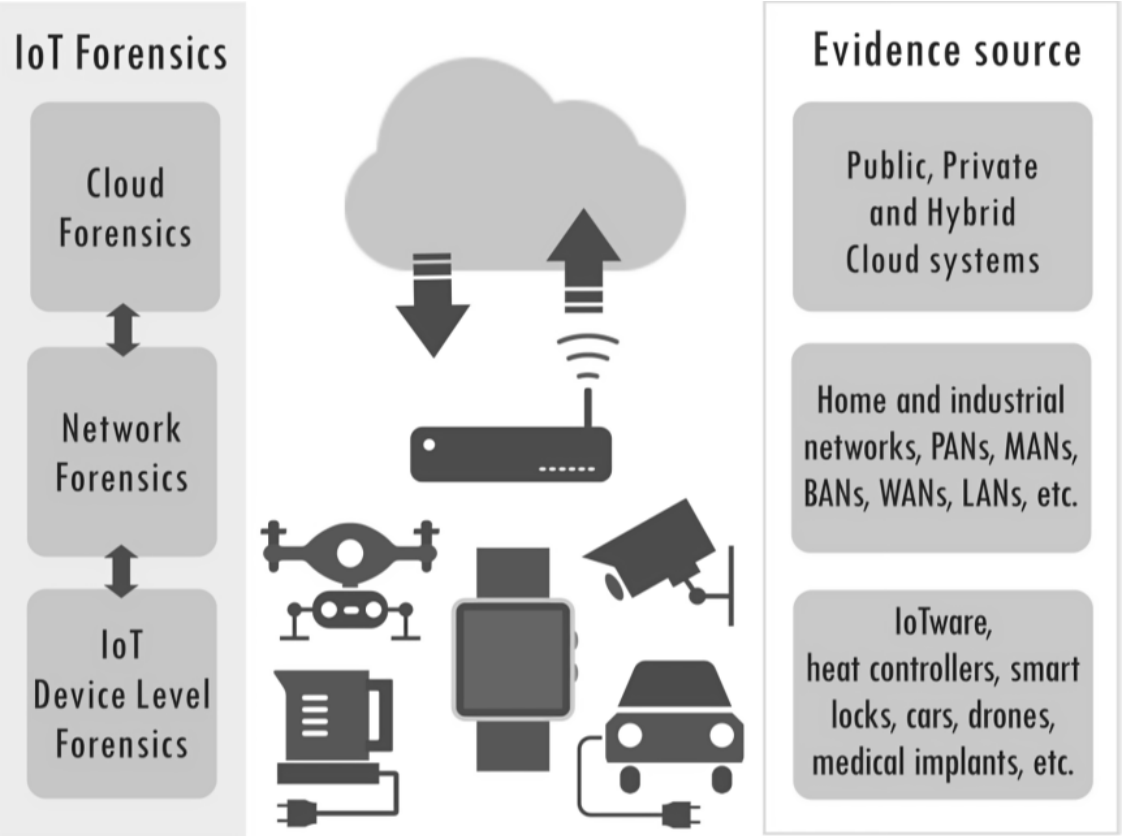

Figure 1. IoT Forensics Domain and Artefacts Categories [4].

Lastly, even though the defence-in-depth approach is obviously necessary in securing an IoT ecosystem, it opens up new complexities for forensic investigations. This involves the application of different mechanisms to protect against possible attacks. However, these defense layers are often compromised due to human errors, misconfigurations, and built-in system vulnerabilities [5]. Since cyber threats have been diversifying and intensifying, a growing number of security controls and measures compound the challenges faced by forensic analysts [6]. These would require not only technical expertise but also deep knowledge of the peculiarities of IoT environments.

This research investigates the forensic processes involved in analysing a Raspberry Pi configuration using Kali Linux as a tool for IoT-based cyberattacks. The study seeks to highlight the differences between forensic investigations conducted on conventional computers and those on IoT devices, particularly in terms of artefact extraction, data retention, and forensic tool compatibility. Additionally, it examines the challenges faced in IoT forensics and proposes best practices to enhance forensic readiness for such attacks.

1.1. Research Motivation

IoT forensics presents complex challenges across several dimensions, starting with evidence source identification, as evidence is often distributed across a variety of interconnected devices with different protocols and data storage formats. Evidence acquisition or forensics imaging is also a challenge, given IoT devices' limited storage, proprietary data formats, and reliance on cloud-based storage, which complicates access [7]. Additionally, traditional forensic tools and techniques are insufficient for IoT-specific needs, as they are not designed to handle the unique architectures and data formats of IoT devices, this necessitates utilising specialised tools. These factors highlight the importance of customized forensic strategies and international legal collaboration to effectively address the complexities of IoT investigations.

 doi:10.20944/preprints202501.0203.v3

1.2. Research Questions

Our Research Questions are formulated as follows:

- **RQ1**: How do forensic processes differ between conventional computers and IoT Devices such as Raspberry Pi devices?
- **RQ2**: What are the key differences in terms of meaningful forensics artefacts between conventional computers and IoT Devices?
- **RQ3**: What are the current challenges and limitations in IoT Forensics and possible best practices to implement to overcome these challenges?

The reminder of this paper is organised as follows: Section 2 presents a literature review on key aspects of IoT forensics. It explores the key challenges and opportunities within the IoT environment, particularly focusing on cybersecurity and deterrence strategies. It critically reviews existing research on ethical hacking and penetration testing and provides a brief comparison with related works. Section 3 describes the methodology employed in this research, focusing on the creation of a test-bed that simulates environments where conventional PCs and the Raspberry Pi, operate together as well as the providing detailed account of the comparative forensics investigation performed. Section 4 presents the research findings and discusses the differences in forensic capabilities between conventional PCs and the Raspberry Pi. Section 5 concludes the paper by emphasizing the significant differences in forensic capabilities between traditional PCs and Raspberry Pi devices, particularly highlighting Raspberry Pi limitations such as storage and compatibility issues. It recommends conventional PCs as a more robust and reliable forensic platform for forensic applications.

2. Literature Review

As IoT devices proliferate across various domains, understanding the unique characteristics of IoT forensics becomes imperative for effective investigation and incident response. This section highlights the scope of IoT Forensics. IoT forensics encompasses a broad range of activities and challenges related to investigating and analysing digital evidence from Internet of Things (IoT) devices and systems. The scope of IoT forensics extends beyond traditional digital forensics practices to address the unique challenges posed by interconnected, heterogeneous, and pervasive IoT environments [8]. The Internet of Things (IoT) is gaining popularity, and numerous sectors have drawn attention to the topic of IoT security and forensics. Research efforts on IoT security and forensics are extensive and cover a wide range of topics, from the theoretical underpinnings of cybersecurity to the practical challenges of securing and investigating IoT devices [7]. The use of low-cost, portable tools like the Raspberry Pi has emerged as a recurring theme, offering both opportunities and challenges in the field of IoT forensics. Future research should continue to explore these areas, particularly focusing on the development of more robust forensic tools and methodologies tailored to the unique challenges posed by IoT environments. This literature review synthesizes key studies focusing on different aspects of IoT security, digital forensics, and the use of low-cost, portable tools like the Raspberry Pi for these purposes. It also offers a thorough examination of existing research on the use of Raspberry Pi in hacking and forensic analysis. It explores the performance, capabilities, and vulnerabilities of these devices within IoT environments, highlighting the crucial role of IoT forensics in criminal investigations and the importance of strong security measures [9]. The uniqueness of IoT forensics can be summarized in the following points:

1. **Device Diversity:** IoT devices come in various forms, including single-board computers (SBC), sensors, actuators, wearables, smart home appliances, and industrial controllers making the task address the diversity in device types, architectures, communication protocols, and operating systems challenging.
2. **Data Acquisition:** Retrieving data from IoT devices while preserving its integrity and ensuring admissibility in legal proceedings is complex with many challenges such as accessing data stored in volatile memory, retrieving logs and configuration settings, and capturing network traffic.

 doi:10.20944/preprints202501.0203.v3

3. **Distributed Nature:** IoT environments involve numerous geographically distributed devices, making data collection and analysis challenging, especially with real-time data generation.
4. **Scalability Issues:** The vast number of devices and data in IoT systems demands new forensic approaches to efficiently process and analyse large-scale information.
5. **Heterogeneous Protocols:** IoT devices use various communication protocols, requiring forensic experts to understand and analyse diverse and often complex interactions.
6. **Privacy and Legal Concerns:** IoT devices collect sensitive data, raising privacy issues. Forensic investigations must navigate legal frameworks to ensure evidence is admissible without violating privacy rights.

Analysing data obtained from IoT devices involves examining logs, event traces, metadata, communication patterns, and potentially large volumes of sensor data. Therefore, investigators need tools and techniques to process, interpret, and correlate diverse data sources for reconstructing events and identifying evidence. Network Forensics refers to IoT devices' communication over wireless and wired networks, this presents challenges for capturing, analysing, and reconstructing network traffic [10]. Therefore, investigators must consider encryption, encapsulation, and fragmentation mechanisms used in IoT communication protocols. Many IoT deployments leverage cloud and edge computing platforms for data processing, storage, and analytics. Forensic investigations may involve accessing data stored in remote servers, analysing data streams at the edge, and tracing data flows across distributed architectures.

A study conducted in 2018 by, [1] explore the topic of cybersecurity and deterrence within IoT environments, focusing on strategies to prevent cyberattacks, particularly those orchestrated by nation-states. They highlight the key differences between cyber weapons and conventional military tools, delving into the motivations that drive cyber operations. Additionally, the authors assess the effectiveness of various deterrence strategies. While their research does not specifically address IoT forensics, it lays the foundation for understanding the broader cybersecurity landscape, which is vital for contextualizing the unique challenges faced in IoT environments. [11] provide a comprehensive survey of the challenges and methodologies in IoT forensics, emphasizing critical areas such as the establishment of data inclusion and exclusion criteria, the automation of forensic processes, and the integration of forensic capabilities into device design referred to as "forensics by design." Their research also addresses the usability of forensic tools, the complexities involved in shutting down IoT devices for analysis, the implications of service level agreements (SLAs) on data access, and the privacy risks associated with encryption and anti-forensics techniques. This study is essential for understanding the intricate landscape of IoT forensics and the various obstacles that practitioners encounter in their investigations.

In a separate investigation, [12] explored the field of ethical hacking and penetration testing, highlighting the advantages of using low-cost, portable hardware such as the Raspberry Pi. The authors provide a thorough overview of ethical hacking, covering essential definitions, techniques, and the practical application of various tools, particularly using a Raspberry Pi for tasks like reconnaissance and remote penetration testing. By integrating theoretical insights and hands-on practices, This study is a valuable resource for understanding how portable devices can enhance cybersecurity efforts and forensic investigations. In their 2022 study, [13] investigated the vulnerabilities using a Raspberry Pi 4 running Raspberry Pi OS to simulate attacks using Kali Linux and various automated tools. Their research reveals significant security concerns inherent to IoT devices, emphasising the critical need for robust security measures to prevent potential exploitation. The methodology outlined in their work provides a comprehensive discussion of the practical challenges faced in securing IoT environments, highlighting the complexities involved in protecting these devices from cyber threats.

[14] investigated the creation of a low-cost, portable digital forensic imaging tool using a Raspberry Pi. The primary objective of their research was to develop an affordable imaging solution capable of effectively collecting and analysing digital evidence. This work is especially significant to IoT forensics, where the need for cost-effective tools is critical due to the extensive variety and prevalence of IoT

 doi:10.20944/preprints202501.0203.v3

devices in various environments. in [15] and [16], researchers conducted an evaluation and comparison of two open-source intrusion detection systems (IDSs) operating on a Raspberry Pi 2 (Model B). The primary objective of their research is to assess the suitability of these systems for deployment in cost-sensitive network environments [17]. This investigation holds significant importance for IoT forensics, emphasising the need for effective intrusion detection mechanisms in resource-constrained scenarios where affordable hardware plays a crucial role.

The research conducted by [18] examined the security vulnerabilities found in two commercial drones, utilising the Raspberry Pi as an automated tool for their analysis. This study not only highlights the significant security weaknesses inherent in these drones but also demonstrates the potential for exploiting such vulnerabilities. By shedding light on these risks, the research contributes valuable insights to the broader field of IoT forensics by emphasizing the dangers associated with the increasing integration of IoT devices across various sectors. A summary of related work, aspects covered, and techniques used are captured in Table 1.

Table 1. Summary of related works.

Reference	Year	IoT	Digital Forensics	Offensive Security	Technique & Approach
[1]	2018	✗	✔	✗	Evaluation and proposal for strategies to deter cyber attacks, particularly those initiated by nation-states. Differences between Cyber and Conventional Weapons, motivation and objectives of cyber operations, deterrence methods (evaluation and effectiveness)
[11]	2020	✔	✔	✔	Surveying challenges, approaches, and open issues in the field of IoT forensic, research broadly highlighted differences and similarities between mobile and IoT forensic, and tackled forensic by design and digital forensic as a service (DFaaS).
[12]	2018	✔	✗	✔	Comprehensive overview of ethical hacking practices, emphasizing the use of low-cost, portable hardware like the Raspberry Pi. Define Ethical Hacking, penetration testing, reconnaissance techniques, and remote penetration testing with the RPI combining theoretical and practical aspects.
[13]	2022	✔	✔	✗	The article focuses on demonstrating the vulnerability of IoT devices using a Raspberry Pi 4 with Raspberry Pi OS. Attacks with Kali Linux and automated tools are employed highlighting the security concerns associated with IoT devices. The methodology of executing the attacks is discussed emphasising the importance of securing IoT devices to prevent exploitation.
[14]	2021	✔	✗	✔	The paper focuses on developing a low-cost, and portable digital forensic imaging tool using the RPI. The goal is to create an image that can be used and analysed as reliable evidence.
[16]	2015	✔	✔	✗	Focus on evaluating and comparing the performance, efficiency, and efficacy of two open-source intrusion detection systems (IDSs) running in the Raspberry Pi 2 (Model B). Aim to determine their suitability for use in cost-sensitive network environments.
[18]	2019	✔	✔	✗	Identify and exploit vulnerabilities in two commercial drones. Aim to demonstrate the security weakness present in these drones by using the Raspberry Pi as an automated tool to interact with the drones.

The literature identifies a notable gap in comparative studies of forensic processes between Raspberry Pi and traditional PCs. While many studies focus on specific aspects of IoT forensics, there is a lack of research that directly compares the forensic capabilities and challenges of these two platforms. The literature also highlights ongoing debates regarding the effectiveness of various forensic tools and methodologies when applied to IoT devices [19].

2.1. Comparison with Existing Research

The increasing weaponization of IoT devices presents significant challenges for digital forensics, necessitating focused research on forensic methodologies tailored for these emerging threats. While existing studies explore broad conceptual frameworks for IoT forensics, this study contributes by

 doi:10.20944/preprints202501.0203.v3

providing a targeted forensic analysis of an easily configurable attack system using a Raspberry Pi with Kali Linux. Previous research has emphasised the complexities of IoT forensics due to the diverse architectures, communication protocols, and storage limitations of IoT devices [11]. However, there remains a gap in practical forensic methodologies that address specific attack scenarios involving low-cost, readily available hardware like the Raspberry Pi. This study bridges that gap by examining the forensic implications of Raspberry Pi-based IoT attacks and comparing forensic evidence collected from both a Raspberry Pi and a traditional PC. Unlike prior studies that primarily focus on ethical hacking and penetration testing using Raspberry Pi [12], this research takes a forensic approach by analysing digital artefacts left behind after simulated attacks. Furthermore, while research by [13] explored security vulnerabilities in IoT devices using Raspberry Pi and Kali Linux, their study focused on attack execution rather than forensic investigation. In contrast, this research contributes directly to the field of IoT forensics by evaluating the evidential value of Raspberry Pi artefacts and identifying forensic challenges in data retrieval, log analysis, and network forensics. Moreover, existing literature has discussed the forensic challenges posed by IoT environments, such as limited storage, lack of standardisation, and the volatility of IoT data [3]. While studies have highlighted the importance of forensic-by-design principles [20], there remains a lack of empirical research demonstrating practical forensic techniques for IoT devices configured for malicious purposes. This study looks at the differences between Raspberry Pi devices and traditional PCs in terms of forensic evidence collection. It highlights important differences and suggests best practices to tackle challenges in analysing Internet of Things (IoT) devices. Additionally, while [19], acknowledged the role of forensics in IoT applications, their study focused on a generalised investigation model without detailed analysis of specific IoT hardware. Similarly, research by [21], discussed forensic methodologies for Raspberry Pi but did not compare the forensic artefacts with traditional computing devices. This study builds upon their findings by providing a structured forensic approach tailored to IoT-based attacks, reinforcing the necessity for specialised forensic tools and methodologies. As a result of highlighting the forensic implications of weaponised IoT devices, this study enhances the existing body of knowledge and serves as a practical guide for forensic investigators. It identifies critical gaps in evidence collection, highlights limitations in existing forensic tools, and proposes recommendations for improving IoT forensics, including the need for live memory analysis techniques and specialised forensic frameworks for IoT environments.

2.2. TABLE I: Summary of Related Works

Table I presents a structured summary of existing research on IoT forensics, cybersecurity, and offensive security techniques, effectively outlining key studies and their methodologies. This table shows the forensic methods used in each study and points out their main limitations and gaps. This, in turn, aids in elucidating the similarities and differences between this research and previous studies. Organising the studies according to their main topics—like IoT security weaknesses, forensic methods, and offensive security—makes them easier to read and allows for better comparisons. An additional column directly contrasting the scope of previous studies with the methodology applied in this research further emphasize the study's unique contributions. These refinements enhance the clarity and depth of the comparative analysis, making it more informative for forensic investigators and researchers.

3. Methodology

The rise of Internet of Things (IoT) devices has introduced significant challenges to traditional forensic investigations, which are often tailored to conventional computing environments. This study addresses these challenges by creating a testbed that simulates environments where conventional PCs and IoT devices, like the Raspberry Pi, coexist. By simulating various cyber-attacks and analysing data such as network traffic, memory dumps, and system logs, the research compares forensic processes between these platforms. The findings highlight the strengths and limitations of existing forensic tools in IoT environments, emphasizing the need for specialized approaches for IoT forensics.

 doi:10.20944/preprints202501.0203.v3

Algorithm 1 *Forensic Analysis on Linux OS Using FTK and UFED.*

Initialisation: Pre-Forensic Preparation Tasks (write-blocking, acquisition and analysis tools (FTK, UFED)).

Step 1: Evidence Acquisition

1. Create a forensic image of the target Linux OS:
   - Use FTK Imager to create disk images (E01, RAW/DD).
   - Hash the image using MD5/SHA-256 for integrity.
2. Acquire volatile memory (if applicable):
   - Use LiME (Linux Memory Extractor) for RAM capture.
   - Validate memory dump integrity using hashing.

Step 2: File System Analysis

1. Load the forensic image in FTK.
2. Identify file system type (Ext4, XFS, Btrfs).
3. Recover deleted files using FTK's file signature analysis.
4. Extract system logs from `/var/log`:
   - Analyze `auth.log`, `syslog`, and `bash_history`.

Step 3: Network and Communication Analysis

1. Extract network logs using Wireshark and FTK:
   - Capture packet data (`.pcap` files).
   - Identify unauthorized SSH, VPN, or FTP connections.
2. Analyze user credentials:
   - Extract `/etc/passwd`, `/etc/shadow` for user details.

Step 4: Mobile & IoT Device Data Extraction

1. Use UFED to analyse connected Linux-based mobile/IoT devices.
2. Extract application logs (WhatsApp, Telegram, emails).
3. Analyze timestamps and metadata.

Step 5: Reporting and Case Documentation

1. Generate a forensic report in FTK:
   - Include extracted logs, timestamps, file hashes.
   - Validate findings by cross-verifying with original data.
2. Export the report in a legally admissible format (PDF, CSV).

3.1. Testbed Design

The forensic investigation in this study required a meticulously designed testbed to evaluate and compare forensic processes between conventional computers and IoT devices. The testbed included both a traditional PC and a Raspberry Pi, configured to simulate a real-world environment where these devices coexist. The PC used was an Acer Aspire V5, equipped with 8GB RAM and a 120GB SSD, running Kali Linux 2023.3. The Raspberry Pi 5, representing the IoT device, featured 5GB RAM and a 32GB SD card, also running Kali Linux 2023.3. Both devices were connected to a common Wi-Fi network using a Nokia HA-140W-B router. To generate relevant forensic data, four distinct cyber-attack scenarios were simulated on both the PC and the Raspberry Pi. These attacks included Windows 7 – EternalBlue, PowerShell-Empire, Windows 10 – Multi/Handler with Msfvenom payload, and Koadic Framework. Network traffic during these attacks was captured using Wireshark, ensuring comprehensive data for forensic analysis. Figure 2 depicts the key components and processes of Tested design and implementation.

 doi:10.20944/preprints202501.0203.v3

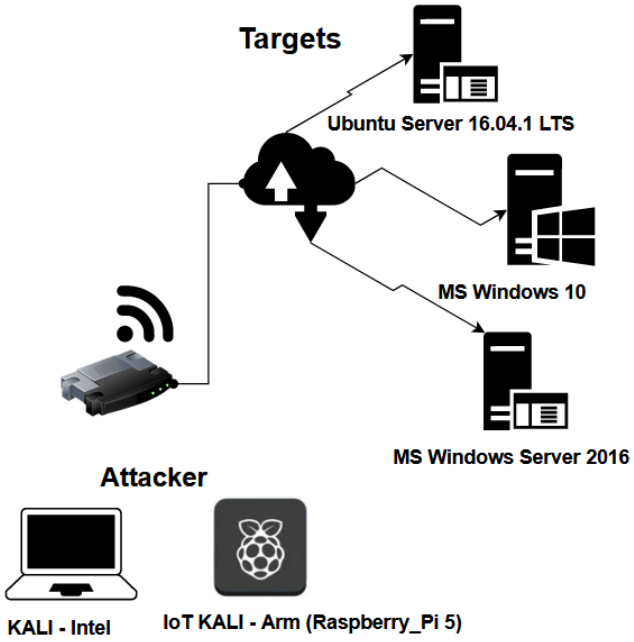

Figure 2. Test Bed Design and Implementation.

3.2. Experimental Setup and Comparative Analysis

We compared traditional PCs and Raspberry Pi devices to show the differences in their forensic abilities, such as which tools they can use, how they keep data, memory testing, and log retrieval. This evaluation offers clear insights into the challenges and benefits of forensic investigations in various computing settings, promoting a more careful and data-based method as illustrated in Algorithm 1.

3.3. Dataset Elaboration

Various types of data were collected from both devices during the simulations to ensure a thorough forensic investigation. Network traffic data, including all incoming and outgoing packets, was captured and saved in pcap format for later analysis. Memory dumps were obtained using LiME (Linux Memory Extractor) for the Raspberry Pi and Microsoft AVML for the PC. These memory dumps were crucial for analysing the processes and system states during the attacks.

Additionally, system logs, such as event, application, and security logs, were collected from both devices to provide context to the network traffic and memory data. File system snapshots were also taken before and after the attack simulations, allowing for the identification of any changes made by the attackers.

3.4. Data Capturing

The forensic data capturing process involved both forensic imaging and live RAM dumps. FTK Imager was used to create forensic images of the PC's hard drive and the Raspberry Pi's SD card, providing a complete snapshot of the data at the time of acquisition. For live data capture, RAM dumps were obtained using LiME for the Raspberry Pi and Microsoft AVML for the PC. These RAM dumps were essential for analysing active processes and volatile data, which would otherwise be lost once the device was powered off. The collected data, which included system logs, memory dumps, and network traffic data, was then thoroughly analysed to identify traces of the simulated attacks.

3.5. Comparative Forensics Analysis

We conducted a thorough investigation to compare the forensic susceptibility of a standard personal computer (PC) and a Raspberry Pi (RPI). The comparative analysis aims to assess the forensics capabilities enabled by each device and how the data could be extracted and analysed in case of a forensic investigation. The focus was on several key areas, namely:

 doi:10.20944/preprints202501.0203.v3

- **Tool compatibility:** The comparative forensic analysis highlighted several significant differences and challenges between conventional computers and IoT devices. Traditional PCs demonstrated high compatibility with most forensic tools, which facilitated a more robust forensic investigation. On the other hand, some of the forensics do not widely support the Raspberry Pi's ARM architecture, leading to significant limitations in its analysis.
- **Data Retention:** Data retention also varied, with PCs retaining extensive logs and system data, allowing for a detailed forensic investigation. The Raspberry Pi, however, had limited storage and logging capabilities, which resulted in fewer retrievable forensic artefacts and challenges in performing thorough analyses.
- **Memory Analysis:** Memory analysis was another area where differences were evident. While memory analysis on PCs was effective, with tools like Volatility providing detailed data from memory dumps, the Raspberry Pi's architecture and limited tool support made this process much more challenging, if not impossible.
- **network traffic analysis:** Network traffic analysis was consistent across both devices, with Wireshark effectively capturing relevant data. However, the contextual information provided by logs and memory analysis was more detailed for the PC, offering a more comprehensive view of the attacks.
- **system log analysis:** System log analysis further underscored the differences, with PCs offering comprehensive and detailed logs that enabled deeper forensic examinations. In contrast, the Raspberry Pi provided limited logs, restricting the scope of analysis.
- **file system snapshots:** Finally. While PCs allowed for detailed file system snapshots before and after the attacks, revealing significant changes, the Raspberry Pi's limited storage capacity resulted in fewer detectable changes, further constraining forensic analysis.

The discussion below evaluates these differences in different categories of forensic artefacts, highlighting their implications in forensic investigations. Table 2 summarises the comparative forensics analysis.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 February 2025 doi:10.20944/preprints202501.0203.v3

Table 2. Comparative Forensics Analysis Highlighting main Similarities and Differences.

Category	Forensics Artefacts	PC Machine	Raspberry Pi 5
Disk Partitions	Root Swap /boot) EFI System Partition (ESP)	FAT32 Ext4 Linux Swap Unpartitioned space dev/pts, dev/shm	FAT32 Ext4 **Not available** **Not available** **Not available**
MBR/UEFI, Grub, initrd/initramfs	boot/grub etc/grub etc/default/grub etc/initramsfs-tools	grub.cfg grub.d conf.d, hooks initramfs.conf modules scripts update-intramfs.conf	**Not available** grub.d conf.d, hooks initramfs.conf modules scripts update-intramfs.conf
File System	boot/efi var/log	boot.efi boot.log dpkg.log installer	**Not available** boot.log dpkg.log **Not available**
Systemd, Boot/shutdown	usr/lib/system etc/systemd	systemd GRUB Bootloader	systemd GRUB Bootloader
Installed Softwares and Tools	var/log/messages var/log/syslog var/log/journal	/var/log/apt/history.log /usr/local/bin system.journal user-1000journal	**Not available** /usr/local/bin system.journal user-1000journal
Log Files and System Journal	var/lib/NetworkManager Trusted Platform Module (TPM)	Wlan0 /etc/tcsd.conf /var/lib/tpm/ /etc/wpa_supplicant.conf	Wlan0 /etc/tcsd.conf **Not available** **Not available**
Cache, Swap and persistent data	System Cache Swap File Persistent Data	.cache/ mkswap/swapfile swapon/swapfiler /dev/sdX3 /lib/live/mount/persistence	.cache/ mkswap/swapfile **Not available** **Not available** **Not available**
Application Logging	var/lib/powershell empire/empire/client multi/handler root/.msf4/history Koadic	empire_client.log serverlogmulti multi/handler ms17(eternalblue) implant/manage/download_file	empire_client.log serverlog multi/handler **Not available** **Not available**
Volatile and Live Memory	Volatility RAM Linux Memory Extractor(LiME) /proc/meminfo	/mem_dump.raw /etc/fstab /proc/kcore /path/to/swap_dump.raw	/mem_dump.raw /etc/fstab **Not available** **Not available**

3.5.1. DisPartitions of the File System

The structure of the file system on a device will, to a large degree, define how forensic analysis is done by determining where and how data is stored, accessed, and managed. The PC machine running Kali Linux offers wider support for multiple partition types, such as FAT32, Ext4, Linux Swap, and unpartitioned space, which enhance flexibility in data storage and system configuration. Furthermore, **dev/pts** and **dev/shm** partitions create temporary storage for the session and temporary data that is quite handy in the capture of ephemeral artefacts. By contrast, the Raspberry Pi 5 only supports FAT32 and ext4 partitions. This greatly constrains its functionality in regard to swap memory and unpartitioned space due to a lack of Linux Swap, dev/pts, and dev/shm partitions, which makes the Raspberry Pi very limited with respect to how it manages memory. It therefore offers less capability to capture artefacts related to temporary storage or session information. Thus, the forensic investigators who would research or analyze a Raspberry Pi 5 would have fewer artefacts to consider compared to what is available on a PC and hence are very likely to miss some key transient data that may reside in swapped or shared memory areas.

3.5.2. MRBF/EFI/Config/Initramfs Files

Understanding boot and configuration files may be needed in the course of the startup process and system configuration, as both might reveal tampering or malicious configurations. Grub.cfg, grub.d, conf.d, hooks, modules, update-initramfs.conf among others, on the PC provided a very

 doi:10.20944/preprints202501.0203.v3

important record of the events of the boot and configuration process that would assist the investigator in reconstructing the system's boot sequence.

However, the main configuration file that is responsible for defining the behaviour of the bootloader in a grub.cfg is not present on Raspberry Pi 5, limiting forensic insight into the process of the boot. The rest of the configuration files, hooks, modules, and update initramfs.conf exist. However, without grub.cfg, it is impossible for forensic analysts to reconstruct or analyze the activity of the bootloader. This difference is critical in cases where evidence of bootloader modification which is a common tactic among attackers required as essential to a forensic investigation.

3.5.3. File System: Boot/EFI Logs

Other significant differences are the boot and EFI logs that one can find. On a PC, logs such as efi, boot.log, and dpkg.log summarize the process of booting up and package handling, hence giving the investigator an overview of the system changes and possible tampering.

However, the Raspberry Pi 5 does not provide efi and installer logs, and the investigator can use only boot.log and dpkg.log. This diminishes the level of detail concerning the boot process, and some critical logs may be missed that could indicate unauthorized changes or suspicious activities. Moreover, since most of the systems have no efi logs, the forensic analyst loses the ability to track some issues related to firmware or hardware-level tampering, which may be needed in the case of some new sophisticated cyber-attacks.

3.5.4. Systemd Boot/Shutdown

Both systems use /usr/lib/systemd and /etc/systemd for storing Systemd records of boots and shutdowns, respectively. Therefore, no significant difference exists between these systems in regard to this area. This homogeneity ensures that comparable records of boot and shutdown processes are equally available to the investigator on either device, thus reinforcing system start-up and shutdown behaviour auditing on either device or platform. This is one of the limited spaces where the forensic artefact landscape is still equivalent across both systems.

3.5.5. Comparative Forensics Analysis Highlighting Main Similarities and Differences

Table II presents a comparative analysis of forensic artefacts between traditional PCs and Raspberry Pi devices, highlighting their similarities and differences. The table effectively illustrates how forensic investigations differ across these platforms, particularly in terms of tool compatibility, data retention, and memory analysis. The table provides valuable insights into the forensic challenges posed by Raspberry Pi, and as a result of the insight, we have further discussion of alternative forensic approaches, such as leveraging Edge and Cloud forensic artefacts, to strengthen the findings.

3.5.6. Installed Software and System Logbook

The installed software and system journal provide insight into the applications running on a system and their respective activities. Both systems do have system.journal and user-1000.journal files, important in capturing logs of user activities and events within the system. On the other hand, it should be noticed that both the PC and the Raspberry Pi 5 do not contain any var/log/messages or var/log/syslog, which might be a limitation to forensic visibility with respect to low-level system messages and error logs.

This similarity emphasizes one of the weaknesses of the default logging configuration in Kali Linux for both platforms, whereby important system messages are not captured by the traditional logs. In an investigation, this may mean losing critical error reports, system warnings, or security notices that usually flood these logs.

3.5.7. Network Log Files

Network logs are some of the most critical logs as far as tracking device connectivity for the purpose of forensic investigation and the determination of possible points of compromise. Below are

 doi:10.20944/preprints202501.0203.v3

the entries recorded in the Network Manager log file of the PC, reflecting some records of target devices along with network interface activity, for example, Wlan0. In the case of the Raspberry Pi 5, it also contains Wlan0. however, an extra secret_key entry is present that was missing in the PC. This unique log artefact on the Raspberry Pi 5 can hint at particular security settings or authentications, adding an extra network dimension of artefacts that could be relevant within some sorts of investigations.

The presence of the secret_key entry on the Raspberry Pi 5 may raise some questions regarding network configuration security, while its absence on the PC shows a difference in processing by each device of authentication logs. This, for an investigator, points to the need for knowledge of the specific platform when examining network activity across dissimilar devices.

3.5.8. Cache, Swap, and Persisted Data

The Cache and swap spaces play a big role in forensic analysis, as generally, residual data is left behind. Although both devices record Wlan0 and some network-related records, the Raspberry Pi 5 adds the secret_key entry. This Raspberry Pi reduces the vulnerable storage that could retain useful data, such as unsaved documents or network credentials since the swapping space is not available in it.

This little swap memory will contain the investigations that can be carried out on the Raspberry Pi, especially if the evidence has to be examined with respect to user activity or unsaved session data. Whereas in PC, swap memory may capture transient data and is an extended set of forensic artefacts.

3.5.9. Other Applications Logging

Both platforms use the same application logs for most default cybersecurity applications, empire_client.log, server.log, and MS17(eternalblue). For forensic investigators, this consistency of application logs presents advantages in allowing consistent analysis of the same application-level artefacts across devices.

3.5.10. Volatile Memory (RAM)

Live memory analysis is crucial for capturing volatile data; however, it's only supported on the PC, which allows complete RAM analysis with tools like Volatility. Due to the architecture of Raspberry Pi 5, it doesn't support Volatility, thusly live memory analysis isn't possible. This has really proved a deep handicap because most live memory images usually contain, in real-time, operating processes, encryption keys, and session information which is very valuable during forensic investigation. Without this capability on the Raspberry Pi, forensic investigators may miss volatile artefacts critical to understanding real-time system behaviour.

4. Research Findings and Discussion

4.1. Key Differences Between PC and Raspberry Pi

Our investigation revealed significant differences between the PC and the Raspberry Pi in terms of forensic capabilities. The PC demonstrated a tendency to retain extensive logs, system data, and processes, facilitating a detailed forensic analysis. This is in stark contrast to the Raspberry Pi, which, due to its limited logging capability and smaller storage capacity, offered fewer forensic artefacts, thus limiting the depth of analysis. One of the most critical areas of difference was memory analysis. While acquiring and analysing AM images from a Windows-based PC was straightforward and provided rich data, the process was significantly more complex with Linux-based systems and IoT devices like the Raspberry Pi. The lack of tool compatibility with the RPI's ARM architecture posed a significant challenge, making it difficult to perform comprehensive forensic analysis.

Table 3 summarizes the differences in forensic capabilities between the PC and Raspberry Pi:

 doi:10.20944/preprints202501.0203.v3

Table 3. Summary of the Overall Forensics Investigation Differences.

Aspect	PC	Raspberry Pi
Tool Compatibility	High - Most tools work effectively	Low - Many tools face compatibility issues
Data Retention	Extensive logs and system data	Limited logs and storage capacity
Memory Analysis	Effective with rich data from memory dumps	Challenging due to tool configuration issues
Network Traffic Analysis	Detailed and consistent analysis	Similar results but less contextual data
System Log Analysis	Comprehensive and detailed	Limited and less detailed
File System Snapshots	Detailed snapshots before and after attacks	Limited changes detected due to small storage
Overall Forensic Capability	High - Robust forensic analysis possible	Low - Significant limitations in forensic analysis

Additionally, a detailed analysis of the file system and other artefacts on both devices further highlighted these differences. Starting with the file system, the PC features multiple partitions, including FAT32, ext4, and Linux Swap, along with unpartitioned space and various directories such as /dev/pts and /dev/shm. In contrast, the RPI5's file system is more limited, comprising only two partitions (FAT32 and ext4) and lacking additional directories and unpartitioned space. This distinction suggests that the PC has a more complex and detailed file system structure, which may offer more artefacts for forensic analysis.

When examining boot processes, the PC demonstrates detailed boot configuration files, including grub.cfg, various grub.d scripts, and configurations for initramfs. The RPI5, however, shows limited support in this area, with many boot-related files not available. This limitation in the RPI5 indicates potential challenges in performing comprehensive forensic investigations related to the boot process.

In terms of system services and scheduling, both devices utilize systemd for boot and service management, suggesting a common approach in handling these functions despite potential differences in implementation details. However, the PC's extensive logging capabilities, including directories like /var/log/messages and /var/log/syslog, contrast with the RPI5's reliance on a journal system (system.journal, user-1000journal). This disparity highlights the PC's superior capacity for retaining detailed logs, which are crucial for forensic analysis.

Log files and system journals further emphasize the differences, with the PC offering comprehensive logs, including those related to network management. The RPI5's logs are more focused on network interfaces, such as Wlan0, and lack the breadth found in the PC. This limitation restricts the depth of forensic analysis that can be performed on the RPI5.

When it comes to application logs, both devices capture logs related to various attack tools like PowerShell Empire, multi/handler, and Koadic. However, the specific logs and their availability differ between the platforms, indicating that while both devices can log similar types of activities, the details and accessibility of these logs vary.

Live memory analysis presents a significant challenge for the RPI5, as the Volatility tool does not support its architecture, making live memory analysis difficult or impossible. In contrast, the PC supports live memory analysis with tools like Volatility, providing detailed insights into the system's state during forensic investigations. This difference underscores the PC's advantage in forensic memory analysis.

Finally, network traffic analysis is consistent across both devices, with tools like Wireshark effectively capturing relevant data. However, the contextual information provided by logs and memory analysis is more detailed for the PC, offering a more comprehensive view of the attacks. The

 doi:10.20944/preprints202501.0203.v3

differences in system log analysis further highlight the PC's capability of offering detailed forensic examinations, while the RPI5's limited logs restrict the scope of analysis.

4.2. Comparative Forensic Performance Evaluation

The forensic investigation revealed notable differences in forensic capabilities between traditional PCs and Raspberry Pi devices. To systematically evaluate these differences, a comparative analysis was conducted based on key forensic performance indicators, including tool compatibility, data retention, memory analysis, and file system snapshots.To quantify these differences, forensic artefact retrieval efficiency was measured across platforms, as shown in ***Figure 3***. The results show that computer-based forensic investigations work much better because they can use more tools, have better system logs, and analyse memories more effectively. In contrast, Raspberry Pi devices posed challenges in tool support and log retention, limiting their forensic analysis depth. Additionally, the graphical representation in Figure 3 visually demonstrates the comparative forensic efficiency of both platforms. These findings reinforce the need for specialised forensic methodologies tailored to IoT environments. The study demonstrates that while PCs provide a robust forensic platform, Raspberry Pi devices introduce significant limitations that must be addressed through alternative forensic strategies, such as Edge and Cloud forensics.

4.3. Summary of the Overall Forensics Investigation Difference

Table III effectively consolidates the key findings from the forensic investigation, summarising the differences in forensic capabilities between traditional PCs and Raspberry Pi devices. The table provides a clear, high-level comparison. One of the critical aspects requiring additional discussion is live memory analysis, where Raspberry Pi lacks tool support, severely limiting forensic capabilities. Alternative solutions, such as capturing memory artefacts through external logging mechanisms or Edge forensic methods, should be explored to address this limitation. We emphasise the practical implications of these differences in forensic investigations, especially regarding evidence collection, data retention, and forensic readiness as illustrated in Figure 3. A case study or real-world example demonstrating how these forensic challenges manifest in practice would further strengthen the discussion.

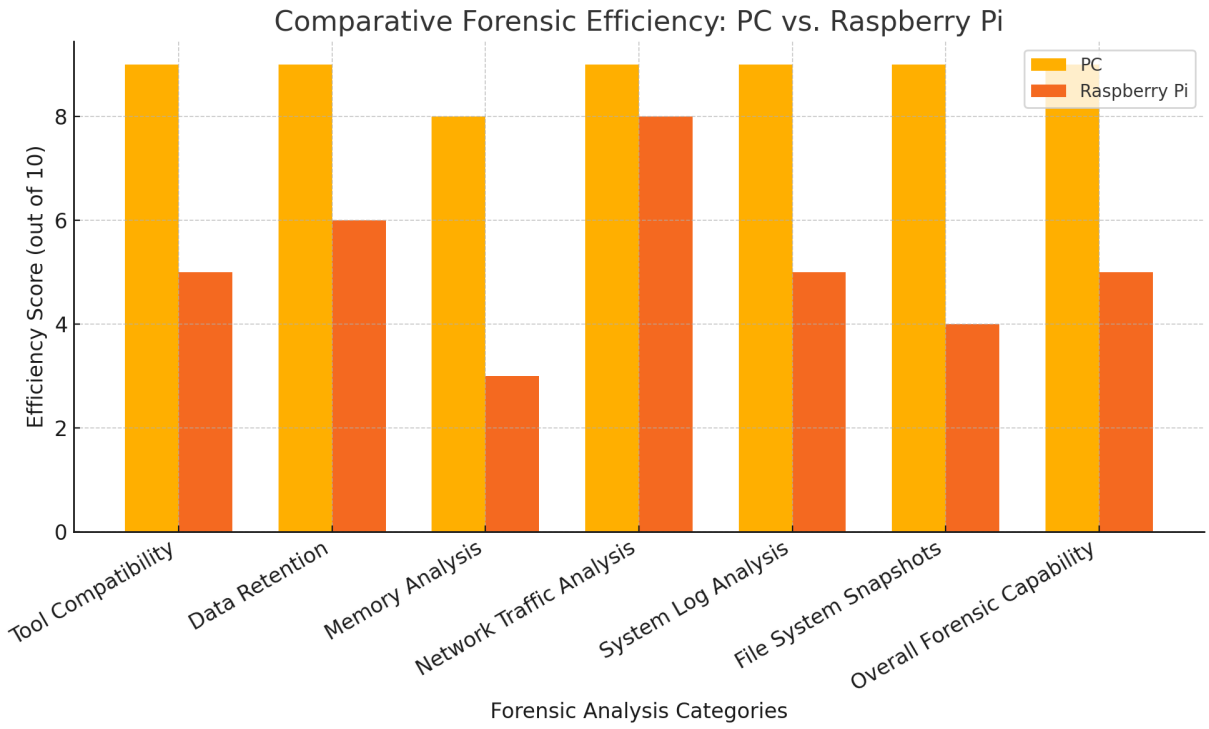

Figure 3. Comparative Forensic Performances Evaluation

 doi:10.20944/preprints202501.0203.v3

4.4. Challenges with Raspberry Pi

The current forensic examination of hacker-oriented systems, using a traditional PC running Kali Linux and a Raspberry Pi 5, affords an unparalleled opportunity to assess how forensic artefacts will change across platforms with distinct hardware architectures and functionalities. Kali Linux remains the favourite choice for cybercriminals and current trends show an important shift towards the use of SBC such as Raspberry which the Cyber Forensics community is not ready yet to cope with this shift is marked by differences in both the level and type of forensic data available due to their base design, hardware, and software composition.

The most significant challenge encountered during this investigation was related to the analysis of RAM in the context of Raspberry Pi when compared to Desktop PC where acquiring RAM images was a relatively straightforward process. However, when dealing with Raspberry Pi and IoT devices in general, the process became more complex. We tested fourteen different tools to analyse Linux evidence, and only two, **Rekall** and **Volatility**, could handle Linux images. Unfortunately, Rekall has not been updated since November 2017, rendering it less effective in producing reliable results. Volatility, on the other hand, encounters issues with Linux symbols, requiring the creation of a symbol table using **Dwarf2Jason** for each Linux version. This process is problematic because the tool does not keep up with the frequent updates of the Linux operating system, limiting its applicability depending on the version in use. For the Raspberry Pi, the challenge was even more pronounced. The Volatility tool does not support the ARM architecture embedded in the Raspberry Pi, making it impossible to analyse live memory from the device. This limitation severely restricts the ability to perform comprehensive forensic analysis on the Raspberry Pi, highlighting a critical gap in the available forensic tools for IoT devices.

4.5. Edge and Fog forensic issues

The forensic challenges associated with IoT devices extend beyond the local device itself and often involve Edge and Fog computing environments. Edge computing enables local processing and storage closer to IoT devices [22], reducing latency and improving efficiency. However, it also presents unique forensic challenges, such as data volatility, decentralised storage, and limited access to logs. Similarly, Fog computing involves a distributed approach where intermediate nodes process and store data before it reaches the cloud. This introduces additional layers of complexity for forensic investigations, including jurisdictional issues and the need for specialised tools to extract and analyse evidence from these intermediary layers. These infrastructures can retain crucial forensic artefacts even when the IoT devices themselves are volatile, offering potential avenues for evidence collection in forensic investigations.

4.6. Addressing Research Questions

For **RQ1**, the forensic procedures vary considerably between traditional PCs and IoT devices such as Raspberry Pi because of the differences in their hardware designs, operating systems, and data storage capacities. Traditional computers, which usually have stronger hardware and storage capabilities, enable thorough forensic examination utilising a wide variety of tools and procedures [21]. Their logging techniques are comprehensive, facilitating the tracking of user actions and system operations. On the other hand, Raspberry Pi devices present difficulties in forensic investigations because of their simplified designs (ARCH architecture) and restricted storage capacity. A significant number of forensic tools do not have compatibility with IoT devices, and the data stored is often inadequate for doing thorough analysis. Acquiring live memory from IoT devices is a more intricate and less dependable operation compared to traditional PCs.

For **RQ2**, the significant distinctions in terms of forensic artefacts difference between traditional PCs and Raspberry Pi devices are due to the Data Storage Capacity and hardware architecture. Traditional computers have a greater capacity to store data and maintain more comprehensive records of user actions and system operations. This encompasses comprehensive system logs, application logs,

 doi:10.20944/preprints202501.0203.v3

and user-generated data, which are essential for forensic investigations. PCs use logging practices that employ strong systems to capture extensive information about system and network operations. Internet of Things (IoT) devices, such as Raspberry Pi, sometimes possess restricted logging capabilities, leading to a reduced quantity and quality of artefacts. Conventional computers have a far higher capability for doing live memory analysis compared to other devices. Volatility Plugins are capable of extracting intricate information about active processes and system conditions from memory dumps. However, IoT devices have difficulties when it comes to memory analysis because of compatibility concerns with forensic tools.

For **RQ3**, the current challenges and limitations in weaponized IoT forensics include:

- Tool Compatibility: Many existing forensic tools are not compatible with the diverse architectures and operating systems used by IoT devices, such as the ARCH architecture in Raspberry Pi.
- Data Retention and Storage: IoT devices typically have limited storage capacity and simplified logging mechanisms, which result in insufficient forensic data retention.
- Live Memory Analysis: Acquiring and analysing live memory from IoT devices is challenging due to tool incompatibility and the technical complexity of configuring existing tools for different architectures.

In summary, traditional PCs provided a robust platform for forensic investigations, offering extensive data retention and tool compatibility. In contrast, IoT devices like the Raspberry Pi posed significant challenges due to limited tool support, reduced data retention, and restricted memory analysis capabilities. These findings underscore the need for the development of specialised forensic tools and methodologies tailored to the unique characteristics of IoT devices to enhance their forensic investigation potential.

5. Conclusions and Future Works

This study provides a focused examination of IoT forensic processes, specifically an analysis of a Raspberry Pi configured for cyberattacks. Unlike traditional forensic investigations that apply well-established methodologies to conventional computing devices, IoT forensics presents unique challenges, including resource constraints, limited logging, and reliance on network connections. To address these complexities, this research introduces a tailored forensic methodology and offers a real-world case study demonstrating its application. The findings serve as a valuable resource for forensic investigators by providing a structured approach to analysing IoT-based attacks.

A comparative analysis of forensic capabilities between traditional PCs and Raspberry Pi devices reveals significant differences, particularly in data retention, logging, and tool compatibility. While PCs offer extensive logging capabilities and support for a broad range of forensic tools, Raspberry Pi devices are hindered by limited storage, incomplete boot files, and a lack of compatibility with essential forensic tools such as Volatility, which restrict live memory analysis. Although the Raspberry Pi's simplicity and flexibility make it a useful platform for targeted forensic investigations, these constraints highlight the need for more advanced forensic tools tailored to IoT environments.This research extends previous studies on IoT forensics by providing a practical case study that bridges the gap between theoretical frameworks and real-world forensic investigations. While earlier research has explored ethical hacking and penetration testing on Raspberry Pi [12], and security vulnerabilities in IoT devices [13], this study uniquely focuses on forensic methodologies for analysing compromised IoT devices. Furthermore, unlike prior studies that broadly discuss IoT forensic challenges [11]; [20], this research presents a structured forensic approach tailored specifically to Raspberry Pi-based attacks. As a result of offering a direct comparison between forensic investigations on PCs and IoT devices, this study highlights critical gaps in existing forensic capabilities and emphasises the urgent need for specialised forensic tools for IoT and Cloud environments [10].

Additionally, while both the PC and the Raspberry Pi, running Kali Linux, provide forensic artefacts, the PC emerges as a more robust forensic platform due to its comprehensive configuration options and greater forensic readiness. This study contributes to the growing field of IoT forensics by

 doi:10.20944/preprints202501.0203.v3

not only identifying key limitations in forensic investigations of IoT-based attacks but also proposing practical methodologies that can be utilised by forensic practitioners in future investigations. We have expanded the experimental setup to include multiple attack scenarios, further validating the forensic methodologies used in this research. These simulations explore different forensic issues that come up when analysing Linux-based hacker machines, helping to support the results with actual forensic investigations. As a result of demonstrating forensic tool performance under different conditions, the study offers practical and reproducible results that strengthen its scientific contribution.

Funding: This research received no external funding.

Institutional Review Board Statement: This research was deemed as not requiring the University's Ethical Committee Approval as it doesn't fall under any of the cases requiring ethical approval.

Data Availability Statement: Disks' Forensics Images and Volatile data generated for this research are available upon request.

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

References

1. Wanic, E. and Rowe, N. (2018). Assessing Deterrence Optinos for Cyber Weapons. in 2018 International Conference on Computational Science and Computational Intelligence (CSCI), pp. 13–18. ttps://doi.org/10.1109/CSCI46756.2018.00011.
2. Kebande, V.R., 2022. Industrial Internet of Things (IIoT) forensics: The forgotten concept in the race towards industry 4.0. Forensic Science International: Reports, 5, p.100257. https://doi.org/10.1016/j.fsir.2022.100257.
3. Mazhar, M.S., Saleem, Y., Almogren, A., Arshad, J., Jaffery, M.H., Rehman, A.U., Shafiq, M. and Hamam, H., 2022. Forensic analysis on Internet of Things (IoT) device using machine-to-machine (M2M) framework. Electronics, 11(7), p.1126. https://doi.org/10.3390/electronics11071126.
4. Y. Salem, M. Owda and A. Y. Owda. A Comprehensive Review of Digital Forensics Frameworks for Internet of Things (IoT) Devices. 2023 International Conference on Information Technology (ICIT), Amman, Jordan, 2023, pp. 89-96. https://doi.org/10.1109/ICIT58056.2023.10226145.
5. Dunsin, D., Ghanem, M.C., Ouazzane, K. and Vassilev, V., 2024. A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response. Forensic Science International: Digital Investigation, 48, p.301675. https://doi.org/10.1016/j.fsidi.2023.301675.
6. Nelufule, N., Singano, T., Masemola, K., Shadung, D., Nkwe, B., Mokoena, J.2024. An Adaptive Digital Forensic Framework for the Evolving Digital Landscape in Industry 4.0 and 5.0, 2024 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), pp.1686-1693, 2024. https://doi.org/10.1109/IDCIoT59759.2024.10467482
7. Dunsin, D., Ghanem, M.C., Ouazzane, K. and Vassilev, V., 2025. Reinforcement learning for an efficient and effective malware investigation during cyber Incident response. High-Confidence Computing, p.100299. https://doi.org/10.1016/j.hcc.2025.100299.
8. Ghanem, M.C., Mulvihill, P., Ouazzane, K., Djemai, R. and Dunsin, D., 2023. D2WFP: a novel protocol for forensically identifying, extracting, and analysing deep and dark web browsing activities. Journal of Cybersecurity and Privacy, 3(4), pp.808-829. https://doi.org/10.3390/jcp3040036.
9. T. Bakhshi. Forensic of Things: Revisiting Digital Forensic Investigations in Internet of Things. 2019 4th International Conference on Emerging Trends in Engineering, Sciences and Technology (ICEEST), Karachi, Pakistan, 2019, pp. 1-8, https://doi.org/10.1109/ICEEST48626.2019.8981675.
10. Farzaan, M.A.M., Ghanem, M.C., El-Hajjar, A. and Ratnayake, D.N., 2024. AI-Enabled System for Efficient and Effective Cyber Incident Detection and Response in Cloud Environments.https://arxiv.org/abs/2404.05602.
11. Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E. and Markakis, E.K., 2020. A survey on the Internet of Things (IoT) forensics: challenges, approaches, and open issues. IEEE Communications Surveys & Tutorials, 22(2), pp.1191-1221. https://doi.org/10.1109/COMST.2019.2962586.
12. Yevdokymenko, M., Mohamed, E. and Onwuakpa, P. (2017) 'Ethical hacking and penetration testing using Raspberry PI', in 2017 4th International Scientific-Practical Conference Problems of Info-communications. Science and Technology (PIC S&T), pp. 179–181. https://doi.org/10.1109/INFOCOMMST.2017.8246375.

13. Mohd Bakry, B. B., Bt Adenan, A. R. and Mohd Yussoff, Y. B. (2022) 'Security Attack on IoT RelatedDevices Using Raspberry Pi and Kali Linux', in 2022 International Conference on Computer and Drone Applications (IConDA), pp. 40–45. https://doi.org/10.1109/ICONDA56696.2022.10000370.
14. Yudha, F., Ramadhani, E. and Komaryan, R. M. (2021) 'A Prototype of Portable Digital Forensics Imaging Tools using Raspberry Device', IOP Conference Series: Materials Science and Engineering, 1077(1), p. 012064. https://doi.org/10.1088/1757-899X/1077/1/012064.
15. Cusack, B., Tian, Z. and Kyaw, A.K., 2017. Identifying DOS and DDOS attack origin: IP traceback methods comparison and evaluation for IoT. In Interoperability, Safety and Security in IoT: Second International Conference, InterIoT 2016 and Third International Conference, SaSeIoT 2016, Paris, France, October 26-27, 2016, (pp. 127-138).https://doi.org/10.1007/978-3-319-52727-7
16. Kyaw, A. K., Chen, Y. and Joseph, J. (2015) 'Pi-IDS: evaluation of open-source intrusion detection systems on Raspberry Pi 2', in 2015 Second International Conference on Information Security and Cyber Forensics (InfoSec). Cape Town: IEEE, pp. 165–170. https://doi.org/10.1109/InfoSec.2015.7435523.
17. Ghanem, M.C., Chen, T.M., Ferrag, M.A. and Kettouche, M.E., 2023. ESASCF: expertise extraction, generalization and reply framework for optimized automation of network security compliance. IEEE Access, 11, pp.129840-129853.https://doi.org/10.1109/ACCESS.2023.3332834.
18. Westerlund, O. and Asif, R. (2019) 'Drone Hacking with Raspberry-Pi 3 and WiFi Pineapple: Security and Privacy Threats for the Internet-of-Things', in 2019 1st International Conference on Unmanned Vehicle Systems-Oman (UVS). Muscat, Oman: IEEE, pp. 1–10. https://doi.org/10.1109/UVS.2019.8658279.
19. Alam M. N. and Kabir, M. S. Forensics in the Internet of Things: Application Specific Investigation Model, Challenges and Future Directions, 2023. 4th International Conference for Emerging Technology (INCET), Belgaum, India, 2023, pp. 1-6. https://doi.org/10.1109/INCET57972.2023.10170607.
20. Torabi, S., Bou-Harb, E., Assi, C. and Debbabi, M., 2020. A scalable platform for enabling the forensic investigation of exploited IoT devices and their generated unsolicited activities. Forensic Science International: Digital Investigation, 32, p.300922. https://doi.org/10.1016/j.fsidi.2020.300922.
21. Ho, S.M. and Burmester, M. (2021). Cyber Forensics on Internet of Things: Slicing and Dicing Raspberry Pi. International Journal of Cyber Forensics and Advanced Threat Investigations, 2(1). pp.29–49. https://doi.org/10.46386/ijcfati.v2i1.22.
22. Premsankar, G., Di Francesco, M. and Taleb, T., 2018. Edge computing for the Internet of Things: A case study. IEEE Internet of Things Journal, 5(2), pp.1275-1284. https://ieeexplore.ieee.org/abstract/document/8289317.
23. Cook, M., Marnerides, A., Johnson, C. and Pezaros, D., 2023. A survey on industrial control system digital forensics: challenges, advances and future directions. IEEE Communications Surveys & Tutorials. https://doi.org/10.1109/COMST.2023.3264680.
24. Case, A. and Richard III, G.G., 2017. Memory forensics: The path forward. Digital investigation, 20, pp.23-33. https://doi.org/10.1016/j.diin.2016.12.004.