International Journal of Computer Engineering in Research Trends
ISSN: 2349-7084/ https://doi.org/10.22362/ijcert/2024/v11/i11/v11i1101
Volume 11, Issue 11, November 2024

Review Paper

Pegasus Spyware: Omar Radi Critical Review

[1*]J Scott

[1] Executive Director, Milad Group, LLC, United States.*

Email id: jonathanbscott@proton.me

Received:11/07/2024 Revised: 27/10/2024 Accepted:20/11/2024 Published:30/11/2024

Abstract: This research critically examines the forensic methodologies employed by Amnesty International and The Citizen Lab in their analysis of NSO Group's Pegasus spyware, with a particular focus on the high-profile case of Moroccan journalist Omar Radi. Despite claims of scientific rigor, significant methodological flaws are evident, including reliance on speculative forensic indicators, the generation of false positives, and the absence of independent peer review. These shortcomings undermine the validity of the findings and raise concerns about their transparency, particularly in politically sensitive cases. Technical inconsistencies, such as the reliance on ambiguous data artifacts like browsing history and process executions, highlight failures to meet established standards for transparency, reproducibility, and accountability. The study also identifies systemic issues related to overlapping personnel between Amnesty International and The Citizen Lab, which compromise the independence of these investigations. These issues are compounded by the lack of rigor in evidence handling, exemplified by Amnesty's quiet retraction of false positives without formal updates to their published findings. Such practices not only diminish the credibility of the conclusions but also risk misrepresenting critical evidence in cases with far-reaching implications. By uncovering these flaws, this research underscores the urgent need for more robust and scientifically validated methodologies in spyware detection. Emphasis is placed on the importance of adopting peer-reviewed practices that prioritize accuracy, reproducibility, and impartiality. Ultimately, the findings contribute to a broader discourse on the critical role of methodological rigor and transparency in digital forensics, particularly when addressing issues with profound implications for human rights and state accountability.

Keywords: Pegasus Spyware, Human Rights Surveillance, Cyber Espionage, Mobile Forensics, Digital Surveillance Tools, Mobile Forensics Methodology, NSO Group, Mobile Surveillance Software, Omar Radi Spyware, Morocco Spyware

1 Introduction

Digital forensics has become an essential tool for investigating cyber threats, particularly in the context of sophisticated surveillance technology like Pegasus, developed by Israeli firm NSO Group. Pegasus is one of the most advanced mobile surveillance tools ever developed, enabling remote infiltration of mobile devices without any interaction from the user, often through zero-click exploits. This software is capable of compromising smartphones to access sensitive data such as messages, emails, microphones, and cameras. Given the nature of Pegasus, its detection and attribution have significant implications for privacy, human rights, and state surveillance. Organizations like Amnesty International and The Citizen Lab have developed forensic methodologies to detect Pegasus infections, which they have applied in high-profile cases, including that of Moroccan journalist Omar Radi [1][2]. However, these methodologies have faced substantial criticism for their lack of scientific rigor, transparency, and the potential for generating false positives.

One of the central challenges in forensic detection of Pegasus is the difficulty in distinguishing legitimate system processes from those initiated by the spyware. Many forensic tools rely on speculative evidence and assumptions about the behavior of mobile devices, which can lead to inaccurate conclusions. Amnesty International's report on the Omar Radi case, for example, claimed to have detected Pegasus using forensic indicators such as suspicious Safari browsing data and abnormal process executions [3]. However, these findings are questioned for lacking sufficient verification and independent peer review. The reliance on speculative forensic artifacts has raised concerns about the integrity and reliability of such conclusions, particularly when used in politically sensitive cases like that of Omar Radi.

This paper critically evaluates Amnesty International's forensic methodology, with a specific focus on the Pegasus detection claims in the case of Omar Radi. By examining the technical details of the forensic processes, this study identifies the limitations of current detection techniques, particularly in their handling of ambiguous data and their failure to rule out false positives.

The key contributions of this paper are as follows:

1. An in-depth critique of Amnesty International's forensic framework, identifying the reliance on

speculative processes and the lack of transparency in their approach.
2. Assessing the likelihood of false positives generated by forensic indicators, especially in the Omar Radi case, where inconclusive evidence was presented as definitive proof.
3. The broader implications of inaccurate forensic reporting are explored, particularly in relation to how these findings can shape international narratives on state surveillance and human rights.
4. Emphasis on the need for greater scientific rigor, transparency, and independent validation of results.

This research builds upon a growing body of work in mobile forensics and spyware detection. While previous forensic methodologies have focused on identifying spyware through trace data analysis, this paper critically examines the limitations of these approaches. By analyzing the Omar Radi case and the forensic claims made by Amnesty International, this research aims to highlight the importance of adhering to more scientifically rigorous standards in forensic investigation, emphasizing transparency, reproducibility, and accuracy in future spyware detection efforts.

This paper is structured as follows: In Section II, we explore the historical development of surveillance technology detection, discussing the evolution of methodologies used to identify advanced surveillance tools and the challenges posed by modern surveillance technologies. Section III outlines the methodology used in this study, detailing the approach taken to critically analyze the forensic processes applied to detect Pegasus in the Omar Radi case. Section IV delves into method results highlighting concerns over false positives, and reproducibility. Finally, Section V summarizes the key findings and emphasizes the need for greater scientific rigor and transparency in the development of forensic methodologies for detecting surveillance technologies.

This research addresses the critical need scientifically sound forensic methodologies in the context of mobile surveillance technology (ST) detection, providing a foundation for improving the reliability of forensic investigations in political cases. For the remainder of this paper, the term "ST" will be used to refer to surveillance technology rather than "spyware," as the latter carries an implicit negative connotation. It is important to acknowledge that Pegasus software is a legitimate tool designed to assist governments and law enforcement agencies in combating terrorism and other criminal activities around the world.

2 Literature Review

The rise of advanced mobile surveillance technologies (ST) has sparked a surge of research aimed at detecting and understanding these technologies. While human rights organizations like The Citizen Lab and Amnesty International have played a role in highlighting the misuse of ST by state actors, the task of accurately detecting and attributing such technologies presents ongoing challenges. This literature review examines the key historical developments in the detection of ST and the methodological challenges that arise in these efforts. Additionally, it explores the ethical considerations involved in forensic investigations, especially concerning conflicts of interest and the reproducibility of results. The sections that follow provide a closer look at the evolution of surveillance technology detection, the ethical implications of investigative methodologies, and the technical barriers that continue to complicate accurate ST detection.

2.1 Historical Development of Surveillance Technology Detection

Surveillance technologies (ST) have advanced considerably over the past few decades, becoming increasingly sophisticated in their capabilities. However, the methodologies for detecting these tools have not evolved at the same pace. In particular, the perceived threat posed by mobile espionage tools such as Pegasus has driven a surge in research among NGOs and special interest groups. Initial detection methods largely relied on the analysis of iCloud or iPhone backups, minimal network activity, DNS string matching, and process string matching—approaches that often lack a logical basis for considering these strings as malicious indicators of compromise (IOCs) [4]. These methods have struggled to keep up with the complexity of modern ST, which utilizes advanced techniques to evade detection, often leading to assumptions that are difficult to validate [5].

A range of organizations, including academic institutions, security researchers, and NGOs, have been working to enhance these detection methodologies by developing more effective tools for identifying digital traces left by ST. While their efforts are not solely focused on technical detection, they have also raised awareness of the potential human rights violations associated with the deployment of surveillance technologies. For instance, Privacy International has been a strong advocate for increased transparency and oversight of these tools, stressing the importance of addressing the ethical issues that arise from their use [6]. This advocacy has contributed to research on the ethical and civil liberties implications of ST, particularly regarding its impact on privacy rights and governmental accountability.

2.2 Ethical Considerations in Surveillance Technology Investigations

Ethical concerns surrounding the detection and reporting of surveillance technologies (ST) have become significant in the discourse on forensic methodologies. A major issue is the objectivity and transparency of investigations, particularly when the same organizations responsible for developing ST detection tools are also involved in validating and reviewing their results. This overlap raises concerns about conflicts of interest and self-referencing, which can undermine the credibility of forensic reports [7].

A pertinent example is the "Briefing note on OECD Complaints against Gamma International and Trovicor in the UK and Germany" published by Privacy International on February 3rd, 2013 [8]. This document focused on the export of surveillance technology, particularly Gamma International's FinSpy software, accusing the company of violating export regulations and facilitating human rights abuses in Bahrain. However, the transparency of these claims is questionable, as the identities of those behind the research were not scrutinized. Furthermore, the research

relied heavily on findings from The Citizen Lab, whose director, Ron Deibert, simultaneously served on the Privacy International Advisory Board [9][10]. This dual role calls into question the impartiality of the investigation.

The issue of potential bias is further complicated by the overlapping roles of key individuals in both The Citizen Lab and Amnesty International. For example, Claudio Guarnieri, a senior research fellow at The Citizen Lab, also worked as a technologist for Amnesty International's Technology group [11][12]. Additionally, Etienne Maynier, a researcher involved in the Omar Radi spyware case, held simultaneous positions at both organizations [13]. These overlapping roles, particularly under the direction of Ron Deibert at The Citizen Lab, blur the lines of independent scrutiny. Moreover, Sarah Jane Beamish, the Chair of Amnesty International's board of directors, held a professorship at the University of Toronto's Monk School, home to The Citizen Lab [14][15], and reported directly to Ron Deibert. These intricate interconnections between individuals within both organizations challenge the notion of objective and independent evaluations, particularly in sensitive cases like Omar Radi's.

The University of Toronto's principles on human ethics emphasize the necessity of avoiding conflicts of interest in research [16]. They highlight the importance of maintaining impartiality during evaluations, suggesting that reviewers must be independent and free from affiliations that could compromise the objectivity of the review process. This ethical framework underscores the need for independent peer review, which is essential to ensure that forensic investigations are scientifically credible and unbiased [17]. However, the overlapping roles within organizations like The Citizen Lab and Amnesty International violate these ethical standards, raising doubts about the objectivity of their conclusions and casting a shadow over the integrity of all their alleged forensic findings.

2.3 Methodological Challenges, NGO Resistance & Lack of Rigor.

The detection of advanced surveillance technologies (ST), such as Pegasus, presents significant methodological challenges for forensic investigators. One of the primary issues is the high likelihood of false positives—where normal system behavior is mistakenly flagged as malware-related activity [18]. The complexity of tools like Pegasus, which often leverages zero-click exploits only heightens this problem. This not only questions the effectiveness of current forensic approaches but also calls for more advanced, scientifically rigorous methodologies.

Moreover, the credibility of forensic findings heavily depends on their reproducibility, a fundamental principle in scientific research. If forensic evidence cannot be independently verified by other researchers, confidence in its conclusions is significantly undermined. Unfortunately, the detection of ST's often suffers from a lack of transparency and reproducibility, weakening the validity of its findings. Numerous studies highlight the need for forensic tools to adhere to strict scientific standards, ensuring that conclusions drawn are not only accurate but can also be replicated in other investigations [19]. Failure to meet these standards leaves forensic evidence, particularly in politically sensitive cases, open to scrutiny.

In cases where a nation is accused of deploying ST, as in the case of Morocco, the accused has the right to review the evidence of the alleged wrongdoing. The Kingdom of Morocco faced resistance from Amnesty International when it requested proof to substantiate claims of human rights abuses. Amnesty confirmed Omar Radi's Pegasus infection a published a report June 22nd, 2020. However, when Moroccan Minister of National Education, Vocational Training, Higher Education, and Scientific Research Saaïd Amzazi demanded evidence to back these allegations, Amnesty International failed to provide any substantive response or materials [20]. This reluctance to present evidence not only raises questions about the transparency of the investigation but also undermines the credibility of Amnesty's claims.

On July 18th, 2021, Amnesty International, with what was presented as an independent peer review from The Citizen Lab, published the "Forensic Methodology Report: How to Catch NSO Group's Pegasus" [3], which gained widespread recognition within the information security community. However, despite its title suggesting a systematic and scientifically grounded approach, the report leaned heavily on speculative claims rather than concrete forensic evidence. Statements like "Amnesty International believes," "we discovered suspected," and "suspicious processes" were prevalent throughout the report. Despite these ambiguities, the report was widely accepted as an authoritative source, without undergoing true independent peer review by the broader security community. Critics who questioned or challenged the findings were often unfairly dismissed and labeled as conspiracy theorists or frauds, effectively stifling valid critique and raising concerns about the impartiality of the involved organizations. This response, however, triggered a Streisand effect, prompting more researchers globally to scrutinize the methods used to detect Pegasus and question the validity of the forensic techniques employed.

Table 1 Summary Table of Key Literature

Paper	Key Contributions	Limitations
Maratsi, M. I., Popov, O., Alexopoulos, C., & Charalabidis, Y. (2022) [7]	Explored the ethical and legal aspects of digital forensics algorithms, focusing on challenges in digital evidence acquisition.	Does not delve deeply into technical solutions for overcoming ethical dilemmas in algorithm design for digital forensics.
Sunde, N. (2022) [17]	Discussed strategies to safeguard examiner objectivity and ensure the reliability of	Does not address specific technical methods for ensuring reliability across diverse forensic tools and environments.

	digital forensic evidence.	
Kim & Lee (2020) [18]	Presented methodologies for managing and identifying potential evidence in Android forensics to improve investigative accuracy.	Limited focus on non-Android platforms; does not address broader mobile forensics issues, particularly with cross-platform investigations.
Hughes & Karabiyik (2020) [19]	Emphasized the importance of using measurement science to improve reliability and objectivity in digital forensics.	Some methodologies are still in development and may not yet be applicable to all forensic contexts or accepted by all scientific communities.

2.4 Research Gaps

From the review of existing literature, several research gaps have been identified:

1. **Lack of Transparent and Reproducible Methodologies:** The forensic methodologies developed by organizations like Amnesty International and The Citizen Lab have been widely adopted, but they often lack transparency and reproducibility. Independent verification of findings is crucial in forensic investigations, especially in politically sensitive cases. However, current methodologies have been criticized for relying on speculative evidence and a lack of scientific rigor, leaving substantial room for improvement in ensuring that these methods can be replicated and validated by external researchers.
2. **Challenges with False Positives in Forensic Detection:** One of the primary challenges identified in the literature is the high likelihood of false positives, where benign system behavior is interpreted as malicious. This issue is particularly pronounced in the detection of sophisticated surveillance tools like Pegasus, which use advanced zero-click exploits that leave minimal traces. Current detection methods often fail to distinguish between normal system activities and spyware-related processes, leading to inaccurate results. More research is needed to develop forensic tools that minimize false positives while maintaining high sensitivity in detecting advanced ST.
3. **Ethical Concerns and Conflicts of Interest:** There is a notable gap in addressing the ethical concerns surrounding the involvement of individuals with overlapping roles in the development, validation, and review of forensic methodologies. The interconnected relationships between key personnel at The Citizen Lab and Amnesty International raise concerns about conflicts of interest, self-referencing, and the impartiality of forensic findings. Further research is needed to develop ethical guidelines and frameworks that ensure objectivity in ST detection and reporting.
4. **Inadequate Peer Review and Independent Scrutiny:** Many of the forensic reports published by NGOs have not been subjected to robust peer review by the broader scientific and security communities. The acceptance of these reports as authoritative without independent scrutiny undermines their credibility. This gap highlights the need for more open-source forensic tools and methodologies that can be critically examined, tested, and validated by the information security community.
5. **Handling of Politically Sensitive Cases:** The reluctance of organizations like Amnesty International to provide substantiating evidence in politically sensitive cases, such as the Omar Radi investigation, exposes a gap in how forensic evidence is handled and shared. There is a need for standardized protocols that ensure transparency and accountability in the presentation of forensic evidence, particularly when accusations of human rights violations are involved. Addressing this gap would help prevent accusations of bias and enhance the credibility of forensic findings in such cases.

In summary, while some progress has been made in the detection of surveillance technologies, there are significant gaps in the transparency, reproducibility, and ethical governance of these methodologies. Addressing these gaps is essential to ensure that future forensic investigations are scientifically robust, ethically sound, and capable of withstanding independent scrutiny.

3 Methodology

Despite the increasing reliance on forensic methodologies by non-governmental organizations and special interest groups such as Amnesty International and The Citizen Lab to detect advanced surveillance technologies like Pegasus, these approaches have faced substantial criticism for their lack of scientific rigor, transparency, and reproducibility. The overlapping roles of key individuals between the investigative bodies, coupled with the use of speculative forensic indicators, have raised concerns about the validity of their findings. In politically sensitive cases like that of Moroccan journalist Omar Radi, these methodological flaws have significant implications for the integrity of the evidence and the broader international narrative on state surveillance and human rights. This research problem seeks to address the gaps in current forensic practices, exploring how a lack of scientific scrutiny, transparency, and reproducibility can lead to false positives, compromising the credibility of critical human rights investigations.

3.1 Amnesty Forensics Methodology Emphasis

Amnesty International's mobile forensics methodology report consists of 17 sections, including subsections, and

upon thorough examination, several key aspects of the methodology became strikingly apparent.

Table 2 Amnesty Forensics Methodology [3]

1	Discovering Pegasus network injection attacks	9	Unravelling the Pegasus attack infrastructure over the years
2	Pegasus' BridgeHead and other malicious processes appear	9.1	Further attempts by NSO Group to hide their infrastructure
2.1	Additional suspicious processes following BridgeHead	9.2	Identifying other NSO attack domains
3	Pegasus processes following potential Apple Photos exploitation	9.3	What can be learned from NSO Group's infrastructure
4	An iMessage zero-click 0day used widely in 2019	9.4	Attack infrastructure hosted primarily in Europe and North America
5	Apple Music leveraged to deliver Pegasus in 2020	9.5	Infection domain resolutions observed in Passive DNS database
6	Megalodon: iMessage zero-click 0-days return in 2021	10	Mobile devices, security and auditability
7	Incomplete attempts to hide evidence of compromise	11	With our Methodology, we release our tools and indicators
8	Pegasus processes disguised as iOS system services		

1. Contrary to initial expectations, the content presented in the report does not focus on a comprehensive methodology but instead appears to target a specific country, namely the Kingdom of Morocco.
2. Of the 17 sections in the forensic methodology report, approximately 52.9% directly address or reference a Moroccan case, making allegations of espionage by Morocco a significant part of the document.

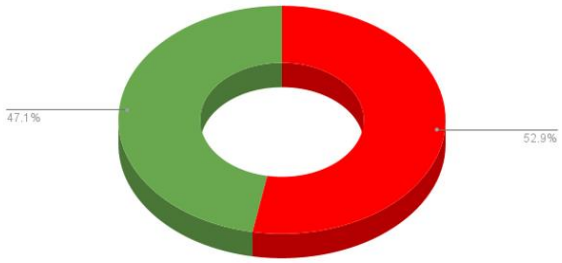

Fig 1. 52.9% of Methodology Focusing on Morocco

9 of 17 sections

3. Four out of the 17 sections are dedicated solely to the alleged espionage case involving Omar Radi, making it the most prominently featured individual case in the report, comprising approximately 23.5% of the content.

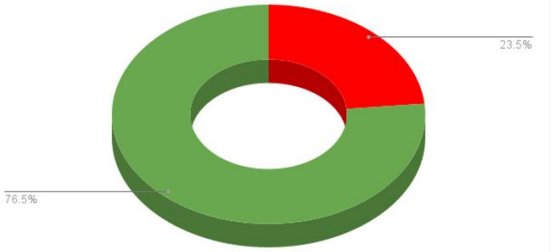

Fig 2. 23% of Methodology Focusing on Omar Radi

4 of 17 sections

4. Upon the initial release of the Methodology Report, 100% of the "forensic traces" presented in Appendix B and Appendix C were exclusively from Moroccan civil society members, despite the report explicitly stating that confirmed infections had also occurred in countries such as France, India, Rwanda, UAE, Hungary, and Azerbaijan

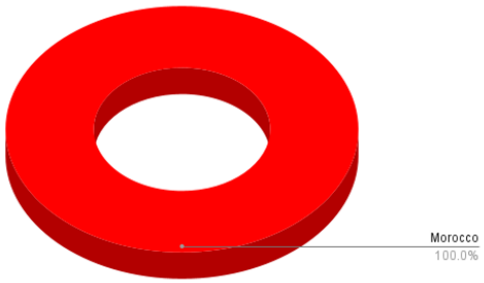

Fig 3. 100% of the forensic traces detailed in Appendix B and C were from Morocco, despite claims that individuals from six other countries were also infected with Pegasus. Only Maati Monjib and Omar Radi were specifically listed in these appendices [21].

When comparing Amnesty International's forensic methodology report to a comprehensive mobile forensics response, such as the one developed by ENISA [22], the shortcomings of the former become even more evident. ENISA's methodology adheres to established industry practices, offering detailed technical guidance on identifying and addressing malicious threats. ENISA's approach emphasizes a clear definition of scope and objectives, ensuring that investigations are focused and systematic. It provides structured guidelines for identifying relevant devices, operating systems, and types of evidence to examine. In contrast, Amnesty International's report lacks a comprehensive scope, focusing heavily on specific cases in Morocco without establishing clear boundaries for its investigation. This narrow focus reduces the report's general applicability as a forensic methodology.

Moreover, ENISA highlights the importance of preparation, including setting up a secure forensic environment and adhering to strict evidence handling procedures to maintain integrity and admissibility in legal proceedings. Amnesty International's report, however, does not specify the protocols or procedures followed for evidence preservation, raising questions about the reliability and credibility of its findings. ENISA also promotes a systematic approach to data acquisition, analysis, and interpretation, providing specific steps and techniques for extracting and analyzing evidence using a variety of forensic tools. In contrast, Amnesty International's report lacks a structured framework for data acquisition and analysis. Instead, it relies heavily on anecdotal evidence from cases like Omar Radi's, without offering a reproducible methodology that can be applied across different scenarios. This absence of a rigorous, systematic approach undermines the reliability and objectivity of Amnesty's findings.

3.2 Amnesty Forensics Methodology: Section 1

Direct Quote Assertions [3]:

1. In our October 2019 report, we detail how we determined these redirections to be the result of network injection attacks performed either through tactical devices, such as rogue cell towers, or through dedicated equipment placed at the mobile operator. When months later we analyzed the iPhone of Moroccan independent journalist Omar Radi, who as documented in our 2020 report was targeted, we found similar records involving the free247downloads.com domain as well.
2. Although Safari history records are typically short lived and are lost after a few months (as well as potentially intentionally purged by malware), we have been able to nevertheless find NSO Group's infection domains in other databases of Omar Radi's phone that did not appear in Safari's History. For example, we could identify visits through Safari's Favicon.db database, which was left intact by Pegasus.
3. Similarly, on a different occasion Omar Radi visited the website of French newspaper Le Parisien, and a network injection redirected him through the staging domain tahmilmilafate[.]com and then eventually to free247downloads[.]com as well. We also saw tahmilmilafate[.]info used in the same way.

Section 1 Factual Conclusions:

1. Amnesty International speculates about the method of infection on Omar Radi's phone, making unsubstantiated claims regarding a network injection attack. They suggest the potential use of tools like rogue cell towers or specialized equipment at the mobile operator. Additionally, they reference domains such as free247download.com and an unrelated URL, urlpush.net, as part of the infection process, but fail to provide concrete evidence supporting the existence of a network injection attack. Their primary justification is that "while the timing is suggestive of a link to NSO, the technical details, including both sites redirecting to the same website and showing several matching execution and forensic artifacts, provide strong evidence linking NSO Group's tools to the targeted attack on Omar Radi [30]."
2. The primary function of the favicon.db database is to store information related to website icons (favicons), rather than maintaining a comprehensive record of browsing history or visited sites. It only contains a limited selection of websites that have associated favicons, and it operates separately from Safari's browsing history.

Since the data within favicon.db can be modified or altered, its reliability and accuracy as a forensic artifact are questionable. Furthermore, if a website was accessed in private browsing mode, there would be no record of it in either the favicon.db database or Safari's browsing history.

3. Amnesty uses the term "network injection attack" to describe what is essentially a man-in-the-middle (MITM) attack. According to Amnesty's own figure [36] they state it depicts "the network injection attack on Omar's phone observed while he was visiting a website in clear text (HTTP and not HTTPS)." Amnesty alleges that Radi visited the website leparisien.fr, but historical data shows that the site was already secured with HTTPS during the 2019-2020 period when Radi supposedly accessed it. Furthermore, Amnesty implies that Radi accessed an unsecured version of leparisien.fr, but does not clarify whether he did so by clicking on a link or manually entering the HTTP address.

Amnesty's reliance on *suspicious redirects* recorded in Safari's browsing history as evidence of network injection attacks is questionable. Odd-looking URLs and non-standard port numbers alone are insufficient to conclusively prove NSO Group's involvement or the presence of malicious activity. Furthermore, the inclusion of domains like free247downloads.com and urlpush.net does not inherently implicate NSO Group or establish a definitive connection to Pegasus. The mere appearance of these domains in Safari's browsing history or other databases does not constitute adequate evidence to support Amnesty's allegations. The absence of clear documentation detailing their analysis methodology further raises doubts about the accuracy and reliability of their findings. Moreover, relying on Safari history and app-specific data as indicators of compromise has its limitations. Amnesty International assumes these records provide conclusive proof of network injection attacks, overlooking other possible factors such as benign website redirects, network anomalies, adware or tracking scripts, browser caching issues, and misconfigurations in the browser itself. Additionally, routine server-side updates or temporary access to non-standard ports could also result in unusual browsing activity [40]. Attributing these incidents solely to NSO Group based on this data is speculative and lacks robust evidence. Amnesty's has a history of releasing reports that are largely self-referential and fail to provide independent corroboration, thereby undermining the credibility of their conclusions.

3.2 Amnesty Forensics Methodology: Section 2

Section 2 outlines eight assertions that attempt to establish a link between a 2016 report by Lookout [23] and the presence of a process named "bh" in an iPhone backup. Each of these claims, taken directly from Amnesty's methodology report, is documented with corresponding reference numbers. This section holds particular importance within the findings related to Omar Radi, as these results often serve as the foundation for attributing Pegasus infections to individuals worldwide. The accuracy and credibility of these assertions are crucial in shaping the overall narrative and determining the potential consequences of Pegasus-related incidents.

Section 2 Direct Quote Assertions [3]:

1. iOS maintains records of process executions and their respective network usage in two SQLite database files called "DataUsage.sqlite" and "netusage.sqlite" which are stored on the device. It is worth noting that while the former is available in iTunes backup, the latter is not. Additionally, it should be noted that only processes that performed network activity will appear in these databases.
2. Both Maati Monjib's and Omar Radi's network usage databases contained records of a suspicious process called "bh". This "bh" process was observed on multiple occasions immediately following visits to Pegasus Installation domains.
3. Crucially, we find references to "bh" in the Pegasus iOS sample recovered from the 2016 attacks against UAE human rights defender Ahmed Mansoor, discovered by Citizen Lab and analyzed in depth by cybersecurity firm Lookout.
4. As described in Lookout's analysis, in 2016 NSO Group leveraged a vulnerability in the iOS JavaScriptCore Binary (jsc) to achieve code execution on the device. This same vulnerability was also used to maintain persistence on the device after reboot. We find references to "bh" throughout the exploit code.
5. bh.c – Loads API functions that relate to the decompression of next stage payloads and their proper placement on the victim's iPhone by using functions such as BZ2_bzDecompress, chmod, and malloc"
6. Lookout further explains that a configuration file located at /var/tmp/jb_cfg is dropped alongside the binary. Interestingly, we find the path to this file exported as _kBridgeHeadConfigurationFilePath in the libaudio.dylib file part of the Pegasus bundle.
7. Therefore, we suspect that "bh" might stand for "BridgeHead", which is likely the internal name assigned by NSO Group to this component of their toolkit.
8. The appearance of the "bh" process right after the successful network injection of Omar Radi's phone is consistent with the evident purpose of the BridgeHead module. It completes the browser

exploitation, roots the device and prepares for its infection with the full Pegasus suite.

Section 2 Factual Conclusions:

1. Amnesty's approach has significant limitations when used as forensic evidence. The exclusion of the "netusage.sqlite" file from iTunes backups means that a complete picture of network usage is unavailable, potentially omitting crucial data. Additionally, relying solely on process data from the "DataUsage.sqlite" file is problematic, as it only captures processes that interacted with the network. This leaves out numerous processes that could still be relevant in a forensic context but did not perform network activity. For example, system-level processes related to local storage access or background data handling, such as managing contacts or local file indexing, would not be captured in this database, despite their potential relevance in a forensic investigation. This selective logging reduces the reliability of the evidence, and therefore, the findings based on these databases should not be considered conclusive or comprehensive in a forensic investigation.
2. The presence of a process named "bh" immediately following visits to alleged Pegasus installation domains does not necessarily imply a direct causal link to Pegasus. Other factors, such as coincidental naming or unrelated system activities, could explain the appearance of this process, and its presence alone is not sufficient evidence to establish Pegasus involvement
3. Amnesty International attempts to link CVE-2016-4657 to an alleged attack on Omar Radi that occurred between 2019 and 2020. Their discovery of the "bh" process in an iPhone backup has led them to speculate that it may be part of another exploit chain. However, CVE-2016-4657 [24], which affects WebKit in Apple iOS versions prior to 9.3.5, would require that Omar Radi's phone had not been updated for three years in order for this vulnerability to be exploited. This raises significant questions regarding the timeline and whether this particular vulnerability could realistically have been used in an attack on his device.
4. It becomes clear once again that Amnesty is relying heavily on the 2016 Lookout report titled "**Technical Analysis of the Pegasus Exploits on iOS.**" What stands out, however, is their claim of discovering references to "**bh**" within the exploit code. Amnesty asserts that this code was recovered from the 2016 attacks on UAE human rights defender Ahmed Mansoor, yet they have not made the malware sample publicly available. Additionally, while they include a code snippet in their report, Amnesty fails to clarify its exact origin, leaving it uncertain whether the snippet pertains to Omar Radi or Ahmed Mansoor, both of whom are referenced in Section 2.

```
var compressed_bh_addr =  shellcode_addr_aligned +
shellcode32.byteLength;
replacePEMagics(shellcode32, dlsym_addr, compressed_bh_addr,
bundle.bhCompressedByteLength);
storeU32Array(shellcode32, shellcode_addr);
storeU32Array(bundle.bhCompressed32, compressed_bh_addr);
```

Fig 4 . Amnesty presents this code snipped without any clear reference to where it came from.

The provided code snippet appears to be related to memory manipulation in the context of shellcode, which is often used in exploits. We can break the code down to understand the functionality.

- **compressed_bh_addr = shellcode_addr_aligned + shellcode32.byteLength;**

- This line calculates an address (compressed_bh_addr) in memory by adding the length of the shellcode32 array to the shellcode_addr_aligned. The new address will point to the location where the compressed "bh" code will be stored.

- **replacePEMagics(shellcode32, dlsym_addr, compressed_bh_addr, bundle.bhCompressedByteLength);**

- This function likely modifies the shellcode (shellcode32) to replace specific values (possibly placeholders or markers) with actual values, such as function addresses (dlsym_addr) or the location of the compressed "bh" code (compressed_bh_addr). "PE Magics" refers to specific bytes in Portable Executable (PE) files, which might imply this is related to tampering with executable code.

- **storeU32Array(shellcode32, shellcode_addr);**

- This function stores the shellcode32 array at the memory location shellcode_addr. The U32 suggests that it's dealing with 32-bit unsigned integers, indicating that it is working with low-level memory operations.

- **storeU32Array(bundle.bhCompressed32, compressed_bh_addr);**

- Similarly, this line stores the compressed "bh" data (bundle.bhCompressed32) at the calculated address compressed_bh_addr.

The biggest concern within this code includes a function call to replacePEMagics. "PE" refers to Portable

Executable, a file format used in **Windows operating systems for executables**, DLLs, and similar objects. iOS, however, does not use the PE format. **iOS apps and binaries are packaged using the Mach-O format**. This difference suggests that the code was written with a different operating system (likely Windows) in mind, and the term "PEMagics" would be out of place in an iOS exploit.

5. Amnesty once again references Lookout's 2016 report, mentioning "bh.c" in an attempt to establish a connection between the "bh" process found in the iPhone backup and the malware detected in 2016. However, a closer look at the Lookout report reveals that Lookout suspects "bh.c" to be part of a larger modular exploit system that generates a stage 2 binary. Furthermore, when Amnesty cites Lookout, stating, "*bh.c - Loads API functions related to decompressing subsequent stage payloads and positioning them on the victim's iPhone using functions such as BZ2_bzDecompress, chmod, and malloc*," it contradicts Amnesty's earlier claim. This is because functions like "BZ2_bzDecompress, chmod, and malloc" **are not relevant to network usage, thereby invalidating Section 2 Assertion #2**. These functions deal with decompressing data and managing local processes rather than interacting with the network.

It was necessary to review the 2016 Lookout report, and identify the exploit referencing "bh.c." The purpose of this was to definitively conclude weather the bh.c binary executed a network function as Amnesty is claiming.

From 2016 Lookout report (pg. 37)

- **if ((unsigned int)(majorVersion - 8) >= 2)**

- This line checks if the major version of the operating system or software is greater than or equal to 10 (majorVersion - 8 >= 2). The major version must be at least 10 for the following block of code to execute.

- **if (majorVersion == 7)**

- This condition checks if the major version is specifically 7. If it is, the next block of code is executed.

- **pszJBFilenamePath = "/bin/sh";**

- If the major version is 7, this line sets the pszJBFilenamePath to the shell executable path, "/bin/sh". This indicates that it's pointing to a shell, likely preparing to execute commands or scripts.

- **if (flag) pszJBFilenamePath = "/private/var/tmp/jb-install";**

- If the variable flag is true, it overrides the previous shell path and sets pszJBFilenamePath to "/private/var/tmp/jb-install". This suggests a possible installation or jailbreak-related directory, as "jb-install" could refer to a "jailbreak install" directory.

- **else { assert(); writeLog(3, "%.2s%5.5d\n", "bh.c", 134); exit(-1); pszJBFilenamePath = 0; }}**

- If the major version is not 7, the code performs a series of actions:

- assert(): This function checks a condition (not shown in this snippet). If the condition fails, it causes the program to abort suggesting this is more of a debugging tool.

- writeLog(): This logs the string "bh.c" along with the value 134. It's likely writing to a log file or console for debugging purposes, noting something related to the "bh.c" process or file.

- exit(-1): This causes the program to terminate with an error code -1. This likely indicates a failure.

- pszJBFilenamePath = 0: The path is set to 0, nullifying any previous values. This suggests that no valid path is available in this scenario.

- **else { pszJBFilenamePath = "/sbin/mount_nfs.temp"; }**

- If the major version is less than 10 (i.e., the condition majorVersion - 8 >= 2 is false), the code sets pszJBFilenamePath to "/sbin/mount_nfs.temp". This path suggests a temporary mount for NFS (Network File System) operations, possibly related to network file mounting.

Based on the Lookout code review **bh.c** appears to be focused on modular **payload execution, not network activity**. The code provided by the lookout team sets a path for mounting network filesystems (NFS), which might have contributed to confusion. The path "/sbin/mount_nfs.temp" refers to a potential network operation related to file mounting, but this is unrelated to the core operations of bh.c. **Amnesty might have seen network-related terms like NFS and assumed a broader network role** for bh.c than is actually true.

6. Amnesty claims that the file path "/var/tmp/jb_cfg" is found in the libaudio.dylib file and links it to the Pegasus bundle, but there is no clear evidence supporting this connection. **libaudio.dylib [25] is a legitimate iOS system library for audio functionality**, and its inclusion

of this file path does not prove its association with Pegasus. The mere presence of a file path in a legitimate library does not indicate malicious intent or use during an attack. Additionally, Amnesty's reference to the "Pegasus bundle" is speculative, as no malware samples or independent verification have been provided. Without corroborating evidence, the conclusions about this bundle and the file path remain unproven, weakening the reliability of Amnesty's claims.

7. Amnesty claims that based on their earlier assertions, which are built on a 2016 exploit that is unrelated to network activity, they have concluded that the two-letter process found in a network usage table within an iPhone backup is actually named "Bridgehead." They further speculate that this is a component of the NSO Group's exploit toolkit. However, this conclusion is speculative and lacks sufficient evidence, as there is no direct connection between the process and NSO's tools, especially since the exploit they reference is unrelated to network usage.

8. The final assertion once again speculates that the presence of the "bh" process represents "Bridgehead," a component believed to be responsible for completing the device's compromise after network injection. However, as with earlier claims, Amnesty fails to provide any concrete evidence to substantiate these conclusions. There is no detailed technical analysis or verifiable data linking "bh" to the Pegasus suite or proving that it serves the purpose they claim. This assumption remains unsupported and speculative.

3.3 Amnesty Forensics Methodology: Section 2.1

Section 2.1 continues the forensic analysis by focusing on a series of processes, such as "roleaboutd" and "msgacntd", which Amnesty International claims to be key indicators of Pegasus infection. This section attempts to connect these processes to a broader exploitation chain, allegedly linked to NSO Group's toolkit. The assertions made in Section 2.1 are pivotal, as they form the basis for how Amnesty is identifying Pegasus activity on Omar Radi's device. However, the lack of clear attribution and reliance on speculative connections raises questions about the validity of these claims.

Section 2.1 Direct Quote Assertions [3]:

1. The bh process first appeared on Omar Radi's phone on 11 February 2019. This occurred 10 seconds after an IndexedDB file was created by the Pegasus Installation Server and a favicon entry was recorded by Safari. At around the same time the file com.apple.CrashReporter.plist file was written in /private/var/root/Library/Preferences/, likely to disable reporting of crash logs back to Apple. The exploit chain had obtained root permission at this stage. Less than a minute later a "roleaboutd" process first appears.

2. Omar Radi's device was exploited again on the 13 September 2019. Again a "bh" process started shortly afterwards. Around this time the com.apple.softwareupdateservicesd.plist file was modified. A "msgacntd" process was also launched.

3. Based on the timing and context of exploitation, Amnesty International believes the roleaboutd and msgacntd processes are a later stage of the Pegasus spyware which was loaded after a successful exploitation and privilege escalation with the BridgeHead payload.

4. Amnesty International verified that no legitimate binaries of the same names were distributed in recent versions of iOS. The discovery of these processes on Omar Radi's and Maati Monjib's phones later became instrumental for Amnesty International's continued investigations, as we found processes with the same names on devices of targeted individuals from around the world.

Section 2.1 Factual Conclusions:

1. Amnesty and The Citizen Lab frequently create scenarios based on assumptions of malicious intent. In this case, Amnesty claims that when Omar Radi visited a suspicious website, a file called com.apple.CrashReporter.plist was written to the directory /private/var/root/Library/Preferences/, allegedly to prevent crash logs from being sent to Apple.

   The presence of the CrashReporter.plist file in Omar Radi's iPhone backup can be explained by normal system behavior related to crash logging, specific iOS versioning, or backup processes that include system files. Amnesty International speculates that this file was placed to disable crash reporting to Apple, but provides no evidence of any modifications or tampering.

   Amnesty went further, asserting that the presence of com.apple.CrashReporter.plist in an iPhone backup indicated Pegasus infection, adding it as an indicator of compromise (IOC) to their STIX2 file. Essentially, Amnesty concluded that finding this file in the root or home domain of an iPhone backup was proof of Pegasus infection.

An iOS developer raised concerns on Amnesty's GitHub [26], explaining that simply finding Library/Preferences/com.apple.CrashReporter.plist could lead to false positives, particularly for developers working on iOS. They suggested checking the content for code modifications before marking the file as an IOC. Amnesty acknowledged the developer's concerns but stated that their MVT-Tool relies solely on manifest files and doesn't inspect the file content, despite the risk of false positives. Eventually, Amnesty recognized com.apple.CrashReporter.plist as a false positive and decided to remove it from their list of IOCs in the STIX2 file [27]. This means that if Radi's device were reanalyzed after the removal, the file would no longer be flagged as malicious, undermining Amnesty's argument.

Furthermore, Amnesty's identification of the "roleaboutd" process as malicious lacks attribution, and the timelines surrounding Radi's infection do not align with their narrative, raising additional doubts about the accuracy of their findings.

2. Amnesty's claim that the com.apple.softwareupdateservicesd.plist file was modified as part of an infection on 13 September 2019 lacks proper attribution, and they prematurely flagged it as an indicator of compromise. However, Amnesty later retracted this claim and acknowledged the file as a false positive, revealing that this is a standard property list on iOS devices and poses no security threat [28]. Interestingly, in The Citizen Lab's assessment of Amnesty's methodology, they state [29], "We have not observed Amnesty's list of 45 process names associated with any benign or legitimate apps." This raises serious concerns about how The Citizen Lab can confidently endorse Amnesty's methodology when numerous false positives have been identified, both by Amnesty themselves and by external developers.

3. Amnesty claims that the processes "roleaboutd" and "msgacntd" represent a later stage of the Pegasus spyware, supposedly triggered after successful exploitation and privilege escalation via the BridgeHead payload. However, as with many of their previous assertions, Amnesty fails to provide concrete evidence to support this claim, instead relying on speculative language like "we believe." This pattern of conjecture without substantial proof weakens their argument and suggests that these conclusions are based on assumptions rather than solid forensic evidence.

4. Amnesty International asserts that no legitimate binaries with the names "roleaboutd" and "msgacntd" were distributed in recent iOS versions—a conclusion also supported by The Citizen Lab in their purported independent peer review. However, Amnesty previously removed "Diagnosticd [30]" from their GitHub repository, labeling it a "false positive," only to later reclassify it as a true positive [31] Indicator of Compromise (IOC), after confusing it with the normal process "diagnosticd." These inconsistencies in the removal and reclassification of IOCs have contributed to the signing of resolutions against Rwanda, particularly in the case of Carine Kanimba. When "Diagnosticd" was considered a false positive, this was not disclosed to the European Union, which subsequently signed a resolution against Rwanda [32] for the alleged spying on Kanimba. After the resolution was signed, Amnesty changed "Diagnosticd" back to a true positive, but by then it was too late to influence the decision. There is no clear scientific method used to determine if these binaries are legitimate iOS processes. Therefore, Amnesty's claim that "roleaboutd" and "msgacntd" were not distributed in recent iOS versions lacks credibility, particularly given that they classified "Diagnosticd" as a false positive on July 22, 2021, just three days after publishing their forensics methodology paper.

3.4 Amnesty Forensics Methodology: Section 6

Section 6 shifts the focus to the forensic analysis of another journalist's device, referred to as CODE MOJRN1. The alleged similarities between this case and the Omar Radi case are presented as evidence of a broader pattern of Pegasus attacks. Amnesty International relies on parallels between the processes found on both devices, particularly the "msgacntd" process, to strengthen their argument for a Pegasus infection. This section plays a role in extending the scope of Amnesty's claims beyond individual cases, attempting to draw connections across multiple instances of suspected ST infections.

Section 6 Direct Quote Assertions [3]:

1. Amnesty International subsequently analyzed the iPhone of a journalist (CODE MOJRN1), which contained very similar records. This device was exploited repeatedly on numerous times between February and April 2021 and across iOS releases. The most recent attempt showed the following indicators of compromise.

2. It is worth noting that among the many other malicious process names observed executed on

this phone we see msgacntd, which we also found running on Omar Radi's phone in 2019, as documented earlier.

Section 6 Factual Conclusions:

1. Amnesty's analysis highlights the iPhone of another Moroccan journalist, identified as CODE MOJRN1, Hicham Mansouri. This is the third Moroccan journalist featured in their forensics methodology report.
2. Amnesty references the case of Omar Radi to link the alleged 2021 attacks on Hicham Mansouri to the Pegasus software, but once again fails to provide attribution for their claim that the supposed malicious process "msgacntd" was executed as part of a Pegasus event. As mentioned earlier, Amnesty mistakenly conflated a normal iOS process with a potentially malicious one, arbitrarily removing and re-adding these processes to their IOC list. This further raises doubts about their credibility in identifying malicious processes, especially since they do not disclose the methodology used to determine these binaries as malicious.

4 Result

Upon closer examination, it becomes evident that the traces, supposedly providing detailed information for each target as outlined in the section titled "Appendix C: Detailed Traces per Target," do not align with the claims made throughout Amnesty's methodology report. Additionally, Amnesty identified "com.apple.softwareupdateservicesd.plist" as a false positive just one day after publishing their forensics methodology report, and similarly found "com.apple.CrashReporter.plist" to be a false positive in certain cases three days after the report's release. Despite these findings, none of these false positives were updated in the methodology report published on July 18, 2021. Updating the report with these false positives would have undermined the validity of the entire document.

4.1 Omar Radi's Forensic Traces

In the case of Omar Radi, sections C.2 and 2.1 of the report show the same alleged malicious URLs and processes, "bh" and "roleaboutd," but with different infection times down to the second. These discrepancies undermine the credibility of the data. This is like claiming a single murder occurred at two different times, which would mislead a jury and in a forensics investigation could be considered evidence tampering. Tables 3 and 4 illustrate these conflicting IOCs and infection times for Omar Radi in different sections of Amnesty's report.

Table 3: Same IOCs Found Different Times to the Second

Time	**Section C.2**	**Time**	**Section 2.1**
Date		**Date**	
2019-02-11 13:45:53	Safari favicon from URL hxxps://d9z3sz93x5ueidq3.get1tn0w.free247downloads[.]com:30897/rdEN5YP	2019-02-11 14:45:53	Safari Favicon record for URL hxxps//d9z3sz93x5ueidq3.get1tn0w.free247downloads[.]com:30897/rdEN5YP
2019-09-13 15:01:38	Safari favicon for URL hxxps://2far1v4lv8.get1tn0w.free247downloads[.]com:31052/meunsnyse#0113565702571729683484570402233897313302433397236	2019-09-13 17:01:38	https://2far1v4lv8.get1tn0w.free247downloads[.]com:31052/meunsnyse#0113565702571729683484570402233897313302433397236
2019-09-13 15:01:56	Safari favicon for URL hxxps://2far1v4lv8.get1tn0w.free247downloads[.]com:31052/meunsnyse#0680995616146262785199253586387891615724278336453 89	2019-09-13 17:01:56	https://2far1v4lv8.get1tn0w.free247downloads[.]com:31052/meunsnyse#0680995616146262785199253586387891615724278336453 89
2020-01-27 10:06:24	Safari favicon for URL hxxps://gnyjv1xltx.info8fvhgl3.urlpush[.]net:30875/zrnv5revj#0741964198279879192740015486227389198355567483259 46	2020-01-27 11:06:24	https://gnyjv1xltx.info8fvhgl3.urlpush[.]net:30875/zrnv5revj#0741964198279879192740015486227389198355567483259 46

Table 4: More of the Same IOCs Found Different Times to the Second

Time **Date**	**Section C.2**	**Time** **Date**	**Section 2.1**
2019-02-11 13:45:56	Process: bh	2019-02-11 14:45:56	Process: bh
2019-02-11 13:46:23	Process: roleaboutd	2019-02-11 14:46:23	Process: roleaboutd
2019-02-11 16:05:24	Process: roleaboutd	2019-02-11 17:05:24	Process: roleaboutd

Figure 5 provides a clearer example of inconsistencies in the mobile forensics data related to Omar Radi's case.

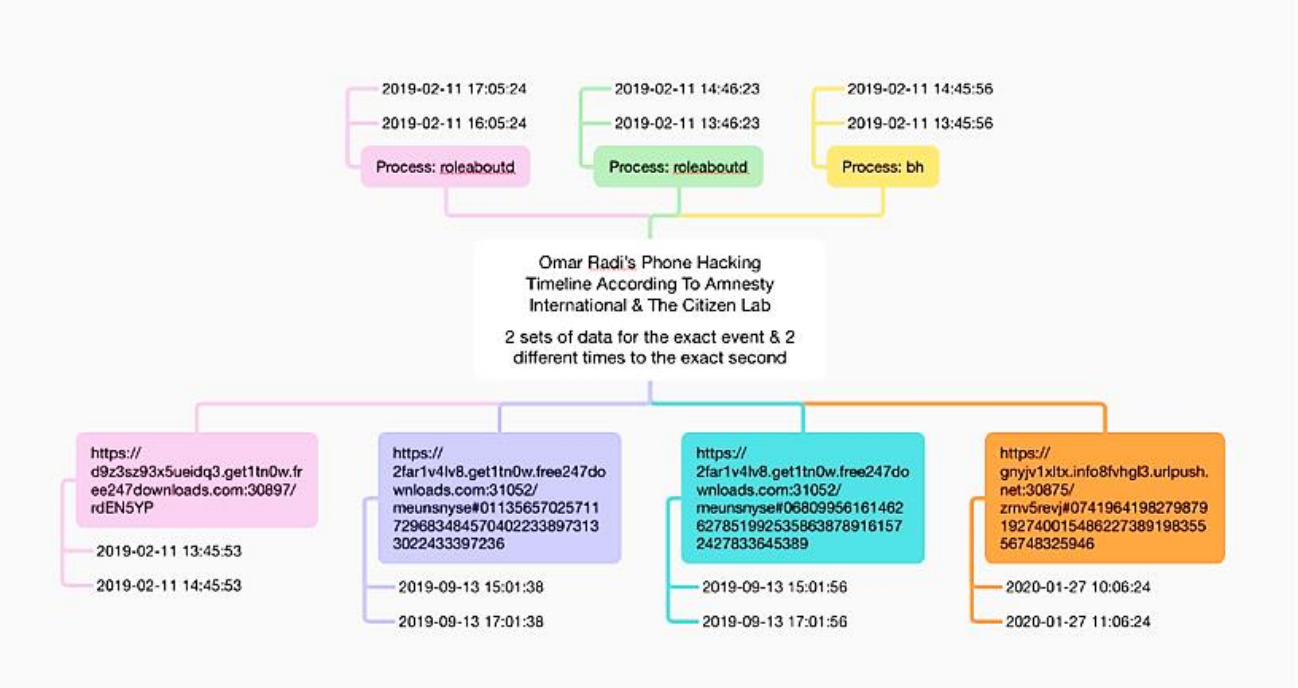

Fig 5. Clear Representation of inconsistencies in Omar Radi Data

4.2 Omar Radi's False Positive Results

Further investigation into the Omar Radi case revealed that the IOC identified on his iOS device, **com.apple.softwareupdateservicesd.plist**, flagged on 2019-09-13 at 17:02:35, was later found to be a false positive [28]. This indicator was removed from the malicious IOC list just one day after Radi's forensic report was released. However, this correction was only mentioned in Amnesty's GitHub repository and was never officially updated in the forensic methodology report or communicated through any major media outlets. Additionally, Radi's mobile device was never reevaluated to verify whether he remained an alleged victim. The process **com.apple.softwareupdateservicesd.plist** is, in fact, a legitimate iOS software update service, and the reasons behind Amnesty and The Citizen Lab initially labeling it as malicious have never been disclosed.

4.3 EU Resolution Against Morocco

Despite knowingly releasing a report containing inconsistent mobile forensics data and false positive results, Amnesty International and The Citizen Lab presented their findings on the Omar Radi case to the European Parliament. Based solely on the testimony and data provided by these organizations, the Parliament signed a motion for a resolution against the Kingdom of Morocco for allegedly violating Radi's human rights. The document, titled "JOINT MOTION FOR A RESOLUTION on the situation of journalists in Morocco, notably the case of Omar Radi [33]," was passed on January 18th, 2023. The full impact of this resolution is yet to be determined. The forensic report, which was later found to contain false positives, was originally published on July 18th, 2021, and the specific false positive (IOC) was identified as such on July 19th, 2021. This means that for over 1 year and 6 months, Amnesty International and The Citizen Lab were aware they were presenting inaccurate data, yet failed to inform the governing bodies to which they appealed.

5 Discussion

The findings from this study highlight serious flaws in the forensic methodologies employed by Amnesty International and The Citizen Lab in high-profile cases such as that of Omar Radi. The identification of false positives and conflicting data in the forensic reports brings into question the scientific rigor and reliability of these investigations. One of the most troubling aspects is the use of speculative forensic indicators of compromise (IOCs), such as the misidentified process com.apple.softwareupdateservicesd.plist, which was later revealed to be a false positive. The fact that this correction was quietly disclosed on a GitHub repository, without any formal update to the forensic methodology report or broader announcement, underscores a significant lack of transparency.

Moreover, the inconsistency in timestamps and data discrepancies, as exemplified by conflicting infection times down to the second, casts doubt on the ability to establish a precise and reliable timeline of the alleged hacking. The reliance on ambiguous forensic artifacts, such as speculative browsing history and process execution logs, further weakens the validity of the findings.

The situation becomes even more concerning when considering the European Parliament's resolution against Morocco, which was based solely on these flawed reports. The failure of Amnesty International and The Citizen Lab to inform governing bodies of the known inaccuracies in the forensic data—while allowing over a year and six months to pass without making the necessary corrections—suggests an

alarming disregard for both transparency and accountability. These findings reveal a broader systemic issue in the way forensic investigations are conducted in politically sensitive cases, where the consequences of erroneous findings can have far-reaching impacts on international relations and human rights discourse.

The key takeaway from this study is the need for more robust and scientifically sound forensic methodologies. Current practices, particularly those involving the identification of Pegasus spyware, must be improved to reduce the risk of false positives and ensure that forensic conclusions are based on reproducible, verifiable data. Furthermore, transparency and independent peer review are essential to restoring credibility to investigations that influence global narratives around state surveillance and human rights abuses..

6 Limitation Study

While this study provides a comprehensive critique of the forensic methodologies applied in the case of Omar Radi, certain limitations should be acknowledged. One challenge faced was the limited access to raw forensic data, as the analysis primarily relied on forensic reports provided by Amnesty International and confirmed by The Citizen Lab. However, this study has made significant strides in critically evaluating these reports, highlighting inconsistencies and questioning their reproducibility and transparency, which are crucial elements of any forensic investigation.

Although this research focuses on a detailed examination of the Omar Radi case, the findings underscore broader concerns about current forensic methodologies used in detecting advanced surveillance technologies (ST). By concentrating on this high-profile case, the study provides insights that can be generalized to other politically sensitive cases involving surveillance technologies. The focus on Omar Radi's case offers a critical lens through which broader systemic issues in the existing methodologies are revealed.

This study also remains centered on improving forensic investigations rather than proposing entirely new methodologies. Its value lies in identifying the weaknesses of current approaches and advocating for the enhancement of scientific rigor, transparency, and reproducibility in future forensic investigations. The insights generated from this critique lay the groundwork for subsequent research and refinement of forensic tools in this evolving field..

7 Conclusion

The investigative practices of Amnesty International and The Citizen Lab demonstrate a troubling pattern of self-referencing and circular validation, significantly undermining the integrity of their findings. The overlapping roles of key individuals, such as Claudio Guarnieri, Etienne Maynier, Sarah Jane Beamish, and Ron Deibert, raise serious concerns about the independence and impartiality of their investigations. These interconnections create a network that erodes credibility and casts doubt on any claims of objectivity. Furthermore, the lack of transparency regarding the identities and roles of individuals involved in these investigations, both to the public and members of the European Parliament, leaves these organizations vulnerable to accusations of bias and conflicts of interest. A more rigorous and impartial investigation conducted at an earlier stage could have exposed the scientific and procedural flaws now plainly evident.

In the Omar Radi spyware investigation, the mutual reinforcement of accusations by Amnesty International and The Citizen Lab exemplifies a flawed approach. The assertion that The Citizen Lab conducted an independent peer review of Amnesty International's forensic methodology is highly questionable, given the shared personnel and potential conflicts of interest. This fact alone severely compromises the objectivity and reliability of their conclusions. Moreover, Amnesty International's failure to provide substantive evidence in response to the Moroccan government's formal requests further exacerbates concerns about the organization's credibility. The delayed and incomplete responses reflect a lack of transparency and accountability, especially troubling for an organization claiming to uphold human rights. Such behavior diminishes the legitimacy of their claims and suggests a disregard for established standards of evidence and due process.

The release of the Forensic Methodology Report by Amnesty International, with its supposed verification by The Citizen Lab, fails to meet the fundamental requirements of a sound and replicable scientific investigation. Instead of presenting clear and verifiable evidence, the report relies heavily on speculation and conjecture. Its disproportionate focus on specific incidents in Morocco, particularly the Omar Radi case, further calls into question its neutrality and objectivity. Such a narrow and selective scope suggests an underlying political bias rather than a commitment to scientific truth. In contrast to recognized industry standards, such as those set by ENISA, Amnesty International's methodology lacks a clearly defined scope, does not adhere to rigorous evidence-handling procedures, and fails to employ a structured approach to data acquisition and analysis. These deficiencies severely limit its reliability as a forensic tool or methodology.

A closer review of the findings in the Omar Radi case reveals numerous methodological flaws and a troubling absence of concrete evidence. The reliance on speculative interpretations, such as those drawn from Safari browsing history and a process referred to as "bh", raises significant concerns about the validity of the attributions made to NSO Group and the credibility of the claimed infections. The identification of false positives, such as the misidentified com.apple.softwareupdateservicesd.plist, further underscores the flaws in Amnesty International's forensic processes. The fact that this error was quietly corrected in Amnesty's GitHub repository, without any formal update to the methodology report or broader announcement, is particularly concerning. Moreover, Amnesty's failure to reevaluate Omar Radi's mobile device after the identification of the false positive raises additional questions about the integrity of their investigation.

The situation becomes even more alarming when considering the impact these flawed forensic reports had on international policymaking. On January 18, 2023, the European Parliament signed a motion for a resolution against the Kingdom of Morocco, allegedly based on the forensic data provided by Amnesty International and The Citizen Lab. The resolution, titled "JOINT MOTION FOR A

RESOLUTION on the situation of journalists in Morocco, notably the case of Omar Radi," was passed over a year and six months after Amnesty and The Citizen Lab became aware of the false positives in their forensic reports. Their failure to inform the European Parliament of these inaccuracies, despite the time that had passed, represents a serious breach of transparency and accountability. This calls into question not only the legitimacy of the forensic findings but also the integrity of the broader international response.

Given the severity of these issues, it is imperative that Amnesty International and The Citizen Lab undergo a comprehensive and independent review of their investigative practices. Without such a re-evaluation, their methodologies will continue to lack the transparency, accountability, and scientific rigor required in the field of digital forensics and human rights investigations. Their approach, as it currently stands, compromises not only their own credibility but also the integrity of the investigations they claim to uphold.

Author Contribution Statement : J. Scott was responsible for conceptualizing the research framework, designing the methodology, and leading the development of the proposed lightweight cryptographic protocols. They performed most of the experimental simulations, data analysis, and interpretation of the results. J. Scott also contributed to drafting and revising the manuscript for publication. All contributions were integral to the successful completion of this research study.

Data availability: Data available upon request.

Conflict of Interest: There is no conflict of Interest.

Ethical Compliance Statement: The study was conducted in accordance with ethical guidelines, this study did not involve human or animal participants.

Funding Disclosure: The research received no external funding.

Similarity checked: Yes.

References

[1.] Amnesty International, "Morocco: Authorities must ensure Omar Radi's fair trial rights," Mar. 3, 2022. [Online]. Available: https://www.amnesty.org/en/latest/news/2022/03/morocco-authorities-must-ensure-omar-radis-fair-trial-rights/

[2.] Amnesty International, "NSO spyware used against Moroccan journalist days after company pledged to respect human rights," Jun. 22, 2020. [Online]. Available: https://www.amnesty.org/en/latest/news/2020/06/nso-spyware-used-against-moroccan-journalist/

[3.] Amnesty International, "Forensic methodology report: How to Catch NSO Group's Pegasus," Jul. 18, 2021. [Online]. Available: https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

[4.] P. Chauhan and P. Bansal, "Assessment of Forensics Investigation Methods," Smart Innovation, Systems and Technologies, pp. 317–324, 2021. doi: 10.1007/978-981-33-4443-3_30.

[5.] A. M. Alashjaee and M. Haney, "A Framework for Mobile Malware Forensics," 2020 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 2020, pp. 175–181. doi: 10.1109/CSCI51800.2020.00037.

[6.] Privacy International, "Taming Pegasus: A way forward on surveillance tech proliferation," Jul. 27, 2021. [Online]. Available: https://privacyinternational.org/news-analysis/4602/taming-pegasus-way-forward-surveillance-tech-proliferation

[7.] Maratsi, M. I., Popov, O., Alexopoulos, C., & Charalabidis, Y. (2022). Ethical and legal aspects of digital forensics algorithms: The case of digital evidence acquisition. Proceedings of the 15th International Conference on Theory and Practice of Electronic Governance, 72, 32–40. https://doi.org/10.1145/3560107.3560114

[8.] Privacy International, "Briefing note on OECD Complaints against Gamma International and Trovicor in the UK and Germany," Feb. 3, 2013. [Online]. Available: https://web.archive.org/web/20130308002112/https://www.privacyinternational.org/sites/privacyinternational.org/files/downloads/press-releases/2013_02_01_oecd_briefing_note.pdf

[9.] Privacy International, "Our People," Jul. 6, 2012. [Online]. Available: https://web.archive.org/web/20120706172455/https://privacyinternational.org/people

[10.] Privacy International, "Our People," Mar. 7, 2013. [Online]. Available: https://web.archive.org/web/20130307220652/https://privacyinternational.org/people

[11.] The Citizen Lab, "People," Jun. 18, 2020. [Online]. Available: https://web.archive.org/web/20200618113556/https://citizenlab.ca/people/

[12.] C. Guarnieri, "Claudio Guarnieri," Sep. 27, 2020. [Online]. Available: https://web.archive.org/web/20200927032322/https://www.allamericanspeakers.com/speakers/398576/Claudio-Guarnieri

[13.] E. Maynier, "About Me," Jan. 24, 2024. [Online]. Available: https://web.archive.org/web/20240124110622/https://randhome.io/about/

[14.] Amnesty International, "Amnesty International Limited: Report and financial statements for the year

ended 31 December 2021," Oct. 1, 2022. [Online]. Available: https://www.amnesty.org/en/documents/fin40/6385/2022/en/

[15.] The Munk School, "Meet MGA alumna-turned-faculty, Sarah Beamish," Apr. 21, 2021. [Online]. Available: https://web.archive.org/web/20221125144203/https://munkschool.utoronto.ca/mga/news/meet-mga-alumna-turned-faculty-sarah-beamish

[16.] University of Toronto, "Human ethics principles & guidelines," Human Ethics Principles & Guidelines, 2019. [Online]. Available: https://research.utoronto.ca/ethics-human-research/human-ethics-principles-guidelines

[17.] N. Sunde, "Strategies for safeguarding examiner objectivity and evidence reliability during digital forensic investigations," Forensic Science International: Digital Investigation, vol. 40, p. 301317, 2022. doi: 10.1016/j.fsidi.2021.301317.

[18.] D. Kim and S. Lee, "Study of identifying and managing the potential evidence for effective Android forensics," Forensic Science International: Digital Investigation, vol. 33, p. 200897, 2020. doi: 10.1016/j.fsidi.2019.200897.

[19.] N. Hughes and U. Karabiyik, "Towards reliable digital forensics investigations through Measurement Science," WIREs Forensic Science, vol. 2, no. 4, 2020. doi: 10.1002/wfs2.1367.

[20.] Le 360, "Omar Radi Case: Government Demands Official Response From Amnesty Again," Le 360 Français, Feb. 7, 2020. [Online]. Available: https://fr.le360.ma/politique/video-affaire-omar-radi-le-gouvernement-exige-de-nouveau-une-reponse-officielle-damnesty-218462/

[21.] Amnesty International, "Forensic methodology report: How to catch NSO group's Pegasus - Original Report," Jul. 18, 2021. [Online]. Available: https://web.archive.org/web/20210718160124/https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

[22.] ENISA, "Mobile threats incident handling," 2014. [Online]. Available: https://www.enisa.europa.eu/topics/training-and-exercises/trainings-for-cybersecurity-specialists/online-training-material/documents/Mobileincidenthandlinghandbook.pdf

[23.] Lookout, "Technical analysis of the Pegasus exploits on iOS," Dec. 13, 2016. [Online]. Available: https://info.lookout.com/rs/051-ESQ-475/images/pegasus-exploits-technical-details.pdf

[24.] Mitre.org, "CVE-2016-4657," CVE, May 11, 2016. [Online]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4657

[25.] Apple Developer Forums, "Many apps crash with EXC_CRASH (SIGABRT)," Sep. 2023. [Online]. Available: https://developer.apple.com/forums/thread/737336

[26.] Rick Rheo, "False indication of Pegasus · issue #19 · AmnestyTech/investigations," GitHub, Jul. 27, 2021. [Online]. Available: https://github.com/AmnestyTech/investigations/issues/19

[27.] AmnestyTech, "Remove a file that creates false positive · AmnestyTech/investigations@928ea5a," GitHub, Jul. 28, 2021. [Online]. Available: https://github.com/AmnestyTech/investigations/commit/928ea5a820df6596762241da147b5afa1458b5ee

[28.] AmnestyTech, "Removing false positive · AmnestyTech/investigations@1c69421," GitHub, Jul. 19, 2021. [Online]. Available: https://github.com/AmnestyTech/investigations/commit/1c694217c3efb4e40f34822b6ef99a7b5bd8a064

[29.] B. Marczak, J. Scott-Railton, S. Anstis, and R. Deibert, "Independent peer review of Amnesty International's forensic methods for identifying Pegasus spyware," The Citizen Lab, Jul. 18, 2021. [Online]. Available: https://citizenlab.ca/2021/07/amnesty-peer-review/

[30.] AmnestyTech, "Warning + remove false positive · AmnestyTech/Investigations@ba749a9," GitHub, Jul. 22, 2021. [Online]. Available: https://github.com/AmnestyTech/investigations/commit/ba749a926cec4bf43920c9300922296689fdc57b

[31.] AmnestyTech, "Re-added indicator that was removed as FP by mistake · AmnestyTech/investigations@6914279," GitHub, Nov. 4, 2021. [Online]. Available: https://github.com/AmnestyTech/investigations/commit/6914279c3c3226c2c88a28f0fb008ef9bc4bc8e5

[32.] EU Parliament, "Joint motion for a resolution on the case of Paul Rusesabagina in Rwanda: RC-B9-0500/2021," Oct. 6, 2021. [Online]. Available: https://www.europarl.europa.eu/doceo/document/RC-9-2021-0500_EN.html

[33.] A. Bielan and A. F. Adam, "Joint motion for a resolution on the situation of journalists in Morocco, notably the case of Omar Radi: RC-B9-0057/2023," Jan. 18, 2023. [Online]. Available: https://www.europarl.europa.eu/doceo/document/RC-9-2023-0057_EN.html