

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/365743925>

Review of Catalangate Amnesty International Validation

Technical Report · November 2022

CITATIONS

0

1 author:



Jonathan Scott

2 PUBLICATIONS 0 CITATIONS

SEE PROFILE

Some of the authors of this publication are also working on these related projects:



UNCOVERING THE CITIZEN LAB AN ANALYTICAL AND TECHNICAL REVIEW DISPROVING CATALANGATE [View project](#)

November, 2022

REVIEW OF CATALANGATE

Amnesty
International
Validation

Jonathan Boyd Scott

Review of Catalangate
Amnesty International Validation

Jonathan Boyd Scott

November 25, 2022

Running head: Review of Catalangate: Amnesty International Validation	2
Abstract	2
Prelude	3
Rules of Procedure	6
The 5 Principals	7
Missing Critical Information	13
The Infected	14
False Positive Results	17
com.apple.CrashReporter.plist	17
False Positive Alert #1	18
False Positive Alert #2	21
False Positive Alert #3	23
Falsifying com.apple.CrashReporter.plist	24
Nullification	26
Confirming The Nullification	28
Global Impact of Non-Disclosure	29
Forging All IOCs	34
Forging Processes	35
Sònia Urpí Garcia (CATPOI1)	36
Meritxell Bonet (CATPOI2)	36
Elisenda Paluzie (CATPOI3)	36
Jordi Sànchez (CATPOI4)	37
Jordi Sànchez Text Discrepancy	37
Conclusion	38
References	40

Abstract

The Spanish government continues to be accused of deploying spyware on 65 Catalans, lawsuits are frequently filed, and The Citizen Lab's Catalangate spyware case is referenced in support of a congressional bill¹. A letter questioning the Catalangate report's ethics and methods was sent to The University of Toronto on 3 separate occasions. A collective of over 120 professors² from around the world requested an independent investigation into claims The Citizen Lab, and Amnesty International made against the Spanish government, but The University of Toronto did not reply. Members of The European Parliament regularly meet to discuss the matter, victim testimony has been heard, but the scientific facts of the case are not being presented. A qualified, unbiased, methodologically reproducible, and independent forensics analysis has never been presented to any

global governing committee. The European PEGA Inquiry Committee has invited independent technical experts to testify on the findings presented in the Catalangate report, but the experts never forensically examined any of the alleged infected mobile devices. This research is a review and analysis of forensics procedure, scientific methods, international forensics data statutes, and the validation data published by Amnesty International pertaining to the Catalangate. I will present a method that yields false positive results when tested against confirmed Pegasus infection data sets published by the Amnesty Tech Security Lab. The method is an iOS database backup manipulation. The manipulation is possible due to Amnesty Tech's failure to hash their forensics data sets, specifically the SQLite files when running their Pegasus detection software, MVT-Tool.

¹ <https://docs.house.gov/meetings/IG/IG00/20220727/115048/HHRG-117-IG00-Wstate-Scott-RailtonJ-20220727.pdf>

² <https://paginadelforodeprofesores.files.wordpress.com/2022/07/letter-to-university-of-toronto-by-foro-de-profesores-5-july-2022-re-Catalangate-report.pdf>

Prelude

April 18th, 2022 The Citizen Lab³, a global affairs and public policy institution at The University of Toronto's Munk School, released a report titled, **Catalangate Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru**⁴. The word gate in the report title is suggestive of a scandal, and is known as “*a suffix that stinks of corruption*.”⁵ The Catalangate affair is the world's largest alleged case of targeted surveillance to date. Committees have formed, lawsuits have been filed⁶, and inquiries have commenced⁷ in part due to allegations that members of Catalan civil society were targeted with Pegasus, **The World's Most Terrifying Spyware**⁸. Israeli based firm, NSO Group is the creator of Pegasus, and for years has been accused of violating human rights by NGOs and institutions around the world. Amnesty Tech, a division of Amnesty International and The Citizen Lab were said to have worked independently to prepare impartial

data for the alleged Catalangate espionage. From 2019 when the Spanish government was first accused of espionage to current 2022, both institutions have maintained active mutual agreements that negate any claims of independent impartial data analysis. Amnesty and The Citizen Lab are financially supported by the Ford Foundation⁹ among others, and failed to disclose that they had employed the same security researcher during the initial investigations into the alleged espionage from 2019 to mid 2021¹⁰. The dually employed researcher Etienne Maynier left The Citizen Lab April, 2021 but remained on the mobile forensics team responsible for writing and maintaining the code Amnesty uses to detect Pegasus spyware called MVT-Tool¹¹. The MVT-Tool would later be used to validate samples of alleged victims mentioned in The Citizen Lab's Catalangate report.

³ The Citizen Lab is not a registered NGO (Non-Governmental Organization)

⁴ <https://citizenlab.ca/2022/04/Catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/>

⁵ <https://www.merriam-webster.com/words-at-play/gate-suffix-scandal-word-history>

⁶ https://files.mediaset.es/file/10002/2022/05/03/Querella_Pegasus_-Gonzalo_BOYE_-_1_-_2_5367.pdf

⁷ <https://emeeting.europarl.europa.eu/emeeting/committee/en/archives/PEGA>

⁸ <https://www.youtube.com/watch?v=QX7X4Ywuotc>

⁹ https://twitter.com/FordFoundation/status/1463568098489946120?s=20&t=EHO FYLxd6s_JXEc5S6zAdA

¹⁰ <https://deibert.citizenlab.ca/wp-content/uploads/2022/05/2022.05.13-L-Ferris-to-J-Canas.pdf> [pg. 6 § 5]

¹¹ <https://docs.mvt.re/en/latest/>

Attorney Sarah Jane Beamish was also dually employed from 2019-2021, during the Catalangate investigations. Beamish was Amnesty International's chair of the Board of Directors¹², a professor at the University of Toronto's Munk School¹³, and was a subordinate of The Citizen Lab's director Ron Deibert. Amnesty and The University of Toronto have had an active partnership since 2016 with the Citizen Evidence Lab¹⁴. The evidence of a conflict of interest between Amnesty International and The Citizen Lab is vast. July 27th, 2021 Amnesty International released a document calling for an immediate suspension of NSO Pegasus software based on a list of 50,000 potential surveillance targets acquired by The Pegasus Project¹⁵. The document titled **Joint open letter by civil society organizations and independent experts calling on states to implement an immediate moratorium on the sale, transfer and use of surveillance technology**¹⁶, is co-signed by 156 civil society organizations and 26 independent experts worldwide¹⁷ (Amnesty, 2021). The

open letter shows a communion between The Citizen Lab, Amnesty International, and calls all states to “*Conduct an immediate, independent, transparent and impartial investigation into cases of targeted surveillance*”¹⁸. The undersigned organizations and experts would request for an independent, impartial investigation into the espionage allegedly facilitated by NSO Group, but when later presented with a reciprocal request by 120 professors¹⁹ as to how Citizen Lab came to these conclusions of espionage, the professor's requests would never been acknowledged.

Amnesty's request for an immediate moratorium would also introduce Elies Campo²⁰ as an independent expert with Telegram. Campo would write and jointly confirm Amnesty's forensics methodology and support their “*forensic tests on mobile phones to identify traces of the Pegasus spyware*”²¹. Amnesty used the exact forensics methodology Campo validated to confirm Citizen Lab's Catalangate in which Elies Campo would be listed as a primary

¹² <https://www.amnesty.org/en/documents/fin40/4743/2021/en/> (Financials, Pg 50, payments to directors 2019 & 2022)

¹³ <https://munkschool.utoronto.ca/mga/news/meet-mga-alumna-turned-faculty-sarah-beamish> (Current professor as of Nov, 2022)

¹⁴ <https://citizenevidence.org/>

¹⁵ <https://forbiddenstories.org/about-the-pegasus-project/>

¹⁶ <https://www.amnesty.org/en/wp-content/uploads/2021/08/DOC1045162021ENGLISH.pdf>

¹⁷ <https://www.amnesty.org/en/documents/doc10/4516/2021/en/#:~:text=July%2027%2C%202021Index%20Number%3A%20DOC>

¹⁸ <https://www.amnesty.org/en/wp-content/uploads/2021/08/DOC1045162021ENGLISH.pdf> [pg. 3 § 4b]

¹⁹ <https://www.eltaquigrafo.com/articulo/investigacion/un-centenar-de-profesores-pide-a-la-universidad-de-toronto-que-revise-el-informe-del-Catalangate/20220710140416019942.html>

²⁰ <https://www.amnesty.org/en/wp-content/uploads/2021/08/DOC1045162021ENGLISH.pdf> [pg. 10]

²¹ <https://www.amnesty.org/en/wp-content/uploads/2021/08/DOC1045162021ENGLISH.pdf> [pg. 1 § 2]

author and forensics investigator. Elies had been working with Citizen Lab since 2020²², but it was not revealed that Elies Campo had been working with Amnesty International at the same time he was working on Citizen Lab's Catalangate investigations.

Moreover, the moratorium shows cooperation with Fundació.cat, a Barcelona based domain registrar where the domain catalangate.cat would be purchased. Another signatory on the list is Xnet,²³ a pro-Catalan independence organization supporting Junts per Cat (JUNTS). Reviewing research data, I noticed the amount of support Amnesty International was giving to the Catalan pro-independence movement was extensive. April 14th, 2022, 4 days before the release of the Catalangate report, members²⁴ of the Global Encryption Coalition²⁵ including The

Citizen Lab, and Internet Society Catalan Chapter (ISOC-CAT) would co-sign a letter to the UK Parliament.

When the Catalangate report was released, the Spanish government faced a global coordinated effort by Amnesty and The Citizen Lab to attribute cellphone phishing links and normal occurring iPhone processes to acts of espionage. Even after knowingly taken part in verifiable conflicts of interest that include financial exchanges, Citizen Lab and Amnesty claimed to have worked ethically and independent from each other. After reviewing evidence presented by Amnesty and Citizen Lab it was evident that neither organization had knowledge on how to properly conduct a mobile forensics investigation.

²² <https://deibert.citizenlab.ca/wp-content/uploads/2022/05/2022.05.13-L-Ferris-to-J-Canas.pdf> [pg. 5 § 4]

²³ <https://xnet-x.net/es/xnet-registra-primera-ley-alertadores-ue/>

²⁴ <https://www.globalencryption.org/about/members/>

²⁵ <https://www.globalencryption.org/2022/04/45-organizations-and-cybersecurity-experts-sign-open-letter-expressing-concerns-with-uks-online-safety-bill/>

Rules of Procedure

Pega Committee²⁶ chair Mr. Jeroen Lenaers, stated *“I think our role as an inquiry committee is to make sure that all the facts become publicly known, that we investigate the situation, but also to come up with conclusions and recommendations, and in the end European legislation to make sure that governments in the European Union cannot abuse this kind of software in the future²⁷”* (Lenaers, 2022). Amnesty supported claims of the Spanish government spying on Catalans by publishing what they call forensics traces for selected alleged victims, but Amnesty’s claims fail to follow ENISA,²⁸ and Europol regulations for digital forensics acquisition²⁹.

Mr. Lenaers recognized the need for Europol to exercise its authority and conduct a full investigation into this matter. Lenaers sent a letter to Europol director Catherine De Bolle, September 28th, 2022 and wrote, *“Spyware abuse has occurred all over Europe: this is a task for Europol. With every day that passes, the risk increases that*

evidence is being destroyed. It is crucial that Europol gets involved in order to secure the evidence and investigate the use of spyware in EU member states. Fighting cybercrime, corruption and extortion fall squarely within the mandate of Europol and is in the interest of European democracy³⁰”

June 26th, 2014 Europol Director Rob Wainwright, and ENISA Executive Director Udo Helmbrecht signed an agreement for strategic operation, uniting the European Union Agency for Network and Information Security (ENISA) and the European Police Office (Europol)³¹. The reason for the agreement between these 2 agencies is as follows: *“The purpose of this Agreement is to establish co-operative relations between Europol and ENISA in order to support to the Member States of the European Union and its Institutions in preventing and combating cybercrime and other forms of related crime with a view to ensuring a high and effective level of network and information security³²”* (Europol, 2018).

²⁶ Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware

²⁷ <https://www.youtube.com/watch?v=LciskOzRD4Y>

²⁸ European Union Agency for Network and Information Security (ENISA)

²⁹ https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders/at_download/fullReport

³⁰ <https://app.box.com/s/ngueyof0qlhqhs5ofjukuj7jyudsqar>

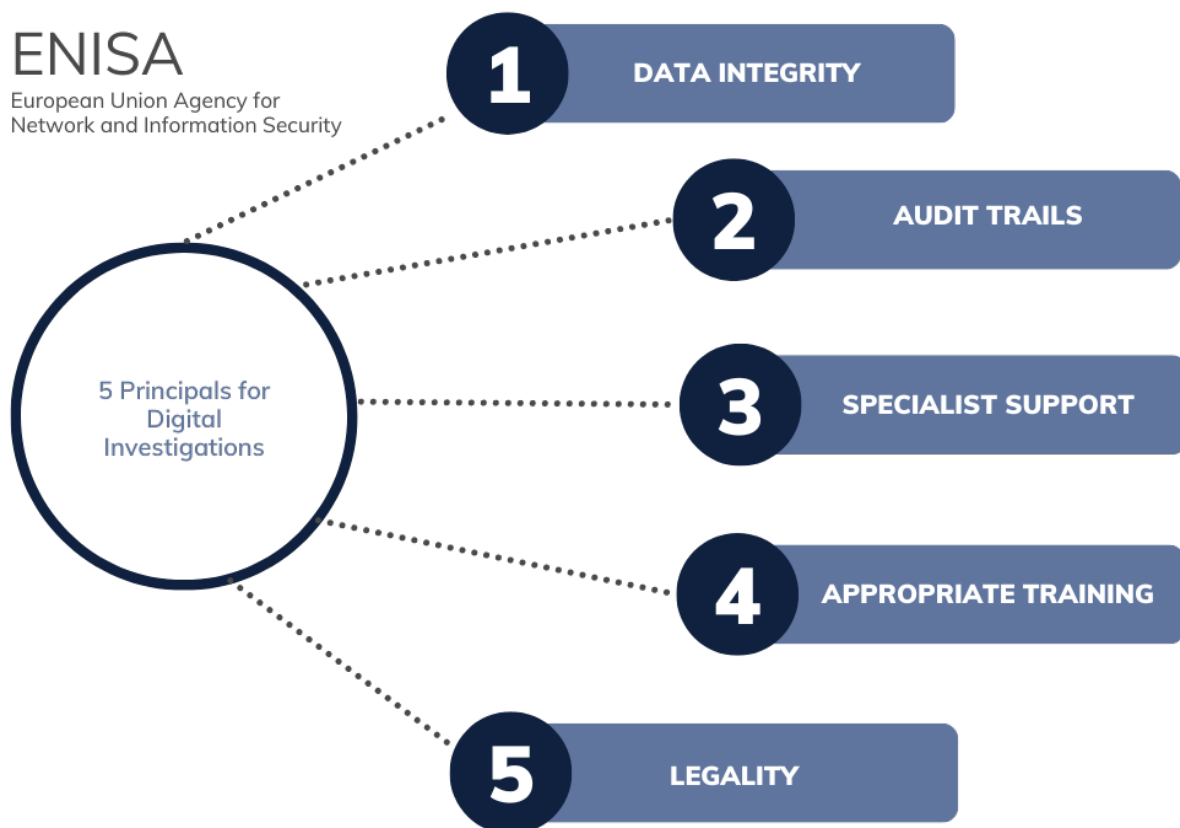
³¹ https://www.europol.europa.eu/cms/sites/default/files/documents/Agreement_on_Strategic_Co-operation_between_the_European_Union_Agency_for_Network_and_Information_Security_and_the_European_Police_Office.pdf

³² <https://www.europol.europa.eu/partners-collaboration/agreements/european-union-agency-for-network-and-information-security-enisa#downloads>

The 5 Principals

ENISA identifies 5 principals that need to be followed when conducting a digital investigation. I will be providing the principal text from ENISA guidelines and an abridged review directly associated to the principal as it pertains to the Amnesty Tech Catalangate validation report³³.

Figure 1 ENISA's 5 Principals for Digital Investigations



³³<https://www.amnesty.org/en/latest/research/2021/08/appendix-e-pegasus-forensic-traces-per-target-identified-in-the-aftermath-of-the-revelations-of-pegasus-project/>

Table 1ENISA Principals, Amnesty International, and The Citizen Lab Violations

ENISA Principal	Definition	Status
Data Integrity	The integrity of digital evidence must be maintained at all stages. “No action taken [...] should change data which may subsequently be relied upon in court.” From all the principles this is probably the most important one. As the integrity of the evidence is of extreme importance, it is vital that the integrity requirement of the evidence is the main driver and should be the most important factor in deciding what to do (and what not do). Digital data is volatile, and the ease with which digital media can be modified implies that documenting a chain of custody is extremely important to establish the authenticity of evidence. In addition, all examination processes must be documented so that if needed, they can be replicated. ³⁴	<ol style="list-style-type: none"> 1. The forensics report has been modified since Amnesty Tech has published April, 19th, 2022³⁵ 2. There was no remark in the document history showing that the Catalan data had been altered. 3. The code based used to confirm the infections of the alleged victims has been tampered since release, an indicator of compromise was removed³⁶ 4. Chain of Custody documentation has never been presented in any version of Amnesty’s forensics reports, and the location of the physical evidence is unknown.
Audit Trail	An audit trail (often referred to as chain of custody or chain of evidence) is the process of preserving the integrity of the digital evidence. “Documentation permeates all steps of investigative process but is particularly important in the digital evidence seizure step. It is necessary to record details of each piece of seized evidence to help to establish its authenticity and initiate the	<ol style="list-style-type: none"> 5. Amnesty does not present an audit trail with steps that can be reproduced by an independent examiner³⁸. 6. No information provided shows the preservation of evidence or logging. 7. The Citizen Lab specifically stated that physical phones were not needed for the

³⁴ https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders/at_download/fullReport [pg. 11 § 4]

³⁵ <https://web.archive.org/web/diff/20220419175052/20220730005403/https://www.amnesty.org/en/latest/research/2021/08/appendix-e-pegasus-forensic-traces-per-target-identified-in-the-aftermath-of-the-revelations-of-pegasus-project/>

³⁶ <https://github.com/AmnestyTech/investigations/commit/928ea5a820df6596762241da147b5afa1458b5ee> [Remove a file that creates false positive]

³⁸ From 2019-2020 I was contracted and paid to work with the United States Government in a role requiring a security clearance. My task was to develop iOS forensics methodologies that could be reproduced and shared amongst government employees and contractors. What Amnesty and The Citizen Lab have presented as forensics “Traces,” proving a spyware infection cannot be followed.

<p>chain of custody.” Indeed, an “audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those actions and achieve the same result.” It is of vital importance that any digital exhibit can be tracked from the moment when it was seized at the crime scene all the way to the courtroom, as well as anywhere else in between such as laboratories or storages. To demonstrate that a robust chain of custody or audit log was maintained details of the evidence and how it was handled, by whom as well as everything that has happened to it needs to be recorded at every step of the investigation. It is important to stress how such details can be crucial. It is better to note down too many details than recording too few details about the actions taken. It is, for example, advisable to note down which keystrokes were entered and which mouse movements have been made rather than just to write down in generic terms that “a forensic backup has been performed”³⁷.</p>	<p>Catalangate investigation in an interview with EL PAÍS³⁹.</p> <p>8. A common theme with Amnesty and The Citizen Lab is to not obtain physical access to the devices, and share the exact “sample” or mobile device backup with each other and then claim that it has been independently verified. An example of this can be seen in the alleged spyware infection cases in Poland,</p> <p>“Donncha Ó Cearbhaill, an expert with Amnesty International’s Security Lab, said he confirmed Citizen Lab’s finding after receiving raw backups of Brejza’s phone from the Canadian researchers. Amnesty uses independently developed tools and methods for its forensic analysis⁴⁰.”</p> <p>Another example can be seen in 2021 when Amnesty shared 4 iPhone backups with The Citizen Lab⁴¹, and Citizen Lab confirmed the spyware infections. Without ever having the mobile device and working with backup that were not taken by them, and can easily be tampered with.</p>
--	---

³⁷ https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders/at_download/fullReport [pg. 12 § 3]

³⁹ <https://elpais.com/espana/2022-05-15/ronald-deibert-fundador-de-citizen-lab-los-gobiernos-usan-pegasus-porque-tienen-apetito-de-espiar.html>

Q. In the case of the President of the Government, the theft of information has been certified through a forensic analysis of his own telephone. But you never physically had in your possession the mobiles of those supposedly spied on.

A. You don't need it. We have a spectrum of data from multiple sources. We have explored the infrastructure used by companies like NSO, which is provided by Pegasus. Everyone leaves digital background. If I access your mobile and the client is the Government, NSO has a server here to send instructions that go from computer to computer and whose traces we can access with great caution. We have access to quite a bit of visibility into the NSO infrastructure. Receiving the mobile might not be that useful for us. Companies make mistakes and leave traces.

⁴⁰ <https://www.timesofisrael.com/amnesty-verifies-polish-senator-was-hacked-with-nso-spyware/>

⁴¹ <https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/>

<p>Specialist Support</p>	<p>Specialist support needs to be requested as soon as possible when evidence gathering raises some specific (technical issues) and the first responders in charge of the evidence collection is not familiar with the issue or its implications. As there exist so many different systems and technical situations, it is almost impossible for a digital forensics expert to have the specific know-how on how to deal with all these sorts of electronic evidence. This is why it is so crucial to call in the right specialists – either internal from the team or from external - when necessary and to have the right equipment ready for them to perform their tasks⁴².</p>	<ol style="list-style-type: none"> 9. Members of European Parliament have withdrawn an invitation extended to Dr. Jose Javier Olivas Osuna, a professor of political science at The London School of Economics and Political Science⁴³. Olivas was invited to give expert testimony in a PEGA inquiry hearing regarding ethical concerns surrounding the Catalangate report. 10. The invitation was withdrawn because unverified credentials were accepted by members of European Parliament in a letter undersigned by 12 academics, researchers, and experts⁴⁴. 11. Łukasz Siewierski is among the experts The Citizen Lab asked to undersign a letter warning the PEGA committee of Dr. Olivas' "Credibility issues"⁴⁵ 12. The Amnesty Tech Catalangate Validation report is 100% based on iOS (iPhone) spyware detection. When speaking about iOS Pegasus detection, Siewierski explicitly stated the following about himself Jan 14th, 2022 "Sorry, I don't know that much about iOS/iPhone to make any informed comments on this one"⁴⁶." 13. Including a non-expert in a list of people alleged to be specialists is fraudulent, and all specialists named by The Citizen Lab and Amnesty should have a
----------------------------------	---	---

⁴² https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders/at_download/fullReport [pg. 12 § 6]

⁴³ <https://www.linkedin.com/in/jose-javier-olivas-osuna-627b99/?originalSubdomain=uk>

⁴⁴ <https://www.linkedin.com/in/jose-javier-olivas-osuna-627b99/?originalSubdomain=uk> (Photo 2 & 3)

⁴⁵ <https://twitter.com/josejolivas/status/1595392536843100160/photo/4>

⁴⁶ <https://twitter.com/maldr0id/status/1482100432239480841>

		thorough investigation of their qualifications.
Appropriate Training	Proper training is a very important prerequisite for the success of the search and seizure of electronic evidence. Appropriate and constant training should be provided to all first responders dealing with digital forensic, especially when they are expected to deal specifically with ‘live’ computer and access original data ⁴⁷ .	14. One of the principal investigators of the Catalangate Elies Campo forged his professional experience ⁴⁸ , and was still able to obtain a fellowship with The Citizen Lab. There is a common theme amongst Amnesty and the Citizen Lab and it is one that requires no validation of credentials, expertise, or appropriate training in order to part of their internal forensics team, or a credible 3 rd party specialist.
Legality	The person in charge of the investigation has overall responsibility for ensuring that the law and these principles [the principles of digital evidence] are adhered to.” Legal guidance for the practitioner varies depending on the jurisdiction in which they reside. Further, a distinction must be made between legislative documents and guidance and principles provided by relevant governing bodies within the forensic industry. Examples of such guidance documents include the above-mentioned electronic evidence guide [5 principals] - A basic guide for police officers, prosecutors and judges developed within the framework of the European Union and the Council of Europe joint project (CyberCrime@IPA project) and the UK ACPO Good Practice Guide for Digital Evidence ⁴⁹ .	<p>15. The Citizen Lab and Amnesty Tech have disregarded international standards for the collection of digital evidence, and are presenting “strong circumstantial evidence” as facts the Spanish government has deployed Pegasus spyware on citizens of Catalonia</p> <p>16. Citizen Lab and Amnesty have not adhered to ENISA principals</p> <p>17. Citizen Lab and Amnesty are using the Catalangate report as validation for wide spread spyware abuse.</p> <p>18. John Scott-Railton on behalf of The Citizen Lab references the hacking of Catalan politicians in testimony given to The United States House Intelligence Committee.⁵⁰</p> <p>19. Scott-Railton never mentioning that false positive indicators were found in the Spanish CatalanGate report results,</p>

⁴⁷ https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders/at_download/fullReport [pg. 13 § 1]

⁴⁸ https://cronicaglobal.elespanol.com/politica/artifice-catalangate-elies-campo-curriculum_661667_102.html

⁴⁹ https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders/at_download/fullReport [pg. 13 § 2]

⁵⁰ <https://docs.house.gov/meetings/IG/IG00/20220727/115048/HHRG-117-IG00-Wstate-Scott-RailtonJ-20220727.pdf> [pg. 6 § 4]

		<p>Rwandan spyware case of Carine Kanimba and many more.</p> <p>20. The exclusion of this information is testimony is a violation of the Truth in Testimony Disclosure signed by John Scott-Railton representing The Citizen Lab the Munk School of Global Affairs, University of Toronto.</p> <p>21. When Scott-Railton and The Citizen Lab signed the Truth in Testimony Disclosure Form they were knowingly concealing the false positive Catalangate results, which is a violated of The United States Criminal Code 18 U.S.C. § 10001</p> <p>The False Statements Certification Signed by John Scott-Railton July 25th, 2022 states,</p> <p>“Knowingly providing material false information to this committee/subcommittee, or knowingly concealing material information from this committee/subcommittee, is a crime 18 U.S.C. § 10001⁵¹”</p>
--	--	--

⁵¹ <https://docs.house.gov/meetings/IG/IG00/20220727/115048/HHRG-117-IG00-TTF-Scott-RailtonJ-20220727.pdf> [pg. 3]

Missing Critical Information

Amnesty Tech's validation of infected Catalans can be found in Annex E of Amnesty International's **Forensic Methodology Report: How to catch NSO Group's Pegasus**⁵². Amnesty's Annex E and Citizen Lab's Catalangate report were both missing key information required by ENISA, Interpol Guidelines for Digital Forensics First Responders⁵³ supported by SPAIN: Cybercrime Unit, General Commissary of Criminal Police (CGPJ) of Spanish National

Police (CNP); and also required by the United Nations (OHCHR) Office of the High Commissioner for Human Rights, Berkeley Protocol on Digital Open-Source Investigations. For example: Annex I-V⁵⁴ has templates the digital forensics examiner is required to fill out if the intention of the victim is to pursue criminal action against their abuser.

Table 2 Standard Forensics Questions

Standard Questions	Answer
Who was the examiner?	Unknown
When did the examination start?	Unknown
When did the examination conclude?	Unknown
What court ordered the forensics examination?	Unknown
Where can the chain of custody logs be found?	Unknown
How were the devices transported?	Unknown
Do the chain of custody logs have signatures from everyone involved, including law enforcement, examiners, analysts, and others?	Unknown

⁵² <https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/>

⁵³ https://www.interpol.int/content/download/16243/file/Guidelines%20to%20Digital%20Forensics%20First%20Responders_V7.pdf

⁵⁴ https://www.ohchr.org/sites/default/files/2022-04/OHCHR_BerkeleyProtocol.pdf

Who else had access to the mobile devices in question?	Unknown
Were these mobile devices owned by the alleged victims or where they purchased, controlled and or managed by their employer?	Unknown
What are the serial numbers of the mobile devices?	Unknown
What are the operating system versions of the mobile devices?	Unknown
Are all of the mobile devices currently held in a secured facility with law enforcement while these ongoing investigations are happening?	Unknown

The Infected

April 18th, 2022 The Citizen Lab released their Catalangate report, and on the same day Amnesty published a press release called **Spain: EU must act to end spyware abuse after prominent Catalans targeted with Pegasus**⁵⁵.

The Amnesty press release speaks about Amnesty independently verifying devices from 4 Pegasus spyware infected victims. The press release states, “*New research by the Citizen Lab has revealed how scores of Catalan politicians, journalists and their families were targeted with NSO Group’s Pegasus spyware between 2015 and 2020. Technical experts from Amnesty International’s Security Lab have*

independently verified evidence of the attacks... Amnesty International’s Security Lab peer reviewed forensic evidence from a sample of individuals first identified in the Citizen Lab investigation, and found evidence of Pegasus targeting and infection in all cases.”

The independent verification and peer review between Amnesty and The Citizen Lab is again stated and April 19th, 2022 Appendix E⁵⁶ was released and included 3 alleged victims Amnesty had validated to be infected with Pegasus spyware. Jordi Sànchez, Meritxell Bonet, and Elisenda Paluzie were listed with their “forensics traces.”

⁵⁵ <https://www.amnesty.org/en/latest/news/2022/04/spain-pegasus-spyware-catalans-targeted/>

⁵⁶ <https://web.archive.org/web/20220419175052/https://www.amnesty.org/en/latest/research/2021/08/appendix-e-pegasus-forensic-traces-per-target-identified-in-the-aftermath-of-the-revelations-of-pegasus-project/>

July 30th, 2022 Appendix E was changed and now included Sònia Urpí Garcia. 102 days after its first publication Amnesty replaced Jordi Sànchez's traces with Sònia Urpí Garcia and gives no explanation as to why. Sònia Urpí Garcia also shows up in an unrelated Hungarian Journalist's forensics trace, Dániel Németh.

If this were a mistake, it should have been noted in Update history log at the bottom of Appendix E, but it was not. This undocumented change has compromised the integrity of the data, and it will be one of many critical changes in data Amnesty Tech will make.

Forensic traces for CATPO11 – Jordi Sànchez

This data was peer reviewed from Citizen Lab analysis.

Date (UTC)	Event
2020-06-22 06:13:43	Process: bh (WIFI IN: 0.00 MB, WIFI OUT: 0.00 MB, WWAN IN: 1.57 MB, WWAN OUT: 0.04 MB)
2020-06-22 06:14:10	Process: keybrd (WIFI IN: 0.98 MB, WIFI OUT: 3.66 MB, WWAN IN: 2.16 MB, WWAN OUT: 17.70 MB)
2020-06-22 14:53:08	Process: keybrd

Figure 2 April 19th, 2022 Jordi Sànchez Forensics Traces

Forensic traces for CATPO11 – Sònia Urpí Garcia

This data was peer reviewed from Citizen Lab analysis.

Date (UTC)	Event
2020-06-22 06:13:43	Process: bh (WIFI IN: 0.00 MB, WIFI OUT: 0.00 MB, WWAN IN: 1.57 MB, WWAN OUT: 0.04 MB)
2020-06-22 06:14:10	Process: keybrd (WIFI IN: 0.98 MB, WIFI OUT: 3.66 MB, WWAN IN: 2.16 MB, WWAN OUT: 17.70 MB)
2020-06-22 14:53:08	Process: keybrd

Figure 3 July 30th, 2022 Sònia Urpí Garcia Replaced Jordi Sànchez's Traces

2021-07-09 06:59:15	Process: keybrd (IN: 0Sònia Urpí Garcia.00 MB, OUT: 0.03 MB)
---------------------	---

Figure 4 Sònia Urpí Garcia Data Mixed with Hungarian Journalist Dániel Németh

False Positive Results

com.apple.CrashReporter.plist

3 of 4 Catalans verified by Amnesty were found to have the same indicator of compromise or IOC. The IOC is com.apple.CrashReporter.plist, and was reported to be a false positive by 6 people to which Amnesty conceded and removed it completely from a STIX2 file. The STIX2 file is used with Amnesty's

MVT-Tool to help match malicious indicators found on the device.

In laymen terms a STIX2 file is a bad keyword list. If any of the bad keywords are found in a backup of your iPhone Amnesty's software will tell you that you are possibly infected with spyware. The indicator **com.apple.CrashReporter.plist** has been listed as malicious since September 18th, 2021⁵⁷.

Table 3 Catalans found with com.apple.CrashReporter.plist as a malicious indicator of compromise

CATPOI4	Spain	Jordi Sánchez	2017-05-26 14:36:01	File Library/Preferences/com.apple.CrashReporter.plist created in RootDomain
CATPOI3	Spain	Elisenda Paluzie	2019-10-29 12:01:24	File Library/Preferences/com.apple.CrashReporter.plist created in RootDomain
CATPOI2	Spain	Meritxell Bonet	2019-06-04 18:18:49	File Library/Preferences/com.apple.CrashReporter.plist created in RootDomain

⁵⁷ <https://github.com/AmnestyTech/investigations/commit/e60689d9765f7402502dde66affb1755a5384b08>

False Positive Alert #1

July 20th, 2021 – July 21st, 2021 4
Users of Amnesty's MVT-Tool reported receiving a false positive result for com.apple.CrashReporter.plist in the HomeDomain. The 3 Catalans were found to have this malicious IOC in the RootDomain. Etienne Maynier of Amnesty Tech responded to the 4 users saying that com.apple.CrashReporter.plist in the HomeDomain *"can be linked to an attack if found with other evidences, but does not mean in itself that a phone is compromised, it can be created by legitimate processes"*⁵⁸
The significance of this statement is that Etienne Maynier (Github handle te-k) confirmed com.apple.CrashReporter.plist in the HomeDomain and in the RootDomain

can be malicious. There have never been any reports of an alleged infection with com.apple.CrashReporter.plist in the HomeDomain, but yet Amnesty has said if the IOC is found in the HomeDomain with other evidence it is part of an exploit chain. The other evidence Amnesty speaks about is never mentioned, and without any more information about this newly revealed malicious indicator of compromise a warning is added to the MVT-Tool code repository README.md file. *"Warning: the com.apple.CrashReporter.plist file listed here can be created by Pegasus but can also be legitimately created by the system during updates. Without additional indicators, it does not confirm the infection of a iPhone"*⁵⁹.

⁵⁸ <https://github.com/AmnestyTech/investigations/issues/8#issuecomment-884237762>

⁵⁹ https://github.com/AmnestyTech/investigations/blob/ba749a926cec4bf43920c9300922296689fdc57b/2021-07-18_nso/README.md

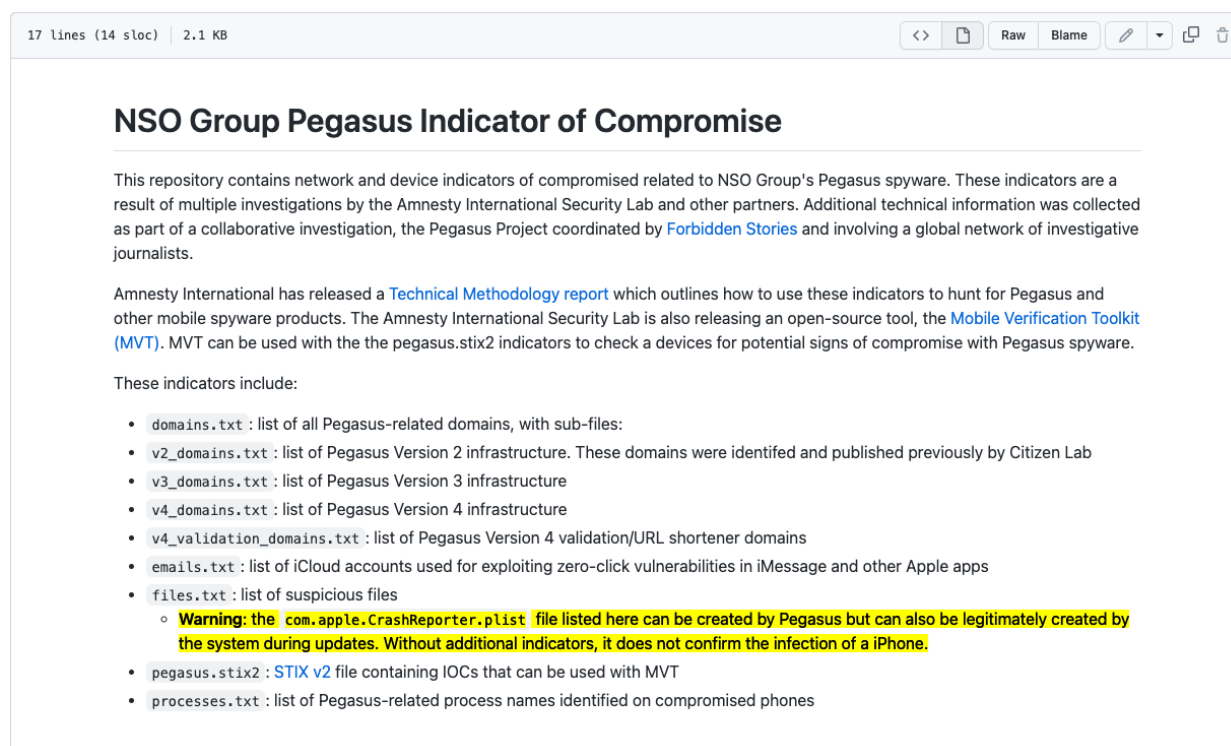


Figure 5 July 22, 2021 Amnesty Admits a False Positive Indicator with `com.apple.CrashReporter.plist`

Table 4 is a timeline of events⁶⁰ first reported false positive issues raised by users of the MVT-Tool. The IOC `com.apple.CrashReporter.plist` was not yet

removed from the STIX2 file during this timeline, and the result was a warning added by Etienne Maynier.

Table 4 Amnesty Tech Investigations Github Issue #8 Users Report `com.apple.CrashReporter.plist` as a false positive

Date	User	issue	Source
July 20th, 2021	joshhopkins	I'm assuming instances of <code>com.apple.CrashReporter.plist</code> in isolation isn't something to be too concerned about (using mtv-project and pegasus.stix2 indicators). Is it worth highlighting this in the output?	https://github.com/AmnestyTech/investigations/issues/8#issue-949322707

⁶⁰ <https://github.com/AmnestyTech/investigations/issues/8>

July 21st, 2021	cormacelf	I have this as well, it is a bplist file which looks like this when you convert to XML (plutil -convert xml1 80/80ef37a6dc6ae1caeffb16149342bd959a139c4f) gives a pretty mundane result.	https://github.com/AmnestyTech/investigations/issues/8#issuecomment-884126962
July 21st, 2021	Xenderblade	Same found also. What to expect?	https://github.com/AmnestyTech/investigations/issues/8#issuecomment-884207548
July 21st, 2021	AlexandreGohier	Same for me, slightly different dates:	https://github.com/AmnestyTech/investigations/issues/8#issuecomment-884232311
July 21st, 2021	Te-k (Etienne Maynier)	Yes, the file com.apple.CrashReporter.plist can be linked to an attack if found with other evidences, but does not mean in itself that a phone is compromised, it can be created by legitimate processes	https://github.com/AmnestyTech/investigations/issues/8#issuecomment-884237762
July 22st, 2021	Te-k (Etienne Maynier)	Warning added, thanks, I close this discussion	https://github.com/AmnestyTech/investigations/issues/8#issuecomment-884691768

I found that CrashReporter.plist was not only created during a system update as Etienne Maynier had stated, but it also came prepackaged in a Chinese Apple demo phone backup. In 2016 while researching, I download a file named “CN-si iPhone6sPlus v11.1.1.rar⁶¹.” After unpacking that .rar file,

a backup file system was presented and one of the files included was “80ef37a6dc6ae1caeffb16149342bd959a139c4f,” the same filename referenced by the MVT-Tool users that reported the false positive. After decoding the Manifest.mbdb the log output confirmed:

⁶¹ <https://www.pansoso.tv/file/15486750>

1. CN-si iPhone6sPlus v11.1.1/80ef37a6dc6ae1caeffb16149342bd959a139c4f
=(exists)=> Library/Preferences/com.apple.CrashReporter.plist
2. HomeDomain-Library/Preferences.

After discovering that CrashReporter.plist in the HomeDomain could be found in a pre-packaged backup used for a demo phone the scenario in which a false positive could be obtained increased.

False Positive Alert #2

The second alert of com.apple.CrashReporter.plist was made on July 27th, 2021. This user is an iOS developer and states that merely searching for the text com.apple.CrashReporter.plist when using the STIX2 file or bad keyword list shows a false positive result. The user says, **“This raises a false flag on any iPhone used for normal iOS development”** The iOS developer suggests that instead of just

looking for a bad keyword, Amnesty should be reading the content of the file, and creating logic to determine if that file is actually malicious.

Etienne Maynier response to the developer saying that Amnesty does not read the content of the file, and if com.apple.CrashReporter.plist is found in the manifest then it is malicious. Etienne says the developer is correct in saying a false positive can be found, but they are going to keep the indicator com.apple.CrashReporter.plist in the STIX2 file because it can be valuable.

After a 5th person has tried to tell Amnesty searching for a bad keyword is delivering false positive results there was still no action taken.

Table 5 Amnesty Tech Investigations #19 False Indication of Pegasus com.apple.CrashReporter.plist

Date	User	issue	Source
July 27th, 2021	rick-rheo	<p>For Pegasus detection (pegasus.stix2) the scan considers the mere presence of Library/Preferences/com.apple.CrashReporter.plist to be an indication of infection. This raises a false flag on any iPhone used for normal iOS development. You're looking for</p> <pre><key>ShouldSubmit</key> <false/></pre> <p>in the contents of that file as a more accurate indicator of Pegasus infection. If the above is</p> <pre><key>ShouldSubmit</key> <true/></pre> <p>that is normal for any iOS developer's iPhone.</p>	https://github.com/AmnestyTech/investigations/issues/19#issue-954044724
July 28th, 2021	Te-k (Etienne Maynier)	<p>Hi,</p> <p>This is indeed correct, but mvt does not check the content of the file, it only relies on the manifest file, so we have decided to keep this indicator that can be valuable and add a note in the IOC page</p>	https://github.com/AmnestyTech/investigations/issues/19#issuecomment-888179856

False Positive Alert #3

July 28th, 2021 Amnesty is alerted again of a false positive in `com.apple.CrashReporter.plist`. The user alerting states that the code `Manifest.py` is specifically checking for `com.apple.CrashReporter.plist` in the `RootDomain`, but when checking for malicious Pegasus indicators with the STIX2 file `com.apple.CrashReporter.plist` will be detected as a positive match for infection in **any domain**.

Claudio Guarnieri⁶² Head of Amnesty's Security Lab concedes, and says *"You are right. This file should not have ended up in the indicators list, we will have that mistake corrected."*

Reading further into Amnesty's methodology, they do not know why `com.apple.CrashReporter.plist` was written in `/private/var/root/Library/Preferences/` and they assume the file is written *"likely to disable reporting of crash logs back to Apple"*⁶³

Table 6 Amnesty Tech Investigations #130 False Positive `com.apple.CrashReporter.plist`

Date	User	issue	Source
July 28th, 2021	gregzo	<p><code>check_indicators</code> in <code>Manifest.py</code> explicitly checks for <code>com.apple.CrashReporter.plist</code> in the <code>RootDomain</code>. Just below,</p> <p><code>self.indicators.check_file(result["relativePath"]):</code> will result in <code>com.apple.CrashReporter.plist</code> to be detected as a positive match in any domain if loading the latest STIX from the investigations repo</p> <p>On some of our devices, this results in what we believe is a false positive</p> <p>on <code>Library/Preferences/com.apple.CrashReporter.plist</code> in the <code>HomeDomain</code>. The file was seemingly created</p>	<p>https://github.com/mvt-project/mvt/issues/130#issue-954934605</p>

⁶² https://rocketreach.co/claudio-guarnieri-email_40587702

⁶³ <https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/#h-2-1-additional-suspicious-processes-following-bridgehead>

		and last modified in February 2014, and can be found on 2 devices. Contents:	
July 28th, 2021	botherder (Claudio Guarnieri)	You are right. This file should not have ended up in the indicators list, we will have that mistake corrected.	https://github.com/mvt-project/mvt/issues/130#issuecomment-888443325

Falsifying com.apple.CrashReporter.plist

One of the most basic steps in digital forensics is hashing the data. Interpol Guidelines for Digital Forensics First Responders, Section 4.3 HASH function⁶⁴ states, *“The HASH function or summary function is used to verify the integrity of a data set. In other words, it is about obtaining its “fingerprint”. In the case of electronic evidence, this procedure is applied when making copies of the original devices, so that, once the HASH value of the origin and destination has been calculated, they must be identical. This process is known as verification.”* The MVT-Tool for iOS has very specific capabilities and taking the

I made a quick encrypted backup from an iPhone 6s, iOS 15.7, serial F17QL8LNGRY7. I used the MVT-Tool to decrypt the backup and sent the decrypted

backup of the device is not one of them. Without having the physical mobile device in a secured facility, Amnesty and The Citizen Lab are examining backups that do not have a hash that can be used to check against tampering. After reading the MVT-Tool code I could see that Amnesty was only checking the Manifest.db file that is included in the device backup when it is looking for com.apple.CrashReporter.plist. The code is only checking for the domain which would be RootDomain or HomeDomain, and the relativePath which means if the domain is set to RootDomain the relativePath would only need to be com.apple.CrashReporter.plist. files into a folder I named “decrypted.” Next, I added a record to the Manifest.db file manually by opening it with DB Browser for SQLite (MacOS application).

⁶⁴ https://www.interpol.int/content/download/16243/file/Guidelines%20to%20Digital%20Forensics%20First%20Responders_V7.pdf [pg.22 § 2]

Figure 6

	fileID	domain	relativePath	flags	file
	Filter	Filter	Filter	Filter	Filter
3022	064d76faeef55598c754d5f4af2f8903229ee889	HomeDomain	Library/BulletinBoard/VersionedSectionInfo.plist	1	BLOB
3023	0fb54654b97099d34461570fab859a2b0570ed1f	HomeDomain	Library/Preferences/com.apple.BTServer.plist	1	BLOB
3024	ca5806ee855e6ef59e9d103a9898ae5b395684a2	HomeDomain	Library/Preferences/com.apple.GEO.plist	1	BLOB
3025	03d7c2ff408d6eaf6e0231d8e48231665902e1	WirelessDomain	Library/Preferences/...	1	BLOB
3026	fe915bffc3ee1f68e22bf2811b5dbbb90bf2a0f	HomeDomain	Library/Preferences/com.apple.asd.plist	1	BLOB
3027	cfa63c2cb0fd80843034e75395ea3be8d1ba6529	HomeDomain	Library/Preferences/com.apple.apsd.plist	1	BLOB
3028	61cd6b3cb447bde009dbd8ed1ea214a1d67dd3	HomeDomain	Library/Preferences/com.apple.assetsd.plist	1	BLOB
3029	61e1e4600e3997adbadda920ade1321e753b2b17	HomeDomain	Library/Preferences/com.apple.aggregated.plist	1	BLOB
3030	7ff7fe545440ab72b1570232d0ed81b84a5334dd	HomeDomain	Library/Preferences/com.apple.MobileSMS.plist	1	BLOB
3031	d697ba78ee5f7fb2f5b869048e79abc4674b7084	HomeDomain	Library/Preferences/com.apple.inCallService.plist	1	BLOB
3032	77e6b5a266733afee2b16119ec40f2164639ab21	SysSharedContainerDomain-...	Library/ConfigurationProfiles/PublicInfo/MCMeta.plist	1	BLOB
3033	c857040ce4ce8654af495a2f04da92a0a5111fac	SysSharedContainerDomain-...	Library/ConfigurationProfiles/UserSettings.plist	1	BLOB
3034	5cebe8d5fd04c62f08b22dd14225a956bf2819b8	AppDomainPlugin-com.apple.FileProvider.LocalStorage	Library/Preferences/com.apple.FileProvider/...	1	BLOB
3035	9c46fd950cb447d02fb55f6bf00251032bda8b4	SysSharedContainerDomain-...	Library/ConfigurationProfiles/MCSettingsEvents.plist	1	BLOB
3036	4800b8726fbd1a324c181bd735d6457f3ced7cc	AppDomain-com.apple.mobilemail	Library/Preferences/com.apple.mobilemail.plist	1	BLOB
3037	8e7f26685d92296da2100cfaf98173f45da1ce88	SysSharedContainerDomain-...	Library/ConfigurationProfiles/PayloadManifest.plist	1	BLOB
3038	e23c4fcbad929e7ae7078da2c19849d4311c0a15	HomeKitDomain	Library/homed/plain-metadata.config	1	BLOB
3039	4bf2c57686ace66ebb9a7edaf27a5f59631b5f4	SysSharedContainerDomain-...	Library/ConfigurationProfiles/PublicInfo/...	1	BLOB
3040	005cc965864ad5e6a4da3b1296509c0fbf7e5f37	AppDomainPlugin-com.apple.news.widget	Library/Preferences/com.apple.news.widget.plist	1	BLOB
3041	b2998988ede72dc5ec6d24d258f060d2b2e961b1	SysSharedContainerDomain-...	Library/ConfigurationProfiles/ProfileTruth.plist	1	BLOB
3042	ed1f8fb5a948b40504c19580a458c384659a605e	WirelessDomain	Library/Databases/CellularUsage.db	1	BLOB
3043	550a09c4f8c4d89df203ab615ffc979d3c56f613	SysSharedContainerDomain-...	Library/ConfigurationProfiles/Client Truth.plist	1	BLOB
3044	8d0167b67f664a3816b4c00115c2dfa6a8f81388	WirelessDomain	Library/Preferences/...	1	BLOB
3045	e2de31866e030d913242400a88f3293d4d740d28	HomeKitDomain	Library/homed/datastore3.sqlite	1	BLOB
3046	ebb20ff73819feef8b7b15ce2bde7295699ad3e	HomeKitDomain	Library/homed/datastore.sqlite	1	BLOB
3047	864b5bb8118e317b7457c179193a9db3b5e9a366	AppDomainGroup-group.com.apple.Maps	Maps/MapsSync_0.0.1_deviceLocalCache.db	1	BLOB
3048	5fe47b24af1681316db428b3b4e8108211665830	SysSharedContainerDomain-...	Library/ConfigurationProfiles/...	1	BLOB
3049	51a4616e576dd33cd2abadfea874eb8ff246bf0e	KeychainDomain	keychain-backup.plist	1	BLOB
3050	0d609c54856a9bb2d56729df1d68f2958a88426b	WirelessDomain	Library/Databases/DataUsage.sqlite	1	BLOB
3051	181c97b0ca7212a1a2910ab5e954686a9062c3b3	AppDomainGroup-group.com.apple.Maps	Maps/MapsSync_0.0.1	1	BLOB
3052	cf15234871aff119d2c4f4418a69a3390a5e823a	SysSharedContainerDomain-...	Documents/BLDatabaseManager/...	1	BLOB
3053	1e6c0783f9b33d00b152067a0661c8fc8841073f	SysSharedContainerDomain-...	Library/ConfigurationProfiles/...	1	BLOB
3054	NULL	RootDomain	com.apple.CrashReporter.plist	1	

Figure 6 Forging com.apple.CrashReporter.plist

I ran the following command “mv-ios check-backup decrypt/” and alas, I had infected myself with com.apple.CrashReporter.plist. There were no integrity checks to ensure the manifest did not contain an extra record, a hash of the database was not made during the initial

decryption, and I knew that I had full reign to spoof any indicator of compromise I wanted. If you notice in Figure 7, com.apple.CrashReporter.plist is in the RootDomain, something that only Amnesty and Citizen Lab say only Pegasus can achieve.

Figure 7

```

INFO      [mvt.ios.modules.backup.manifest] Running module Manifest...
INFO      [mvt.ios.modules.backup.manifest] Found Manifest.db database
          at path: decrypt/Manifest.db
20:20:12 INFO      [mvt.ios.modules.backup.manifest] Extracted a total of 3054
          file metadata items
WARNING   [mvt.ios.modules.backup.manifest] Found a potentially
          suspicious "com.apple.CrashReporter.plist" file created in
          RootDomain

```

Figure 7 Manifest.db tampering, inserting a record to spoof a spyware infection with com.apple.CrashReporter.plist

Nullification

Explaining how I forged com.apple.CrashReporter.plist was necessary, as the forgery will be used as supporting evidence in this section of the report. After Claudio Guarnieri agreed to remove com.apple.CrashReporter.plist from the STIX2 bad keyword list, Etienne Maynier committed a change to the code repository and made a code comment saying, “*Remove a file that creates false positive*”⁶⁵. The consequence of removing the file

com.apple.CrashReporter.plist because it creates a false positive regressively nullified every case that included com.apple.CrashReporter.plist before Jan 12th, 2022 (version 1.4.2⁶⁶ of MVT-Tool). The indicator that was removed contained a pattern prefix “file:name” that the MVT-Tool uses to match what the program has found internally to the STIX2 bad keyword list or so they thought.

```

{
    "type": "indicator",
    "spec_version": "2.1",
    "id": "indicator--8180affb-110d-435e-89b8-dd4a56c9211f",
    "created": "2021-07-18T14:59:48.38858Z",
    "modified": "2021-07-18T14:59:48.38858Z",
    "indicator_types": [
        "malicious-activity"
    ],
    "pattern": "[file:name='com.apple.CrashReporter.plist']",
    "pattern_type": "stix",
    "pattern_version": "2.1",
    "valid_from": "2021-07-18T14:59:48.38858Z"
},

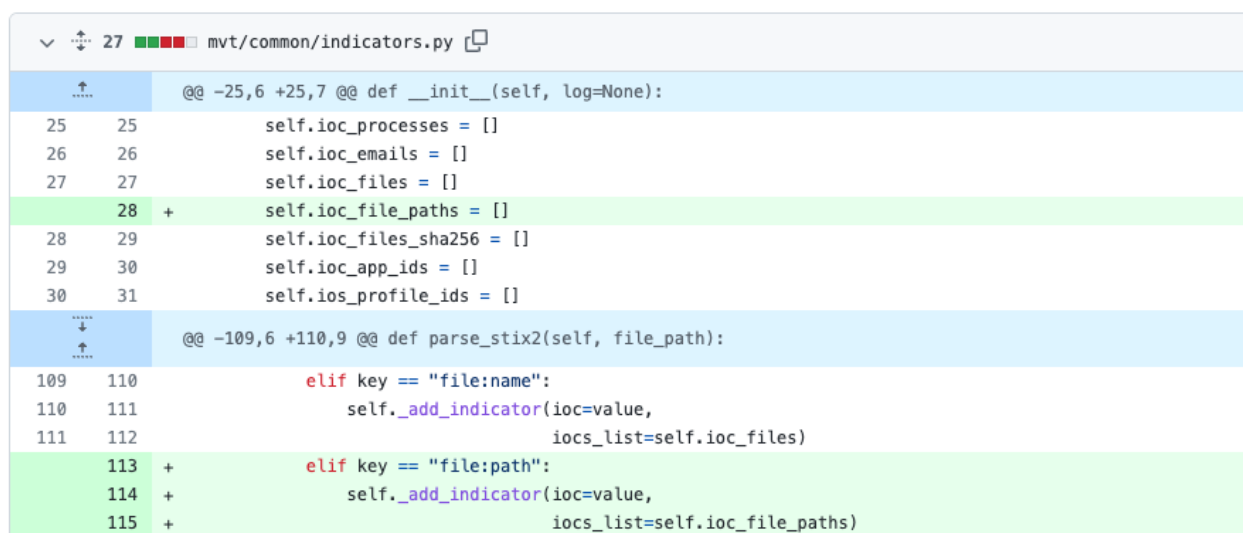
```

⁶⁵ <https://github.com/AmnestyTech/investigations/commit/928ea5a820df6596762241da147b5afa1458b5ee>

⁶⁶ <https://github.com/mvt-project/mvt/releases/tag/v1.4.2>

When Amnesty removed the false positive indicator `com.apple.CrashReporter.plist` July 28th, 2021 from the STIX2 file, they removed the only way to check for `com.apple.CrashReporter.plist` in the RootDomain and the HomeDomain. In simpler terms, if Amnesty were to recheck all

of the people they said were infected with `com.apple.CrashReporter.plist`, 100% would come back negative or not infected with `com.apple.CrashReporter.plist`. It would not be until almost 6 months later January 20th, 2022 when Amnesty would write the code that does not require a STIX2 file to check for `com.apple.CrashReporter.plist`⁶⁷.



```

27 mvt/common/indicators.py
@@ -25,6 +25,7 @@ def __init__(self, log=None):
25     self.ioc_processes = []
26     self.ioc_emails = []
27     self.ioc_files = []
28 +     self.ioc_file_paths = []
28     self.ioc_files_sha256 = []
29     self.ioc_app_ids = []
30     self.ios_profile_ids = []

@@ -109,6 +110,9 @@ def parse_stix2(self, file_path):
109     elif key == "file:name":
110         self._add_indicator(ioc=value,
111                             iocs_list=self.ioc_files)
113 +     elif key == "file:path":
114 +         self._add_indicator(ioc=value,
115                             iocs_list=self.ioc_file_paths)

```

Figure 8 Jan 20th, 2022 Amnesty writes the code to detect `com.apple.CrashReporter.plist` without the needs of a STIX2 file, but the damage has already been done

⁶⁷ <https://github.com/mvt-project/mvt/commit/083bc12351eac43a1be4f7473e87400e8e4c3b52>

Confirming The Nullification

To confirm that Amnesty had nullified victims with the IOC com.apple.CrashReporter.plist, I manually checked 26 versions of the MVT-Tool and used my forged Manifest.db backup as the

control. 26 versions of the MVT-Tool did not show any signs of infection, when checking against my forged Manifest.db. It was not until MVT-Tool Version 1.4.2 that my forged Manifest.db showed signs of infection.

Table 7 MVT-Tool Versions Checked with Forged Manifest.db

MVT-Version	Release Date	Confirmed infection with forged Manifest.db
v1.0.11	Jul 20, 2021	no
v1.0.13	Jul 27, 2021	no
v1.0.14	Jul 31, 2021	no
v1.0.15	Aug 1, 2021	no
v1.0.16	Aug 5, 2021	no
v1.0.17	Aug 6, 2021	no
v1.1.0	Aug 12, 2021	no
v1.2.0	Aug 16, 2021	no
v1.2.1	Aug 18, 2021	no
v1.2.2	Aug 25, 2021	no
v1.2.3	Aug 25, 2021	no
v1.2.5	Aug 26, 2021	no
v1.2.6	Sep 2, 2021	no
v1.3	Sep 2, 2021	no
v1.2.7	Sep 14, 2021	no
v1.2.8	Sep 16, 2021	no
v1.2.9	Sep 22, 2021	no
v1.2.11	Oct 14, 2021	no
v1.2.12	Oct 18, 2021	no
v1.2.10	Oct 23, 2021	no
v1.2.13	Oct 23, 2021	no
v1.2.14	Oct 30, 2021	no

v1.3.1	Dec 16, 2021	no
v1.3.2	Dec 17, 2021	no
v1.4.0	Dec 17, 2021	no
v1.4.1	Dec 27, 2021	no
v1.4.2	Jan 12, 2022	yes

Global Impact of Non-Disclosure

Amnesty conceded and removed com.apple.CrashReporter.plist, and declared that it was a false positive result when found in the HomeDomain. When Amnesty removed this IOC from the STIX2 file they also removed any way to forensically confirm their findings of a malicious trace found with com.apple.CrashReporter.plist in the RootDomain of a backup. The method

that was once used to confirm the infection would have no longer existed. The self-nullification by way of IOC removal negates any claims of a Pegasus spyware infection associated to com.apple.CrashReporter.plist. The following table represents everyone that Amnesty International had associated with the IOC com.apple.CrashReporter.plist.

Table 8 Alleged Pegasus Victims said to be infected by com.apple.CrashReporter.plist - Their results have been nullified by Amnesty International

ID	Country	Name	Date
PLPOI4	Poland	Andrzej Długosz	2018-11-22 11:56:07
PLPOI3	Poland	Pawel Tamborski	2018-04-05 6:44:30
INHRL1	India	Jagdeep Singh	2019-07-07 7:33:51
INHRD2	India	Rona Wilson	2018-03-29 6:19:54
INHRD2	India	Rona Wilson	2017-07-05 14:24:46
HUJRN1	Hungary	No Information Provided	No Information Provided
HUJRN3	Hungary	Brigitta Csikász	2019-04-05 11:06:41
HUJRN3	Hungary	Brigitta Csikász	2019-04-05 11:06:39
FRPOI6	France	Arnaud Montebourg	2019-09-01 20:24:41
CATPOI4	Spain	Jordi Sánchez	2017-05-26 14:36:01
CATPOI3	Spain	Elisenda Paluzie	2019-10-29 12:01:24

CATPOI2	Spain	Meritxell Bonet	2019-06-04 18:18:49
BHHRD	Bahrain	Ebtisam al Saegh	2019-08-08 8:45:12
AZHRL1	Azerbaijan	Asabali Mustafayev	2019-04-29 6:11:50
AZHRL1	Azerbaijan	Asabali Mustafayev	2019-03-28 7:43:14
AZJRN2	Azerbaijan	Sevinc Vaqifqizi	2019-04-17 10:53:04
AZJRN3	Azerbaijan	Aziz Orujov	2019-06-21 15:47:28
FRHRL1	France	Joseph Breham	2019-10-29 9:05:08
FRHRL2	No Information Provided	No Information Provided	2019-06-13 14:03:23
FRJRN1	France	Lenaig Bredoux	2019-10-10 12:39:17
FRJRN2	France	No Information Provided	2019-08-16 12:37:55
FRJRN3	France	Edwy Plenel	2019-07-05 11:23:29
FRJRN4	France	Bruno Delport	2019-07-05 13:21:47
FRJRN4	France	Bruno Delport	2019-07-05 13:21:53
FRJRN5	No Information Provided	No Information Provided	2019-08-19 9:20:01
HUJRN1	Hungary	András Szabó	2019-06-13 11:15:40
HUJRN2	Hungary	Szabolcs Panyi	2019-04-04 5:33:02
HUPOI1	No Information Provided	No Information Provided	2018-06-21 7:02:55
HUPOI2	Hungary	Adrien Beauduin	2018-12-19 9:13:48
INHRD1	India	SAR Geelani	2019-01-25 7:33:59
INHRD1	India	SAR Geelani	2019-01-25 7:34:08
INHRD1	India	SAR Geelani	2019-01-26 14:16:19
INJRN3	India	SNM Abdi	2019-04-02 4:51:19
INJRN4	India	Siddharth Varadarajan	2018-04-27 4:41:37
INJRN5	India	Paranjay Guha Thakurta	2018-07-25 3:58:42
KASH01	Saudi Arabia	Hatice Cengiz	2018-10-06 0:33:28
KASH03	Saudi Arabia	Wadah Khanfar	2019-11-02 17:19:29
Not Provided	Morocco	Omar Radi	2019-02-11 14:45:54

Knowingly withholding information from world governments pertaining to the discovery of a false positive indicator is common practice for Amnesty and Citizen Lab. July 19th, 2021 Etienne Maynier removed an indicator of compromise without any reasoning other than “removing false positive⁶⁸” The indicator removed for reason of a false positive was `com.apple.softwareupdateservicesd.plist`. The removal of this indicator impacted the forensics traces of 2 individuals Omar Radi

and Claude Mangin. Omar Radi is a convicted spy and rapist and is serving 6 years in prison for his crimes⁶⁹. Amnesty has been advocating for his release since 2020 stating that he has been spied on with NSO Pegasus spyware deployed by the Moroccan government⁷⁰. The Moroccan government has repeatedly denied the use of Pegasus spyware, and the revelation of a false positive found in the case of Omar Radi makes a stronger argument against their accusers at Amnesty International.

Table 9 False Positive Indicator Found com.apple.softwareupdateservicesd.plist, Morocco & France

ID	Country	Name	Date	Event
Not Provided	Morocco	Omar Radi	2019-09-13 17:02:35	<code>com.apple.softwareupdateservicesd.plist</code>
FRHRD1	France	Claude Mangin	2020-10-08 8:40:42	<code>com.apple.softwareupdateservicesd.plist</code>

⁶⁸ <https://github.com/AmnestyTech/investigations/commit/1c694217c3efb4e40f34822b6cf99a7b5bd8a064>

⁶⁹ <https://www.africanews.com/2021/07/20/morocco-prominent-journalist-omar-radi-sentenced-to-6-years-in-prison/>

⁷⁰ <https://www.amnesty.org/en/latest/news/2022/03/morocco-authorities-must-ensure-omar-radis-fair-trial-rights/>

July 22nd, 2021 Etienne Maynier removed another false positive indicator “Diagnosticd.” The removal of the indicator of compromise and its non-disclosure by Amnesty and The Citizen Lab has materially impacted The Republic of Rwanda, and

illicitly been withheld from The United States Congress. The European Parliament adopted a motion against Rwanda for the alleged spying of Carine Kanimba, and MEPs were never made aware of the false positive indicator that had been found in her case.

Table 10 False Positive Indicator Found Case of Carine Kanimba, Rwanda

July 18th, 2021	Carine Kanimba’s mobile forensics report is released to the public by Amnesty International and confirmed by The Citizen Lab ⁷¹
July 21st, 2021	A false positive indicator in Carine Kanimba’s forensics report was found by mobile security research firm ZecOps ⁷²
July 22nd, 2021	Amnesty Tech removes the false positive indicator from their code base, but Carine Kanimba’s forensics report never changes and there is no public statement stating the results of the forensics report are false. ⁷³
October 6th, 2021	The European Parliament proposes a Joint Motion for Resolution in regards to the Pegasus phone hacking of Carine Kanimba ⁷⁴
October 7th, 2021	The European Parliament adopts the Motion for Resolution and rules against Rwanda for the Pegasus phone hacking of Carine Kanimba. The false positive indicator was still never mentioned during this resolution against Rwanda ⁷⁵
November 4th, 2021	Amnesty Tech puts back the false positive indicator stating that they accidentally removed it ⁷⁶

Rwanda, Morocco/Western Sahara, and Kazakhstan would all be impacted by the removal of this false positive, and their governments would never be made aware. Kazakhstan publicly denied the use of

Pegasus spyware calling it claims without evidence⁷⁷. Rwanda firmly denies the use of Pegasus spyware and calls the claims a smear campaign⁷⁸.

⁷¹ <https://www.amnesty.org/en/documents/doc10/4487/2021/en/> [pg. 22-26,78-81]

⁷² <https://twitter.com/ZecOps/status/1417849130118877185?s=20&t=BU4EZ73lsZsIRpRNOFUKsA>

⁷³ <https://github.com/AmnestyTech/investigations/commit/ba749a926cec4bf43920c9300922296689fdc57b>

⁷⁴ https://www.europarl.europa.eu/doceo/document/RC-9-2021-0500_EN.pdf [pg. 5]

⁷⁵ https://www.europarl.europa.eu/doceo/document/TA-9-2021-0418_EN.pdf

⁷⁶ <https://github.com/AmnestyTech/investigations/commit/6914279c3c3226c2e88a28f0fb008ef9bc4bc8e5>

⁷⁷ <https://www.newarab.com/news/kazakhstan-says-pegasus-spy-claims-without-evidence>

⁷⁸ <https://apnews.com/article/technology-africa-genocides-rwanda-72ecb6eb631c021004c3a017e7aeb2ce>

Table 11 Full List of people affected by the false positive indicator Diagnosticd

ID	Country	Name	Date	Event
KZHRD2	Kazakhstan	Dimash Alzhanov	2021-06-26 2:56:58	Diagnosticd
KZHRD3	Kazakhstan	Aizat Abilseit	2021-06-09 3:29:18	Diagnosticd
KZHRD4	Kazakhstan	Darkhan Sharipov	2021-06-24 6:52:53	Diagnosticd
WSHRD1	Morocco/Western Sahara	Mahjoub Mleiha	2021-01-29 13:17:06	Diagnosticd
RWHRD1	Rwanda	Carine Kanimba	2021-01-28 22:42:56	Diagnosticd

July 21st, 2021 Etienne Maynier merges a commit from user secure411dotorg stating “Removing a dyndns base domain with hundreds of thousands of non-NSO URLs⁷⁹.”

February 1st, 2022 Etienne Maynier removed 35,992 false positive indicators that Amnesty had attributed to the NSO Group⁸⁰. There is a clear lack of due diligence, knowledge of the subject matter, and refusal

to disclose errors in research. After thoroughly studying Amnesty’s forensics methodology I have concluded that their method is not sound, and all of the indicators of compromise associated to a forensics trace can easily be forged. Without chain of custody documentation, detailed written procedure, and a truly impartial review performed by several sources, all of Amnesty International’s claim fail.

⁷⁹ <https://github.com/AmnestyTech/investigations/pull/10>

⁸⁰ <https://github.com/AmnestyTech/investigations/commit/2f9d4e4ae55f0905ea0357dac30c1ff9a040682b>

Forging All IOCs

Amnesty has a list of Pegasus IOCs, and specifically processes that they deem to be malicious. I have taken the process.txt list, created a CSV file⁸¹, and inserted this list into DataUsage.sqlite. The DataUsage database is one of the main sqlite files MVT-Tool

checks for malicious indicators of compromise. Knowing that none of the database files are hashed, we will easily be able to add records and generate false positive results when running a backup through the MVT-Tool.

1. brew install sqlite
2. mkdir POC
3. cd POC
4. Download the ZPROCESS_2.csv from https://github.com/jonathandata1/Pegasus-CatalanGate-False-Positives/blob/main/IOC_CSV/ZPROCESS_2.csv
5. mkdir decrypted
6. mkdir results
7. idevicebackup2 backup encryption on 123
8. idevicebackup2 backup --full .
 - a. The backup will create a folder similar to this
a46e61b9b29bd67a677d0ee635fa1fa59316bdaf
9. mvt-ios decrypt-backup -p 123 -d decrypted/
a46e61b9b29bd67a677d0ee635fa1fa59316bdaf/
10. During the decryption process you are going to notice this in your terminal
 - a. INFO [mvt.ios.decrypt] Decrypted file Library/Databases/DataUsage.sqlite [WirelessDomain] to
decrypted/0d/0d609c54856a9bb2d56729df1d68f2958a88426b
 - b. Note: Decrypted/0d/ = file path
 - c. Note: 0d609c54856a9bb2d56729df1d68f2958a88426b = DataUsage.sqlite
11. cd 0d

⁸¹ CSV File can be found on https://github.com/jonathandata1/Pegasus-CatalanGate-False-Positives/tree/main/IOC_CSV

12. sqlite3 0d609c54856a9bb2d56729df1d68f2958a88426b ".import --csv
 ../../ZPROCESS_2.csv ZPROCESS"
13. cd –
 - a. this will take you back to the main dir
14. mvt-ios check-backup -o results/ decrypted/

```

WARNING [mvt.ios.modules.mixed.net_datausage] Found a known suspicious process name "CommsCenterRootHelper" matching
indicators from "Pegasus"
WARNING [mvt.ios.modules.mixed.net_datausage] Found a known suspicious process name "Diagnostic-2543" matching indicators from
"Pegasus"
WARNING [mvt.ios.modules.mixed.net_datausage] Found a known suspicious process name "Diagnosticd" matching indicators from
"Pegasus"
WARNING [mvt.ios.modules.mixed.net_datausage] Found a known suspicious process name "Diagnostics-2543" matching indicators
from "Pegasus"
WARNING [mvt.ios.modules.mixed.net_datausage] Found a known suspicious process name "GoldenGate" matching indicators from
"Pegasus"
WARNING [mvt.ios.modules.mixed.net_datausage] Found a known suspicious process name "JarvisPluginMgr" matching indicators from
"Pegasus"
WARNING [mvt.ios.modules.mixed.net_datausage] Found a known suspicious process name "MobileSMSd" matching indicators from
"Pegasus"
WARNING [mvt.ios.modules.mixed.net_datausage] Found a known suspicious process name "PDPDialogs" matching indicators from
"Pegasus"
WARNING [mvt.ios.modules.mixed.net_datausage] Found a known suspicious process name "ReminderIntentsUIExtension" matching
indicators from "Pegasus"
WARNING [mvt.ios.modules.mixed.net_datausage] Found a known suspicious process name "accountpfd" matching indicators from
"Pegasus"
WARNING [mvt.ios.modules.mixed.net_datausage] Found a known suspicious process name "actmanaged" matching indicators from
"Pegasus"
WARNING [mvt.ios.modules.mixed.net_datausage] Found a known suspicious process name "aggregatenotd" matching indicators from
"Pegasus"
WARNING [mvt.ios.modules.mixed.net_datausage] Found a known suspicious process name "appccntd" matching indicators from
"Pegasus"
WARNING [mvt.ios.modules.mixed.net_datausage] Found a known suspicious process name "bfrgbd" matching indicators from
"Pegasus"
WARNING [mvt.ios.modules.mixed.net_datausage] Found a known suspicious process name "bh" matching indicators from "Pegasus"
WARNING [mvt.ios.modules.mixed.net_datausage] Found a known suspicious process name "bluetoothfs" matching indicators from
"Pegasus"
WARNING [mvt.ios.modules.mixed.net_datausage] Found a known suspicious process name "boardframed" matching indicators from
  
```

Figure 9 Result of Forging IOCS

Forging Processes

All of the Catalangate victims Amnesty International confirmed have processes as indicators of compromise in common. I have run a proof of concept from the method previously described that shows all Catalangate victims can have their indicators easily forged. Proof of concepts such as these are essential to run before presenting scientific data.

Sònia Urpí Garcia (CATPOI1)

Table 12 Sònia Urpí Garcia All Pegasus indicators can be forged

Date (UTC)	Event	Action
2020-06-22 6:13:43	Process: bh (WIFI IN: 0.00 MB, WIFI OUT: 0.00 MB, WWAN IN: 1.57 MB, WWAN OUT: 0.04 MB)	Forgery Proof of Concept completed ⁸²
2020-06-22 6:14:10	Process: keybrd (WIFI IN: 0.98 MB, WIFI OUT: 3.66 MB, WWAN IN: 2.16 MB, WWAN OUT: 17.70 MB)	Forgery Proof of Concept completed
2020-06-22 14:53:08	Process: keybrd	Forgery Proof of Concept completed

Meritxell Bonet (CATPOI2)

Date (UTC)	Event	Action
2019-06-04 18:33:48	Process: roleaccountd (IN: 0.01 MB, OUT: 0.00 MB)	Forgery Proof of Concept completed
2019-06-04 18:33:51	Process: stagingd (IN: 1.46 MB, OUT: 0.07 MB)	Forgery Proof of Concept completed
2019-06-04 18:34:16	Process: logseld (WIFI IN: 4.70 MB, WIFI OUT: 18.68 MB, WWAN IN: 3.28 MB, WWAN OUT: 13.54 MB)	Forgery Proof of Concept completed
2019-06-06 9:39:11	Process: logseld	Forgery Proof of Concept completed

Elisenda Paluzie (CATPOI3)

Date (UTC)	Event	Action
2019-10-29 12:01:22	Process: bh (IN: 1.51 MB, OUT: 0.05 MB)	Forgery Proof of Concept completed
2019-10-29 12:01:35	Process: bh	Forgery Proof of Concept completed
2019-10-29 12:01:44	Process: locserviced (IN: 1.73 MB, OUT: 15.93 MB)	Forgery Proof of Concept completed
2019-10-29 17:49:43	Process: locserviced	Forgery Proof of Concept completed

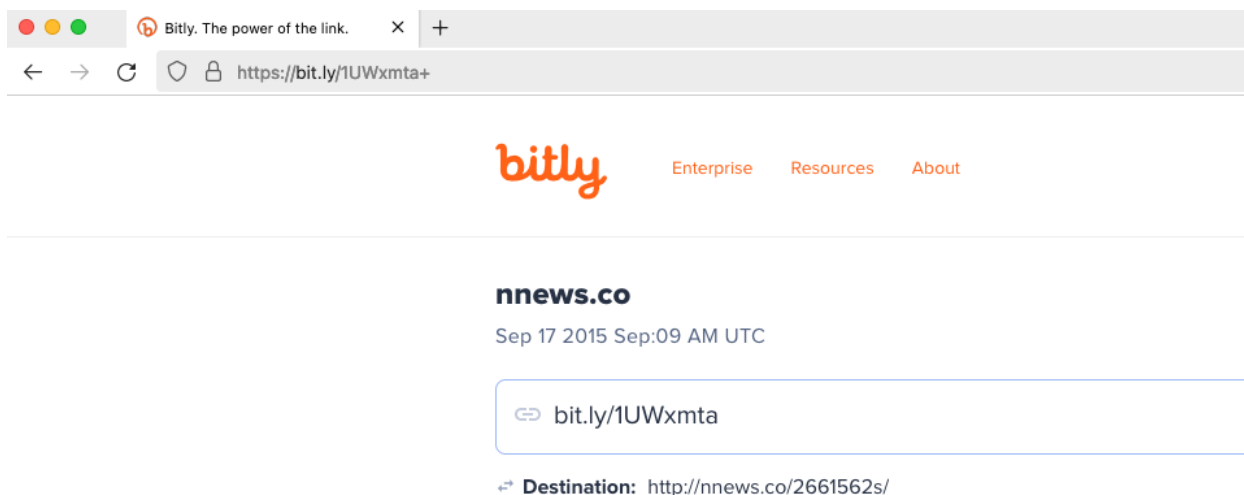
⁸² https://github.com/jonathandata1/Pegasus-CatalanGate-False-Positives/tree/main/Forged_Catalangate_data/processes
Proof of Concept for all 4 Catalan Process forgeries can be found in this repository

Jordi Sànchez (CATPOI4)

Date (UTC)	Event	Action
2017-05-26 14:37:10	Process: pcsd (IN: 12.18 MB, OUT: 164.00 MB)	Forgery Proof of Concept completed
2017-09-11 8:28:19	Process: pcsd	Forgery Proof of Concept completed
2017-09-15 13:11:13	Process: GoldenGate (IN: 3.52 MB, OUT: 0.02 MB)	Forgery Proof of Concept completed
2017-10-13 13:34:57	Process: pcsd (IN: 2.12 MB, OUT: 43.98 MB)	Forgery Proof of Concept completed
2017-10-13 21:47:50	Process: pcsd	Forgery Proof of Concept completed

Jordi Sànchez Text Discrepancy

A well-known fact about bit.ly short URLs is that their metadata can be easily accessed by simply typing a plus sign (+) after the URL. Using the bit.ly metadata, I found that 3 of 5 text messages links Jordi received were created after the time Amnesty marked. 2 of the bit.ly links were created almost 2 hours after Amnesty claimed Jordi received the text. For Amnesty and The Citizen Lab did not have caught this discrepancy speaks to their lack of rigor when presenting such essential data to the world.



The screenshot shows a web browser window with the Bitly logo and navigation links (Enterprise, Resources, About). The main content area displays the Bitly link 'bit.ly/1UWxmta' with a metadata box showing the destination URL: 'http://nnews.co/2661562s/'. The browser's address bar shows the URL 'https://bit.ly/1UWxmta+'.

bitly Enterprise Resources About

nnews.co
Sep 17 2015 Sep:09 AM UTC

bit.ly/1UWxmta

Destination: http://nnews.co/2661562s/

Date (UTC)	Event	Short URL	Short URL Metadata Time and Date of Creation	Notes
2015-09-17 8:01:14	SMS from smsmedia: Noves ingerencies dels fiscals espanyols. Amenaces a Junts pel Si i la CUP http://bit.ly/1UWxmta (http://nnews[.]co/2661562s/)	http://bit.ly/1UWxmta	9/17/2015 9:00 AM UTC	This short URL was created 58 minutes after the text was sent
2017-07-14 8:25:33	SMS from desconegut: El Confidencial: La purga de Puigdemont http://bit.ly/2tlLc1g (https://statsads[.]co/JcnBlk9)	http://bit.ly/2tlLc1g	7/14/2017 7:00 AM UTC	This short URL was created 1 hour 25 minutes before the text was sent
2017-09-08 10:14:25	SMS from twitter: @assemblea “”En directe la roda de premsa de #LaDiadaDelSi des del Parlament”” http://bit.ly/2gQpHoU (https://statsads[.]co/uWgGyEy)	http://bit.ly/2gQpHoU	9/8/2017 9:00 AM UTC	This short URL was created 1 hour 14 minutes before the text was sent
2017-09-09 19:05:32	SMS from twitter: @larazon Puigdemont de nuevo viral http://bit.ly/2fbgeEZ (https://statsads[.]co/amJpgd1)	http://bit.ly/2fbgeEZ	9/9/2017 21:00 PM UTC	This short URL was created 1 hour 54 minutes after the text was sent
2017-09-30 7:01:48	SMS from vanguardia: Assange: “”La primera guerra mundial en internet ha comenzado en Catalunya”” http://bit.ly/2k9HSXL (https://statsads[.]co/VydNfLH)	http://bit.ly/2k9HSXL	9/30/2017 9:00 AM UTC	This short URL was created 1 hour 58 minutes after the text was sent

Conclusion

Amnesty International presented their confirmed evidence of espionage by the Spanish government via Pegasus spyware. After examining the data methodology, and creating a proof of concept that easily forges the evidence Amnesty presented, I have concluded that there is no evidence to prove the Spanish government, nor Pegasus spyware was used. The science behind Amnesty’s spyware detection methodology is based on a large keyword list, and if any of those keywords are found the user of their software is warned of a possible infection. Many false positives have been found since 2021 to present, and Amnesty International along with The Citizen Lab have kept this information from global government leaders. The inactions of these organizations have led to world leaders making decisions based on false information. Allowing The Citizen Lab and Amnesty International to continue presenting research without having a truly

impartial analysis is peril. Continuing to allow these organizations to act with impunity and disregard legal requirements and global standards for conducting forensics analysis undermines all purpose of a democracy.

References

- AfricaNews. (2021, July 20). *Morocco: Prominent journalist Omar Radi sentenced to 6 years in prison*. Africanews. Retrieved November 25, 2022, from <https://www.africanews.com/2021/07/20/morocco-prominent-journalist-omar-radi-sentenced-to-6-years-in-prison/>
- Amnesty International. (2017, October 18). *Spain: Charges for sedition and pre-trial detention against Jordi Cuixart and Jordi Sanchez are excessive*. Amnesty International. Retrieved November 14, 2022, from <https://www.amnesty.org/en/documents/eur41/7308/2017/en/>
- Amnesty International. (2019, November 19). *Spain: Analysis of the Supreme Court's ruling in the case of Catalan leaders*. Amnesty International. Retrieved November 14, 2022, from <https://www.amnesty.org/en/documents/eur41/1393/2019/en/>
- Amnesty International. (2020, December 31). Report and financial statements for the year ended 31 December 2020 . Retrieved November 13, 2022, from <https://www.amnesty.org/en/documents/fin40/4743/2021/en/>
- Amnesty International. (2021, July 27). *Joint open letter by civil society organizations and independent experts calling on states to implement an immediate moratorium on the sale, transfer and use of surveillance technology*. Amnesty International. Retrieved November 13, 2022, from <https://www.amnesty.org/en/documents/doc10/4516/2021/en/#:~:text=July%2027%2C%202021Index%20Number%3A%20DOC>
- Amnesty International. (2022, March 4). *Morocco: Authorities must ensure Omar Radi's fair trial rights*. Amnesty International. Retrieved November 25, 2022, from <https://www.amnesty.org/en/latest/news/2022/03/morocco-authorities-must-ensure-omar-radis-fair-trial-rights/>
- Amnesty International. (2022, May 11). *Civil society statement on the proposed EU Corporate Sustainability due diligence directive*. Amnesty International. Retrieved November 22, 2022, from <https://www.amnesty.org/en/documents/ior60/5588/2022/en/>
- Amnesty Tech. (2021, July 16). *Mobile Verification Toolkit*. Mobile verification toolkit. Retrieved November 12, 2022, from <https://docs.mvt.re/en/latest/>
- Bechtold, L. (2021, April 21). *Meet MGA alumna-turned-faculty, Sarah Beamish*. The Munk School. Retrieved November 13, 2022, from <https://munkschool.utoronto.ca/mga/news/meet-mga-alumna-turned-faculty-sarah-beamish>
- Boye, G. (2022, May 3). Crime of discovery and disclosure of secrets against NSO. Retrieved November 1, 2022, from

https://files.mediaset.es/file/10002/2022/05/03/Querella_Pegasus_-Gonzalo_BOYE-_1-_2_5367.pdf

Britannica. (2022). *Argumentum ad populum*. Encyclopædia Britannica. Retrieved November 18, 2022, from <https://www.britannica.com/topic/argumentum-ad-populum>

Cearbhaill, D. Ó. (2021, December 28). *Catching NSO group's pegasus spyware*. Amnesty Tech Catching NSO group's pegasus spyware . Retrieved November 19, 2022, from <https://media.ccc.de/v/rc3-2021-cbase-410-catching-nso-groups-p>

Civicus, C. (2020). *Catalan independence leaders targeted spyware*. Civicus. Retrieved November 14, 2022, from <https://monitor.civicus.org/updates/2020/08/18/catalan-independence-leaders-targeted-spyware-calls-revise-gag-law-five-year-anniversary/>

Deibert, R. (2017, April 18). *Digital epidemic*. UC Berkeley Center for Long-Term Cybersecurity. Retrieved November 18, 2022, from <https://youtu.be/dJSxp7dI-pQ>

Deibert, R. (2022, May 14). *Ronald Deibert - Pg 6*. Was Etienne Maynier the person who conducted the external validation at Amnesty Tech? Retrieved November 10, 2022, from <https://deibert.citizenlab.ca/>

Eltaquigrafo. (2022, July 10). *UN Centenar de Profesores Pide a la universidad de toronto que revise el informe del 'Catalangate'*. Eltaquigrafo. Retrieved November 13, 2022, from <https://www.eltaquigrafo.com/articulo/investigacion/un-centenar-de-profesores-pide-a-la-universidad-de-toronto-que-revise-el-informe-del-catalangate/20220710140416019942.html>

España, A. I. (2021, July 21). *Proyecto Pegasus: Exige El Fin de la Vigilancia Digital ilegítima*. Proyecto Pegasus: Exige el fin de la vigilancia digital ilegítima. Retrieved November 15, 2022, from <https://www.es.amnesty.org/actua/acciones/pegasus-vigilancia-jul21/>

European Commission. (2022, February 23). *Corporate sustainability due diligence*. European Commission - European Commission. Retrieved November 22, 2022, from https://ec.europa.eu/info/business-economy-euro/doing-business-eu/corporate-sustainability-due-diligence_en

European Parliament. (2014, June 26). *Agreement on Strategic Co-operation between the European Agency for Network and Information Security and the European Police Office*. Europol. Retrieved November 12, 2022, from <https://www.europol.europa.eu/>

European Parliament. (2022). *The European Parliament: Powers: Fact sheets on the European Union: European Parliament*. Fact Sheets on the European Union | European Parliament. Retrieved November 22, 2022, from <https://www.europarl.europa.eu/factsheets/en/sheet/19/the-european-parliament-powers>

- Europol. (2018, October 4). *European Union Agency for Network and Information Security (ENISA)*. Europol. Retrieved November 12, 2022, from <https://www.europol.europa.eu/partners-collaboration/agreements/european-union-agency-for-network-and-information-security-enisa#downloads>
- Forbidden Stories. (2022). *The pegasus project*. Forbidden Stories. Retrieved November 10, 2022, from <https://forbiddenstories.org/case/the-pegasus-project/>
- Foro de Profesores. (2022, July 5). *Foro de Profesores*. Independent investigation request on Citizen Lab's report "CatalanGate: Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru." Retrieved November 10, 2022, from <https://paginadelforodeprofesores.files.wordpress.com/2022/07/letter-to-university-of-toronto-by-foro-de-profesores-5-july-2022-re-catalangate-report.pdf>
- Gera, V., staff, T. O. I., Fabian, E., Afp, AP, T. O. I. staff and, Lazareva, I., Agencies, Leicester, J., Surkes, S., Surkes, S., HOOD, M., Seth Borenstein, S. M. and F. J., staff, M. B. and T. O. I., Keller-Lynn, C., Magid, J., Siegal, T., Agencies, T. O. I. staff and, staff, A. and T. O. I., Klein, D. I., ... McFETRIDGE, S. T. E. F. A. N. I. E. D. A. Z. I. O. and S. C. O. T. T. (2022, January 7). *Amnesty verifies Polish senator was hacked with NSO spyware*. The Times of Israel. Retrieved November 23, 2022, from <https://www.timesofisrael.com/amnesty-verifies-polish-senator-was-hacked-with-nso-spyware/>
- Gillette, G. H. (2020, February 13). *Ransomware attack 'rude awakening' for hospital, officials say*. Wyoming Tribune Eagle. Retrieved November 18, 2022, from https://www.wyomingnews.com/laramieboomerang/news/ransomware-attack-rude-awakening-for-hospital-officials-say/article_0a13aa92-bfbf-5e71-ac7d-c951541d79c7.html
- Global Encryption Coalition. (2022, April 14). *45 organizations and cybersecurity experts sign open letter expressing concerns with UK's online safety bill*. Global Encryption Coalition. Retrieved November 13, 2022, from <https://www.globalencryption.org/2022/04/45-organizations-and-cybersecurity-experts-sign-open-letter-expressing-concerns-with-uks-online-safety-bill/>
- Global Encryption Coalition. (2022, November 9). *Our members*. Global Encryption Coalition. Retrieved November 13, 2022, from <https://www.globalencryption.org/about/members/>
- Lenaers, J. (2022, September 28). *Letter Pega to Europol MS de Bolle 2022.09.28*. Box. Retrieved November 2, 2022, from <https://app.box.com/s/ngueyof0qlhqhs5ofjukuj7jyudsqqlar>
- Lenaers, J. (2022, September 21). *EU Parliament Pega Committee investigates the use of pegasus and other spyware*. YouTube. Retrieved November 1, 2022, from <https://www.youtube.com/watch?v=LciskOzRD4Y>

- Marczak, B. (2021, July 18). *.@FbdnStories worked with @AmnestyTech to investigate 67 phones on the leaked list, and discovered that 37 showed signs of hacking. we @citizenlab peer-reviewed the forensic methodology, and also examined four of the phones four of the phones: <https://t.co/echrhtnljs>*. Twitter. Retrieved November 15, 2022, from <https://twitter.com/billmarczak/status/1416798610977562624?s=20&t=dt7PWig7fyVgsRKdUt7wDA>
- Marin, M., Dubberley, S., Fan, W., Farzanefar, Y., Garcia, M., Mashadi, S., Maurat, L., Vadillo, R., Yadav, A., Yazikov, N., Farr, R. A. R., Mondragón, A. J. A., Díaz, F. L., Reyes, J. R., Cárdenas, J. L. S., & Castner, B. (2022). *Amnesty International*. CITIZEN EVIDENCE LAB. Retrieved November 23, 2022, from <https://citizenevidence.org/>
- Maynier, É. (2022, June 12). Smartphone et forensique : comment attraper Pegasus for fun and non-profit. Retrieved November 2, 2022, from <https://actes.sstic.org/SSTIC22/sstic-2022-actes.pdf>
- Merchant, N. (2022, July 28). *Victim of private spyware warns it can be used against US*. AP NEWS. Retrieved November 25, 2022, from <https://apnews.com/article/technology-africa-genocides-rwanda-72ecb6eb631c021004c3a017e7aeb2ce>
- The New Arab Staff & Agencies. (2021, July 23). *Kazakhstan says pegasus spy claims 'without evidence'*. The New Arab. Retrieved November 25, 2022, from <https://www.newarab.com/news/kazakhstan-says-pegasus-spy-claims-without-evidence>
- Pega Committee. (2022, April 19). Emeeting for Committees - Pega. Retrieved October 31, 2022, from <https://emeeting.europarl.europa.eu/emeeting/committee/en/archives/PEGA>
- Pega Committees. (2022, April 19). *Highlights: Home: Pega: Committees: European Parliament*. Highlights | Home | PEGA | Committees | European Parliament. Retrieved October 31, 2022, from <https://www.europarl.europa.eu/committees/en/pega/home/highlights>
- Pegg, D., & Cutler, S. (2021, July 18). *What is pegasus spyware and how does it hack phones?* The Guardian. Retrieved November 15, 2022, from <https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones>
- Quino Petit, M. G. (2022, May 15). *Ronald Deibert, Fundador de Citizen Lab: "los gobiernos usan pegasus porque tienen apetito de espiar"*. El País. Retrieved November 2, 2022, from <https://elpais.com/espana/2022-05-15/ronald-deibert-fundador-de-citizen-lab-los-gobiernos-usan-pegasus-porque-tienen-apetito-de-espiar.html>
- Scott-Railton, J. (2022, July 27). *Combating the Threats to U.S. National Security from the Proliferation of Foreign Commercial Spyware*. Written testimony of John Scott-Railton, Senior Researcher, the Citizen Lab House Permanent Select Committee on Intelligence. Retrieved November 2, 2022, from

<https://docs.house.gov/meetings/IG/IG00/20220727/115048/HHRG-117-IG00-Transcript-20220727.pdf>

Scott-Railton, J. (2022, July 27). Truth in Testimony Disclosure Form. Retrieved November 23, 2022, from <https://docs.house.gov/meetings/IG/IG00/20220727/115048/HHRG-117-IG00-TTF-Scott-RailtonJ-20220727.pdf>

Scott-Railton, J. (2022, July 27). *Written testimony of John Scott-Railton House Intelligence Committee*. Written testimony of John Scott-Railton. Retrieved November 23, 2022, from <https://docs.house.gov/meetings/IG/IG00/20220727/115048/HHRG-117-IG00-Wstate-Scott-RailtonJ-20220727.pdf>

Scott-Railton, J., Campo, E., Marczak, B., Razzak, B. A., Anstis, S., Böcü, G., Solimano, S., & Deibert, R. (2022, April 18). *Catalangate: Extensive mercenary spyware operation against Catalans using pegasus and Candiru*. The Citizen Lab. Retrieved October 31, 2022, from <https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/>

Singh, A. (2017, July 17). *Google policy fellowship at citizen lab and Cippic - "premier research group"*. The Citizen Lab. Retrieved November 18, 2022, from <https://citizenlab.ca/2017/04/google-policy-fellowship-citizen-lab-cippic/>

Timberg, C., & Priest, D. (2021, July 18). *Private Israeli spyware used to hack cellphones of journalists, activists worldwide*. The Washington Post. Retrieved November 15, 2022, from <https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/>

vicenews, V. (2021, October 2). *The world's most terrifying spyware | investigators*. Vice. Retrieved November 10, 2022, from <https://www.youtube.com/watch?v=QX7X4Ywuotc>

Webster. (2022). *The '-gate' suffix: Why every scandal ends in 'gate'*. Merriam-Webster. Retrieved October 30, 2022, from <https://www.merriam-webster.com/words-at-play/gate-suffix-scandal-word-history>

Xnet. (2021, July 27). *La Primera transposición de ley de alertadores de la ue*. Xnet. Retrieved November 13, 2022, from <https://xnet-x.net/es/xnet-registra-primera-ley-alertadores-ue/>