maria [lab]
feminist internet research network
APC ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS

Feminist digital forensics:

A study and a proposal for development

Feminist digital forensics: A study and a proposal for development

Feminist digital forensics: A study and a proposal for development

Authors
Carl Jancz
Dany Araújo

Research team
Carl Jancz
Dany Araújo

Research coordinators
Carl Jancz (MariaLab)
Dany Araújo (Marialab)
Tigist S. Hussen (FIRN, APC)
Diana Bichanga (FIRN, APC)
Serene Lim (FIRN, APC)

Collaborators/participants
Laura Ramos
Sonia Acosta
Florencia Machado
Claudia Suárez

FIRN reviewers
Horacio F. Sívori
Tigist S. Hussen

Content editing
Tigist S. Hussen

Proofreading
Sugandhi Ravindranathan

Layout proofreading
Drew McKevitt

Publication production
Carl Jancz (MariaLab)
Dany Araújo (Marialab)
Cathy Chen (APC)
Lori Nordstrom (APC)

Design and layout
Camila Rodriguez

Illustrations
Fernanda Serejo

Published in English by Association for Progressive Communications (APC) and MariaLab, 2026

Published in Portuguese and Spanish by MariaLab, 2026

Acknowledgments

We are grateful for the contributions of participants who shared their time, knowledge and experiences with us. Their insights were invaluable in shaping the research.

This work forms part of the third edition of the Feminist Internet Research Network (FIRN) project, supported by the APC Women's Rights Programme and the International Development Research Centre (IDRC). The views expressed herein do not necessarily represent those of APC and its board members or of IDRC and its Board of Governors.

FIRN is a network of researchers, activists and practitioners from Global South countries in Africa, Asia, Eastern Europe and Latin America. FIRN focuses on the making of a feminist internet, seeing this as critical to bringing about transformation in gendered structures of power that exist online and offline and to capture fully the fluidity of these spaces and our experiences with them. Members of the network undertake data-driven research that provides substantial evidence to drive change in policy and law, and in the discourse around internet rights.

MariaLab
contato@marialab.org
marialab.org

ISBN 978-92-95113-80-0
APC-202601-WRP-R-EN-DIGITAL-370

IDRC · CRDI
International Development Research Centre
Centre de recherches pour le développement international

Canada

1.

How it began

The growing interest of civil society in digital forensics arises amid escalating digital threats to human rights defenders, particularly through surveillance tools on electronic devices. The case of Pegasus,[1] spyware developed by the Israeli company NSO Group,[2] and notorious for targeting journalists and activists globally, is perhaps the best-known example. Yet it represents only one facet of a more complex problem.

Digital forensics became especially relevant for us at MariaLab when we faced the challenges of creating Maria d'Ajuda,[3] a feminist helpline to address digital security emergencies. Our work experience and interaction with other feminist helplines led us to identify a common problem: the limitation of resources – human, financial and technical knowledge – that often restricts helplines in supporting harm-reduction actions and digital care.

Our research report, *Feminist digital forensics: A study and a proposal for development*, unfolds our incursion into the field of digital forensics. Starting with the investigation of what we call traditional forensics, a technical field deeply connected to the criminal justice system, where forensic experts and other actors, such as lawyers and police officers, work together in legal investigations. Our research questions inquired how forensic analysis can be a tool to advance the fight against technology-facilitated gender-based violence (TFGBV). We started with the hypothesis that improving our knowledge for identification and collection of evidence for forensic analysis would improve our collective capacity to generate data about digital threats from an intersectional and feminist perspective. The central objective of this research is to boost the development of feminist helplines through the systematisation of information and the development of knowledge in digital forensics.

For the development of the study, we dialogue mainly with two types of interlocutors: international organisations that respond to civil society security incidents, recognised as references in this field; and with feminist digital security

[1] Pegg, D., & Cutler, S. (2021, 18 July). What is Pegasus spyware and how does it hack phones? *The Guardian*. https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones
[2] https://www.nsogroup.com/
[3] https://mariadajuda.org/

helplines from Latin America,[4] with whom we have already collaborated on prior projects and established a relationship of trust.

It is important to highlight that in this research we occupy a dual role as both researchers and participants interested in the investigated theme. This duality between "investigating" and "participating" is natural to our practice as a feminist hacker organisation – and when applied in a scientific research context, it requires additional caution and reflection. We understand that our personal experience and political engagement with the researched topic are integral parts of the investigation process, and that critical reflection on our own positions is fundamental for knowledge production. This also includes recognising the position of "power and privilege" that come with "community trust" due to "shared identities".[5]

From this recognition of non-objectivity, we sought methods to ensure that the ideas, data, and experiences gathered in our research would not merely reflect the perspectives of those writing it. Instead, action research – an investigative process that intentionally seeks to create practical effects in the reality being studied – was our chosen approach.[6]

Thus, the entire research process unfolded through constant interaction with our interlocutors. Beyond the discussions presented in this report, we compiled an informational guide based on the collective knowledge accumulated throughout all stages. This guide aims to include case examples, provocative questions, testing models, and a proposed framework that will support feminist helplines in their work of triaging cases to be referred for forensic analysis.[7]

The initial phase of field exploration was conducted through interviews with representatives from seven expert organisations providing digital security support to civil society and human rights defenders. These interviews allowed us to map out the scope of work of these groups and their many changes in recent years.

Our direct participation in alliances and training processes was fundamental for outlining the state of the art in digital forensics for civil society. In recent years, several organisations have undertaken efforts to this end, organising different models of educational processes. In March 2024, we joined a consortium of Latin American organisations led by Fundación Acceso,[8] with the objective of discussing and analysing surveillance in Latin America. As part of this consortium,

[4] https://feministhelplines.org/

[5] Hussen, T. S. (2019, 29 August). All that you walk on to get there: How to centre feminist ways of knowing. *GenderIT.org.* https://firn.genderit.org/blog/all-you-walk-get-there-how-centre-feminist-ways-knowing

[6] Tripp, D. (2005). Pesquisa-ação: uma introdução metodológica. *Educação e pesquisa, 31*(3), 443-466. https://doi.org/10.1590/s1517-97022005000300009

[7] https://marialab.org/feministforensics

[8] https://www.acceso.or.cr

we attended three in-person meetings[9] that provided an opportunity to learn and gather information on the tools, methodologies, protocols and practices currently used to analyse and respond to advanced digital threats.

In July 2024, we also participated in training led by Front Line Defenders[10] and the Mesoamerican Initiative of Women Human Rights Defenders (IM-Defensoras)[11] aimed at feminist organisations and activists in Latin America and the Caribbean. During the preparatory meetings for this gathering, we had the opportunity to discuss support methodologies and protocols with other feminist digital security educators, and from there we developed the idea of the feminist support chain, which we will detail in the following chapters.

Finally, as the last methodological step, we held an immersive in-person meeting for three days with representatives from each feminist helpline participating in this project. For didactic purposes, we organised this meeting around a case simulation, covering all steps, from receiving a case to its conclusion. During each stage we discussed how our helplines would act, and facilitated practical sessions on the usage of technical tools. Beyond a workshop on implementing forensic techniques in helplines' routines, the meeting was a time of sharing and collaboration that resulted in rich discussions about what we aim to achieve by applying forensic analysis with a feminist care perspective.

This report is organised into four chapters, where we explore when digital forensics becomes a human rights issue, how the digital security community for civil society has been preparing to address the challenges of advanced digital threats, and where the feminist approach intersects with this topic.

Chapter 2 briefly presents the development of digital forensics in civil society following the increase in surveillance technology cases used against human rights defenders – a context still largely defined by the Pegasus Project and the hunt for the next major spyware. At the end of the chapter, we seek to broaden the horizons of this topic and situate how gender issues fit into this discussion.

In Chapter 3, we introduce some concepts of digital forensic analysis within criminalistics and discuss how its tools and methodologies have been appropriated to develop forensic analysis for supporting human rights defenders, culminating in what is being called consensual digital forensics.

Chapter 4 presents the role of helplines in responding to digital incidents, including spyware threats, and the helplines' desire to improve their technical

[9] The meetings took place from 11 to 15 March 2024 in San José, Costa Rica; 14 to 16 May 2024 in São Paulo, Brazil; and 29 to 31 July 2024 in Bogotá, Colombia.

[10] https://www.frontlinedefenders.org

[11] https://im-defensoras.org/en

capabilities in order to integrate digital forensics into their response to TFGBV. In this chapter, we present a systematic overview of the feminist helplines included in this study, comparing their organisational structures and operational frameworks. Additionally, we highlight their key similarities and differences.

In the final chapter (Chapter 5), we envision what feminist digital forensics could be. We develop the concept of the feminist support chain as a visual summary of feminist helplines' intake process, including a proposal to integrate this chain with the practice of consensual forensic analysis. This chapter does not aim to be conclusive or definitive about a concept, but rather brings together the central aspects of this field's development, showing not only how digital forensics can support gender violence cases but also how the feminist perspective of digital care contributes to the development of consensual forensics.

2.

Digital surveillance, a concern for human rights

Since 2016, organisations like Amnesty Tech[12] and The Citizen Lab[13] have published relevant forensic reports[14] focused on governmental spyware. The most scandalous case yet was possibly the Pegasus Project.[15] In July 2021, a consortium of 17 international media organisations, led by Forbidden Stories with technical support from Amnesty International's Security Lab, revealed an extensive list of more than 50,000 phone numbers that were potential targets of surveillance by NSO Group's Pegasus spyware since 2016.

Forensic analysis conducted by Amnesty International's Security Lab and other partner organisations has confirmed the presence of spyware on phones belonging to individuals in several countries. The Pegasus Project allegations triggered substantial international repercussions, leading to numerous investigations by governments, international agencies and civil society organisations.

The Pegasus spyware operates silently. It can be covertly installed on mobile phones using a zero-click exploit technique, infecting devices without any user interaction. Pegasus can access various data and functions on infected devices, including contacts, messages, photos, microphone, camera, and location – violating individuals' right to privacy.[16]

There is great concern about the misuse of these powerful tools, which, contrary to their creators' claims, are being widely abused by governments to identify, monitor, and ultimately silence journalists.[17] The Forbidden Stories consortium revealed that at least 180 journalists were selected as targets in countries including India, Mexico, Hungary, Morocco and France, among others. Other potential targets include human rights defenders, academics, business people, lawyers, doctors, diplomats, union leaders, politicians and several heads of state.

Pegasus, however, is not the only concern. Many other types of spyware on the market have yet to be detected, and new surveillance tools continue to be created and launched. The downfall of companies like Germany's FinFisher and Italy's Hacking Team was not enough to discourage this sector. The spyware industry is worth billions of dollars and continues to attract new players like the NSO Group, Cytrox and Candiru.[18]

[12] https://www.amnesty.org/

[13] https://citizenlab.ca/

[14] Scott-Railton, J., Marczak, B., Guarnieri, C., & Crete-Nishihata, M. (2017). *Bitter Sweet: Supporters of Mexico's Soda Tax Targeted With NSO Exploit Links*. The Citizen Lab. https://citizenlab.ca/2017/02/bittersweet-nso-mexico-spyware/

[15] Pegg, D., & Cutler, S. (2021, 18 July). Op. cit.

[16] Cardillo, M., Fischer, S., & Kekre, A. (2023). *Targeting, infecting, surveilling, harming*. Geneva Graduate Institute & CyberPeace Institute. https://www.graduateinstitute.ch/sites/internet/files/2024-01/ARP%20FINAL%20REPORT%20-%20Aditi%20Amol%20Kekre.pdf

[17] Woodhams, S. (2021). *Spyware: An Unregulated and Escalating Threat to Independent Media*. Center for International Media Assistance. https://www.cima.ned.org/wp-content/uploads/2021/08/CIMA_Spyware-Report_web_150ppi.pdf

[18] Ibid.; Feldstein, S., & Kot, B. (2023, 2 March). Global Inventory of Commercial Spyware & Digital Forensics. *Mendeley Data*. https://data.mendeley.com/datasets/csvhpkt8tm/10

All these revelations provoked a strong reaction among human rights defenders, leaving them in a state of uncertainty about potential surveillance of their activities. In our interviews with Access Now and Amnesty Tech, they reported a rise in inquiries from individuals describing various concerns. Some mentioned vague but unsettling incidents like, “I received a weird message”; others reported unusual device behaviour like, “My phone battery drains too fast”; while yet others raised more specific issues such as, “I worked with someone named in the leaks.” These reports ranged from vague suspicions to specific allegations, reflecting growing public anxiety about digital privacy and surveillance.

Even organisations with long-established rapid response practices for digital secruity incidents found themselves inundated with unprecedented volumes of requests, far exceeding their capacity:

> So we got really big questions and we were not really ready to start this. So we looked into our partners and tried to push the partnership with them, but at the same time we tried to also do more learning in-house. So while we are working all these cases and escalating them to partners, mainly Citizen Lab and Amnesty, we started to look into the artefacts we are collecting.[19]

The rise of digital forensics within civil society represents a crucial response to the growing use of surveillance technologies against human rights defenders. Distinct from traditional criminalistics – which focuses on state-led prosecution – this civil society approach is characterised by its independent methodology, designed to protect activists, journalists, and vulnerable groups who are routinely subjected to illegal surveillance.

2.1 THE ROLE OF DIGITAL SECURITY HELP DESKS FOR CIVIL SOCIETY

Digital security help desks for civil society (DSHCS) comprise organisations that provide technical support to human rights organisations and defenders.[20] These organisations implement initiatives focused on providing digital security guidance and training. They assist civil society in addressing digital threats and play a fundamental role in developing digital forensics for civil society.

We engaged with key organisations at the forefront of advancing digital forensics – both as a methodology and a strategy for investigating digital threats. These organisations were chosen based on their substantial contributions to the field,

[19] Interview with Access Now, 19 September 2024.

[20] Digital Defenders Partnership. (2022). *Tech Care: A step-by-step guide to providing digital support for civil society*. https://tech-care.cc/TechCare_Guide_en.pdf

their standing within the digital security community, and the unique approaches they apply in forensic analysis.

In Table 1, we identify each of these organisations, and throughout the text, they will be referenced through quotations from interviews.

Table 1. Organisations at the forefront of digital forensics

Organisation	Description
SocialTIC	SocialTIC is a Mexican organisation dedicated to strengthening activists, journalists, social organisations, and human rights defenders, through the strategic and secure use of digital technologies, information, and communication. The organisation was created in 2012 and its areas of expertise include digital security, open data, and infoactivism. In 2016, SocialTIC carried out the GobiernoEspía project in partnership with The Citizen Lab, Artículo 19 and R3D. It was an investigation and documentation of digital surveillance using the NSO Group's Pegasus malware, which was used to spy on journalists and human rights defenders in Mexico. Based on this discovery, SocialTIC supported forensic analysis in Mexico and El Salvador on the use of Pegasus and other malware in other Latin American countries. In 2025, the organisation launched SocialTIC Forensics,[21] a repository of technical documentation that promotes consensual digital forensics as a tool for the defense of human rights.
Conexo	Conexo is a Latin American organisation specialised in digital security, providing training and support services to civil society organisations and human rights defenders. It adopts a holistic approach, integrating three pillars into its initiatives: digital, physical and psychosocial security. Conexo operates through long-term processes, typically spanning several months, involving multiple actions and recommendations

[21] https://forensics.socialtic.org/

Conexo

across different areas. Its approach is primarily preventive, prioritising risk mitigation before incidents occur, but it also includes a reactive component to respond to security breaches when necessary.

The main services provided by Conexo are:

- Independent security audits
- Training in holistic security topics
- Support for implementing organisational security measures
- Policy and protocol development
- Advanced technical services, focusing on cases of malware infections, malicious infrastructure management, investigations into targeted phishing, and analysis of suspicious servers.

Conexo, in collaboration with Internews, DefendDefenders and the Jordan Open Source Association (JOSA), contributed to the development of Infuse[22] – a community-driven framework designed to help digital security professionals (including trainers, technologists and auditors) enhance their expertise in specialised technical areas.

Access Now

Access Now is a non-profit organisation founded in USA in July 2009. It focuses on digital civil rights and has a global reach.

The organisation operates in the following areas:

- Advocacy and public policy
- Digital crisis response providing emergency support (via helpline) to victims of digital rights violations, including journalists and human rights defenders.
- Campaigns and mobilisation
- Grant funding to grassroots and frontline organisations working with communities and are most impacted by digital rights violations.
- Development of reports and tools to expose technology abuses.

[22] https://infuse.quest/

FemBloc

FemBloc was founded in 2021 in Catalonia and is a helpline specialising in digital gender-based violence.

They provide support for victims of digital gender-based violence, primarily women, LGBTQIA+ individuals and their close networks. The organisation provides comprehensive assistance encompassing psychological support, technical guidance and legal counsel.

It conducts infrastructure audits while also providing specialised support for hate speech-related incidents, including digital protection plans for public figures and land defenders, combining preventive measures with response strategies.

FemBloc has been specialising in forensic expertise in order to improve the helpline service and provide digital forensic analysis for legal proceedings.

Defensive Lab Agency

Defensive Lab Agency is a small organisation situated in Europe and dedicated to developing open-source digital forensic tools through the PiRogue Tool Suite (PTS) Project.[23] While numerous proprietary tools exist in this field, their high costs often place them out of reach for many NGOs and independent groups. The main goal of Defensive Lab is facilitating civil society organisations with cost-effective solutions for their investigative needs.

In addition to software development, the organisation also conducts training sessions, security audits and penetration testing, as well as digital forensic analysis for legal and investigative purposes.

Front Line Defenders

Front Line Defenders was established in 2001 as a small organisation dedicated to providing rapid support to human rights defenders at risk. Initially run by just a handful of people, its goal was to deliver rapid response in urgent cases. Over the past two decades, it has expanded to a team of around 80 people.

Front Line Defenders operates globally. With its offices in Ireland and an advocacy office in Brussels, it maintains a broad support network, collaborating with partner organisations worldwide to enhance protection efforts.

[23] https://pts-project.org/

Front Line Defenders

It is a holistic protection organisation that provides support on a case-by-case basis, addressing multiple aspects of security, including physical, digital, psychosocial, legal and medical needs. Beyond direct protection, the organisation offers several key programmes:

- Protection grants: Emergency financial support processed and delivered quickly to those in urgent need.
- Capacity building: Training in digital security, physical safety, well-being and other critical areas to strengthen defenders' resilience.
- Emergency helpline: Beyond immediate crisis response, the helpline proactively engages with defenders, assessing risks and building capacity ahead of critical events like elections or shifting security trends.
- Training of trainers (ToT): A long-standing initiative, particularly in digital protection since 2014, mentoring local champions and organisations to create sustainable support networks.
- Security training: Both one-on-one and group training, adapted to risk assessments and situational needs.

Amnesty International Security Lab

The Security Lab is part of Amnesty Tech – a broader division at Amnesty International. This division operates at the intersection of technology and human rights, having launched between 2016 and 2017. Its work addresses issues like algorithmic discrimination and Big Tech's accountability.

The Security Lab is a multidisciplinary team of experts conducting technical investigations into cyberattacks targeting activists and human rights defenders.

- Developing tools and services to counter digital threats, including spyware and internet shutdowns.
- Collaborating with digital rights communities to strengthen collective protection efforts.
- Conducting evidence-based research to inform targeted campaigns and advocacy.
- Managing the Digital Forensic Fellowship,[24] a programme that builds technical capacity among civil society

[24] https://securitylab.amnesty.org/digital-forensics-fellowship/

Amnesty International Security Lab

technologists worldwide. Through collaboration with Security Lab experts, fellows enhance their digital forensic expertise to better protect local human rights defenders from emerging threats.

2.2 THE LEARNING CURVE

It is impossible to discuss the evolution of spyware investigation practices within civil society without acknowledging the work of Amnesty Tech, which, alongside The Citizen Lab, pioneered this field. Both organisations are internationally recognised for their investigations and publication of forensic reports on the abuse of surveillance tools against human rights defenders. In our interviews, nearly everyone cited these two organisations as benchmarks in advanced threat analysis. Examining their trajectory gave us clearer insight into this field's developments and how their progress followed a learning curve.

The investigation of spyware attacks emerged organically from Amnesty Tech's work, beginning with initial efforts between 2016 and 2017. Early research on entities like the NSO Group developed reactively, driven by case-specific encounters that later evolved into proactive forensic methodologies. The first confirmed case of NSO's Pegasus spyware in 2018 marked a turning point for Amnesty Tech, leading to team expansion and cross-regional collaboration to scale investigations.

Initially, detection relied on self-reported incidents (e.g. suspicious messages or device anomalies). However, researchers quickly recognised this approach's limitations, as zero-click attacks – requiring no user interaction – left no visible traces. This gap necessitated proactive forensic outreach, demonstrated by targeted device examinations in Morocco, where high-risk civil society actors were found infected. These cases refined detection protocols, later applied in Hungary and France. The leak provided to Forbidden Stories included 300 Hungarian phone numbers, including those of journalists who were investigating the Hungarian developments related to the use of NSO's Pegasus spyware.[25] French intelligence investigators have even confirmed that Pegasus spyware was found on the phones of three journalists, including a senior member of staff at one of the country's international television stations.[26]

[25] Bleyer-Simon, K. (2021, 12 August). Pegasus in Hungary: A Surveillance State Unmasked. *Henrich Böll Stiftung*. https://cz.boell.org/en/2021/08/02/pegasus-hungary-surveillance-state-unmasked

[26] Willsher, K. (2021, 2 August). Pegasus spyware found on journalists' phones, French intelligence confirms. *The Guardian*. https://www.theguardian.com/news/2021/aug/02/pegasus-spyware-found-on-journalists-phones-french-intelligence-confirms

The 2021 Pegasus Project posed a paradigm shift, enabling large-scale analysis of hundreds of likely targeted devices. This dataset significantly advanced forensic methodologies and revealed broader surveillance patterns.[27] The project highlighted how most attacks remain invisible to victims, underscoring the need for systematic investigations.

> So that's broadly the framework in Amnesty [Tech]. We do evidence-based research, we find whether human rights research or now forensic research, and we use that to show where human rights abuses are happening in the world and take that evidence to try and create change through campaigning and advocacy work.[28]

The profound impact of spyware cases and the urgent need for professionals with advanced technical expertise have driven efforts to strengthen digital forensic capabilities within the community of digital security help desks for civil society (DSHCS) in Latin America. These help desks have a practice of collaborating with reference organisations from the Global North when dealing with suspected malware cases. However, this collaboration used to be highly unidirectional, as data was provided, but most analyses were not conducted in partnership, and the technical and procedural capacity of these groups did not advance enough to make them autonomous. While collaborative networks enhance the credibility of forensic analyses and strengthen evidence for public advocacy, they simultaneously create dependencies on more technically advanced partner organisations.

The challenge is twofold. On the one hand, there is a shortage of professionals with technical expertise and procedural knowledge required in digital forensics. On the other, there is a lack of individuals who possess the technopolitical perspective necessary to properly address and comprehend the unique requirements of human rights work. Unsurprisingly, the limited number of individuals currently qualified to perform this work often aligns with the stereotype of white cisgender males occupying more technical roles, while women and gender non-conforming individuals tend to predominate in less technical digital security support.

In recent years, there have been initiatives to address this perceived shortage of qualified professionals, with efforts primarily focused on education, mentoring, and network building for individuals who already work in the field of DSHCS, instead of trying to attract qualified forensic analysts from other areas. These initiatives can be categorised into four main areas and share many similarities: enrolment is often limited to those affiliated with organisations from civil society,

[27] Forbidden Stories. (2021, 18 July). About the Pegasus Project. https://forbiddenstories.org/about-the-pegasus-project/
[28] Interview with Amnesty Tech, 17 October 2024.

and selection criteria are based on gender diversity and work's relevance to human rights.

- Online courses with closed participants: these tend to have multiple facilitators, giving preference to women and gender dissidents. For example: Digital Defenders Partnership's Identification of Spyware and Documentation of Digital Threats with a Human Rights and Gender Perspective[29] and MariaLab's Introduction to Digital Forensics for Human Rights.[30]
- Mentoring programmes offering a more private and in-depth formation. These may include other experience-sharing strategies such as internships at high-risk organisations or mini grants to develop internal projects. For example, Amnesty Tech's digital forensic fellowship[31] and Internews' MONITOR Scaled project.[32]
- Community-developed frameworks for self-study. Intended as a resource library with study pathways focused on digital protectors to advance their knowledge and skill sets in areas of specialised technical expertise, e.g. Infuse.[33]
- Network enabling projects. Focused on the connection of individuals and organisations already supporting civil society with digital forensics-related work or have plans to do so. For example, the aforementioned consortium of Latin American organisations led by Fundación Acceso.

Many of these initiatives have only been possible due to the growing interest of powerful players to fund projects that aim to improve civil society's answer to the big spyware threat. A notable example is the Stop Spyware Fund[34] that has injected millions of dollars into such projects and has Ford Foundation and Apple as its biggest stakeholders. This fund provides grants and access to a network of organisations and advocacy for dozens of projects in the Global South.

The fund's primary goal is to detect new spyware being used against the civil society, something that at times seems like the hunt for a new Pegasus. But as smaller organisations are drafted to carry out short-term projects, other local needs have emerged, encompassing both education and research on the psychosocial effects of malware surveillance.

[29] https://www.digitaldefenders.org/introduction-to-forensics-of-mobile-devices-identification-of-spyware-and-documentation-of-digital-threats-with-a-human-rights-and-gender-perspective

[30] Carl. (2023, 26 June). Feminist sparks of reflection about digital forensics. GenderIT.org. https://genderit.org/feminist-talk/feminist-sparks-reflection-about-digital-forensics

[31] https://securitylab.amnesty.org/digital-forensics-fellowship/

[32] https://internews.org/areas-of-expertise/global-tech/global-tech-projects/global-tech-monitor/

[33] https://infuse.quest/

[34] https://stopspyware.fund/about

Despite the developments around digital forensics being driven by the spyware crisis, the knowledge of forensic analysis itself can be highly relevant to the investigation of other types of digital threats.

In the interview with Amnesty Tech, there is this argument for a broad view of forensics, which focuses on device analysis as well as investigations involving digital evidence from various sources. A common example is phishing emails, where forensic analysts determine whether an attack was targeted and attempt to trace its origin. Beyond phishing, forensic experts also examine Windows malware, email-based attacks, WhatsApp scams, and other threat vectors. Regardless of the attack type, the investigative process follows a structured approach: evidence collection, correlation with known indicators (such as malicious domains or previously identified attack patterns), and contextual analysis using broader threat intelligence to establish connections and identify patterns.

2.3 GENDER MATTERS

Amid the countless scandals and billions generated by the spyware industry, a parallel market is rapidly developing. Classified as stalkerware, this software category has surveillance capabilities but is routinely marketed to the public to facilitate intimate partner violence (IPV), abuse or harassment. While some companies claim legitimate uses like parent-child monitoring or employee control – still problematic though – these tools are commonly repurposed for online gender-based violence (OGBV). The Citizen Lab's 2019 study exposed companies actively promoting their software for stalking purposes, enabling abusers' obsessive behaviour that violates privacy and threatens victims' safety.[35] Technology-facilitated gender-based violence (TFGBV) is characterised by specific distinguishing factors: perpetrator anonymity, low technical barriers to committing offences, and permanent record of violating content on the internet. While abusers hide behind anonymity, victims face ongoing revictimisation as online content proves virtually impossible to fully erase.[36]

This violence thrives by exploiting vulnerabilities in legitimate app functions. So-called dual-use apps – which serve both legitimate and malicious purposes – often come pre-installed on devices. Poor configuration of features like Find My Phone or parental control apps creates loopholes for attackers to easily access and monitor data. The digital gender gap is a huge component of these risks, as

[35] Parsons, C., Molnar, A., Dalek, J., Knockel, J., Kenyon, M., Haselton, B., Khoo, C., & Deibert, R. (2019). *The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry*. The Citizen Lab. https://citizenlab.ca/2019/06/the-predator-in-your-pocket-a-multidisciplinary-assessment-of-the-stalkerware-application-industry/; Mason, C. L., & Magnet, S. (2012). Surveillance Studies and Violence Against Women. *Surveillance & Society. 10*(2), 105-118. https://doi.org/10.24908/ss.v10i2.4094

[36] Taller Comunicación Mujer. (2023). *Mediciones de la violencia de género digital en América Latina y el Caribe*. https://navegandolibres.org/mediciones-de-la-violencia-de-genero-digital-en-america-latina-y-el-caribe-aborda-las-metodologias-y-contenidos-generados-sobre-la-tematica-ademas-de-los-retos-en-su-abordaje/

victims frequently delegate account and device security to partners who exploit this dependence for control and stalking.[37] This pattern appears consistently across TFGBV support groups, revealing stalkerware as less prevalent than dual-use software abuse.[38]

The work of feminist organisations and activists has brought this issue to the attention of technology creators, such as the Internet Engineering Task Force (IETF), which is a reference in internet architecture development. This draft[39] proposes considerations for minimising technology abuse in IPV, both in tools development and in the implementation of network protocols.

Much of TFGBV assistance is provided by feminist organisations and collectives that are part of DSHCS and are deeply committed to addressing gender-based violence in all spheres. In Latin America, feminist helplines established in recent years share a digital security perspective that prioritises survivors' needs. They adopt a political perspective emphasising collectivity, autonomy and intersectionality as fundamental elements for creating protection strategies that go beyond technical solutions. These security measures respond to a combination of subjectivities, co-responsibilities and mutual care.[40]

Despite originating from diverse contexts and organisations, the challenges in our work are remarkably similar when faced with the need to handle cases requiring digital forensic analysis. While organisations and digital care professionals provide initial first aid to supported persons, our capacity for thorough digital forensic examinations is frequently limited by quick check-up constraints. Additionally, online support and the limitations of remote communication pose significant challenges for devices data collection.

During our meeting with feminist activists at the invitation of Front Line Defenders and IM-Defensoras, a critical discussion point was the necessity to perform risk assessment for each case. This task typically falls to organisations and individuals serving as the first line of defence, who use trust-based relationships to analyse context and specific risks. This information is vital throughout the support chain and must be shared to ensure successful comprehensive digital forensic analysis. Digital helplines for civil society,

[37] Ibid.; Havron, S., Freed, D., Chatterjee, R., McCoy, D., Dell, N., & Ristenpart, T. (2019). Clinical Computer Security for Victims of Intimate Partner Violence. Paper presented at the 28th Usenix Security Symposium, Santa Clara, USA, 13 to 16 August. https://www.usenix.org/conference/usenixsecurity19/presentation/havron

[38] A notable example is the clinic to end tech abuse, whose many findings about fighting stalkerware were shared in the presentation "Understanding and Responding To Tech Abuse". https://datatracker.ietf.org/meeting/114/materials/slides-114-hrpc-understanding-and-responding-to-tech-abuse-00

[39] Celi, S., Guerra, J., & Knodel, M. (2023, 18 October). Intimate Partner Violence Digital Considerations. Understanding and Responding To Tech Abuse. *IETF*. https://www.ietf.org/archive/id/draft-irtf-hrpc-ipvc-00.html#name-kinds-of-tech-enabled-ipv-a

[40] de Araujo, D., Manica, D., & Kanashiro, M. (2020). Tecnopolíticas de Gênero. *Cadernos Pagu, 59*. https://doi.org/10.1590/18094449202000590000; Natansohn, G., & Reis, J. (2020). Digitalizando o cuidado: mulheres e novas codificações para a ética hacker. *Cadernos Pagu, 59*. https://doi.org/10.1590/18094449202000590005

particularly feminist digital helplines, are well known for this work. However, compared to advanced digital threats and the hunt for the next Pegasus, basic digital care actions are less exciting or prioritised in computer research.[41] This is reflected in research and civil society funding, where substantial amounts go to spyware investigation while programmes supporting women's rights, free software and autonomous infrastructures face cuts.

Organisations like Amnesty Tech and Access Now, focused specifically on forensic analysis for civil society, often refer TFGBV cases unrelated to activists to other networks specialising in psychosocial digital care. According to Access Now interviews, they have specific protocols for digital gender-based violence cases (involving ex-partners, attacks against feminists or gender-motivated harassment) that address both technical and human aspects. The immediate priority is assessing physical safety, sometimes requiring creative solutions like trusted intermediaries when victims face imminent danger. The emotional intensity of these cases demands specialised handling, leading to their employment of trained holistic security coordinators who apply mental health-based crisis-response principles to address both digital threats and human consequences. This approach reflects hard-won institutional knowledge about digital crisis management, with staff receiving ongoing training for high-stress digital interactions that limit traditional de-escalation techniques.

While this approach proves valuable – particularly for gender-based violence given its complex nature – it reveals an operational paradox. On one hand, TFGBV cases seldom receive the in-depth technical analysis that could bolster legal protections. When redirected to gender-focused groups (which typically lack resources for advanced digital threats), resolution often defaults to basic first-aid support, depriving victims of specialised forensic expertise that could validate their cases.

Conversely, consider the psychosocial support for spyware victims: while care is undoubtedly exercised during assistance, formal psychosocial protocols rarely receive the same emphasis as in gender-violence cases, where they constitute a primary response. This imbalance prompts crucial questions about the psychosocial consequences of spyware surveillance – questions this project's scope prevents us from fully investigating, though existing research has begun this examination.[42]

[41] Maynier, E. (2020, 23 August). Some Thoughts About Stalkerware and Technology in Intimate Partner Violence. https://maynier.eu/blog/2020/08/23/some-thoughts-about-stalkerware-and-technology-in-intimate-partner-violence/

[42] Fundaccion Acesso has done excellent research about the psychological impacts of spyware. (The link will be added in the final version as it's yet to be published)

However, it's worth noting the risk of an essentialist perspective[43] that reductively frames gender violence (frequently narrowed to mean violence against women) as primarily emotional or abstract, thereby neglecting its material realities. Such a view risks both obscuring surveillance technology's tangible harms and perpetuating gendered assumptions about which forms of violence merit technical versus emotional interventions.

Fear remains a dominant feature in reported cases. According to Amnesty Tech:

> [B]ecause there's been a lot of media attention and public attention on spyware, a lot of people come to us because they think it's highly likely that they might have been targeted. And so there's a lot more interest now than there was, as we said. And so when you're working with the feminist helplines, I think this type of triaging process is really important because it's really scary. People are very worried about spyware, but it's often not the main threat that people are facing. So it's good to have that in mind for people when they're doing triaging, especially if they're not used to working on forensics.[44]

We advocate for an approach that understands the technical and political as inseparable dimensions in analysing and combating digital violence. When applied to feminist helplines practices, this perspective reveals its transformative potential: technical excellence in forensic analysis is not only compatible with psychosocial care but is strengthened when combined with it. In operational practice, this translates into methodologies that integrate investigative rigor with political sensitivity, where detailed examination of digital evidence goes hand in hand with attention to the emotional and social impacts experienced by affected people. This breaks with the false dichotomy that opposes technical objectivity to the subjectivity of care, proposing instead a comprehensive model of action that recognises the complexity of TFGBV and of the digital threats in general.

[43] Heyman, G. D., & Giles, J. W. (2006). Gender and Psychological Essentialism. *Enfance, 58*(3), 293-310. https://psycnet.apa.org/record/2006-21300-007

[44] Interview with Amnesty Tech, 17 October 2024.

3.

Digital forensics: From criminal field to consensual forensics

3.1 TRADITIONAL DIGITAL FORENSICS: A GLOBAL EFFORT ROOTED IN CRIMINALISTICS

Also known as computational forensics, cyber forensics and network forensics, digital forensics is generally defined as the scientific examination of digital evidence from electronic devices, typically divided into five phases: recovery, preservation, analysis, interpretation and documentation. This process must adhere to strict legal guidelines, ensuring evidence integrity and admissibility in court.[45]

The broader field of forensic sciences encompasses an array of disciplines with a common goal: the application of scientific and technological knowledge to aid in criminal investigations. The knowledge generated by these disciplines is systematically organised under the umbrella of criminalistics, which establishes a framework for the precise and secure application of forensic techniques in accordance with legal principles.[46]

In general terms, what we traditionally call forensics is deeply connected to the criminal justice system and depends on the creation of widely recognised procedures and guidelines. This is necessary in a field where forensic experts and other actors – such as lawyers and police officers – work together in legal investigations.

The development and adoption of forensic science have historically been heavily influenced by international standards and methodologies originating from the Global North, particularly in the context of international cooperation among law enforcement agencies. More than inspiration, international guidelines are often adapted to Latin American countries' directives and laws with an underlying militaristic tone. Notably, two of the most referenced authorities in the field of digital forensics are Interpol[47] and the National Institute of Standards and Technology (NIST), which belongs to the US Government.[48]

The digital forensics expert is called a computer forensic expert, a professional who combines technical knowledge in computing, law and forensic methodologies. Since the very nature of forensic work is integrated into each country's criminal system, the rules and qualification requirements for working in

[45] Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to Integrating Forensic Techniques into Incident Response*. National Institute of Standards and Technology. https://csrc.nist.gov/publications/detail/sp/800-86/final

[46] Velho, J. A., Geiser, G. C., & Espindula, A. (2017). Capítulo 1: Introdução às ciências forenses. *Ciências forenses: Uma introdução às principais áreas da criminalística moderna*. Millennium Editora, Campinas-SP

[47] Interpol. (2021). *Guidelines for Digital Forensics First Responders*. https://www.interpol.int/content/download/16243/file/Guidelines%20to%20Digital%20Forensics%20First%20Responders_V7.pdf

[48] Here we believe it is pertinent to highlight that this colonial legacy in the ICT field is part of what some authors call neocolonialism in the digital age: Avelino, R. (2023). *Colonialismo Digital: Tecnologias de Rastreamento Online e a Economia Informacional*. Alameda Editorial; Ricaurte, P. (2019). Data Epistemologies, The Coloniality of Power, and Resistance. Television & New Media, 20(4), 350-365. https://doi.org/10.1177/1527476419831640

this field vary significantly. Generally, most forensic work (also called perícia or peritagem) is performed by official examiners selected by the justice system. However, some countries allow independent examiners to engage in this practice.

In Spain, it is possible to hire private experts,[49] provided they hold a professional degree and are *acreditados expertos en la materia* (accredited experts in the field).[50] In Brazil, the official expert responsible for a case is appointed by the judge and must be a certified judicial examiner; however there is the option to hire an independent expert, called a technical assistant.[51] In Bolivia, all forensic investigative work falls under the jurisdiction of the police's Forensic Investigations Institute (IDIF).[52]

These examples are relevant to our research because they present the contexts where three of the interviewed helplines operate: Maria d'Ajuda (Brazil), to which we belong, SOS Digital (Bolivia), and FemBloc (Catalonia). Each of these organisations seeks to provide a counterpoint to traditional forensic application, although their challenges and possibilities differ.

Over time, the specialised capabilities of digital forensics have been adapted to the corporate world. Many of its techniques are now used to investigate business incidents that do not necessarily constitute crimes, such as internal policy violations or data leaks, representing a specialised type of incident response.[53] These two are strongly connected, as both serve to support victims of digital events, whether criminal or not. While they have distinct objectives – forensics focuses on evidence collection and analysis, while incident response prioritises containment and recovery – they complement and reinforce each other.

Digital forensic methodologies result from collaborative efforts involving various actors, including police, military, corporations and academia. The rigidity of procedures, such as maintaining chain of custody – whether in criminal investigations, corporate audits or academic research – ensures evidence integrity, which depends on using specific procedures and tools widely validated by this international community.[54]

The collaboration between the many players that constitute the digital forensics ecosystem also translates to a vast array of tools, including open-source and

[49] FemBloc. (n/d). Sistematización, preservación y validez de la prueba sobre las violencias machistas digitales. https://docs.fembloc.cat/legal-medios-prueba-procesojudicial.html

[50] According to Article 340 of the Law on Civil Procedure. https://www.boe.es/buscar/act.php?id=BOE-A-2000-323

[51] These roles are defined in Article 465 of the Brazilian Code of Civil Procedure. https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm

[52] https://www.fiscalia.gob.bo/quienes-somos/instituto-de-investigacion-forense

[53] National Institute of Standards and Technology. (2024). *Computer Security Incident Handling Guide*. US Department of Commerce. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf

[54] International Organization for Standardization. (2012). *ISO/IEC 27037:2012 Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence*. https://www.iso.org/standard/44381.html

enterprise-level solutions. Both types are widely used by forensic analysts worldwide and attempts to compile comprehensive lists of software often result in hundreds of entries with multiple tools serving the same purpose.[55] This redundancy is necessary during the analysis and extraction phase, since analysts often need to test multiple tools to get a satisfactory result. But given the sheer number of tools, with new ones emerging constantly, many professionals seek to utilise software that has undergone testing and approval by their peers.[56]

It is worth noting that these lists put together open-source software and enterprise solutions from cybersecurity giants. The same task – forensic data extraction from an Android device, for example – can be done with free command-line tools or with software included in million-dollar contracts like the FTK Forensic Toolkit and Cellebrite's suite.[57] In 2020, Brazil spent approximately USD 9 million (about BRL 55 million) to purchase investigative software from these international companies that are now widespread in every state. Argentina is one of the key markets for Cellebrite's forensic solutions, ranking third in the Americas licences, with over USD 1 million in documented contracts between 2018 and 2020.[58] Although there is no public data about Mexico's investments in the Israeli company, Cellebrite maintains strong operations in the country,[59] evidenced, for example, by the Cellebrite Connect México 2023[60] event, where the company presented its technological solutions and strengthened partnerships with local authorities.

Paradoxically, there are several notable contributions from Latin America to development open-source software, including a full Linux forensic operating system called Tequila SO, developed by students from Mexico's UNAM university.[61] Two Brazilian software tools are widely recognised within the global digital forensics community: developed by experts at the Brazilian Federal Police in 2012, IPED is a software for processing and analysing digital evidence.[62] A similar effort is Avilla Forensic, a free mobile forensic tool developed by São Paulo State Police and launched in February 2021, designed to assist investigators in obtaining information and evidence from mobile devices.[63] Both toolkits, if put together, can objectively perform the same activities as Cellebrite's main product, Universal Forensic Extraction Device (UFED), a tool that facilitates data extraction and transfer between various devices.[64]

[55] https://start.me/p/q6mw4Q/forensics and https://github.com/cugu/awesome-forensics

[56] Digital Forensic Research Conference. (2001). A Road Map for Digital Forensic Research: Report from the Digital Forensic Research Workshop, Utica, USA, 7 to 8 August. https://dfrws.org/wp-content/uploads/2019/06/2001_USA_a_road_map_for_digital_forensic_research.pdf

[57] Ramiro, A., Amaral, P., Canto, M., & Pereira M. C. M. (2022). *Mercadores da Insegurança: conjuntura e riscos do hacking governamental no Brasil*. Instituto de Pesquisa em Direito e Tecnologia do Recife. https://ip.rec.br/publicacoes/mercadores-da-inseguranca-conjuntura-e-riscos-do-hacking-governamental-no-brasil/

[58] Access Now. (2021). *Surveillance Tech in Latin America: Made Abroad, Deployed at Home*. https://www.accessnow.org/wp-content/uploads/2021/08/Surveillance-Tech-Latam-Report.pdf

[59] https://www.miguelgallardo.es/cellebrite-mexico.pdf

[60] https://cellebrite.com/es/events/cellebrite-connect-mexico-2023/

[61] https://tequila-so.org/

[62] https://github.com/sepinf-inc/IPED

[63] https://github.com/AvillaDaniel/AvillaForensics

[64] https://cellebrite.com/en/ufed/

Despite the recognition that our region has internationally in the open-source community, and the fact that digital forensic analysts constantly use open-source toolkits, Latin America's law enforcement agencies rely heavily on commercial tools with user-friendly interfaces, such as Cellebrite, Verint and Magnet forensics. There are multiple reasons for that, including major political lobbying,[65] but oftentimes the usage of these pricey commercial tools are perceived as necessary compromises, allowing individuals with less technical proficiency to operate them.[66] There are limited technical training among personnel in investigative agencies, many of whom are hired through rigid bureaucratic processes that do not always prioritise digital expertise.

To us, this justification falls short. The widespread adoption of these tools raises serious concerns, prompting two critical questions we initially posed:

- Weakening of data privacy for citizens: A potential infringement on the privacy rights of citizens to allow access to investigation data by the manufacturing companies. Products such as Cellebrite Advanced Services[67] is described as a tool that helps law enforcers alleviate backlogs by allowing experts to extract and decode data. Clients need only send compatible devices and they will receive a USB drive with the data. "In other words, investigation data must pass through the hands of Cellebrite, which collects, processes, and shares (and discards?) personal data of a suspected individual and the users in their network of connections".[68] Furthermore, it has been reported that Cellebrite tools are being sold on the black market, still containing sensitive information about past investigations.[69]
- Support for companies linked to human rights violations: Latin American governments routinely procure surveillance and forensic tools from firms with documented ties to human rights abuses – including the deliberate targeting of journalists, activists and dissidents through mass monitoring technologies.[70] Despite corporate claims that these tools serve legitimate investigative purposes, evidence reveals systemic failures in client vetting, with repeated sales to authoritarian regimes and private entities accused of weaponising them for political gain.[71] By sustaining commercial relationships with these suppliers, state actors risk direct complicity in enabling systemic rights violations.

[65] Dias, T. (2025, 8 July). Licenças de Bilhões. *Intercept Brasil*. https://www.intercept.com.br/2025/07/08/brasil-torrou-10-bilhoes-em-um-ano-com-bigtechs/

[66] Access Now. (2021). Op. cit.

[67] https://cellebrite.com/en/advanced-services/

[68] National Institute of Standards and Technology. (2024). Op. cit.

[69] Brewster, T. (2019, 27 February). The Feds' Favorite iPhone Hacking Tool Is Selling On eBay for $100 and It's Leaking Data. *Forbes*. https://www.forbes.com/sites/thomasbrewster/2019/02/27/the-feds-favorite-iphone-hacking-tool-is-selling-on-ebay-for-100and-its-leaking-data/?sh=57997d355dd4

[70] Marczak, B., Scott-Railton, J., McKune, S., Razzak, B., & Deibert, R. (2018). *Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*. The Citizen Lab. https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

[71] Feldstein, S., & Kot, B. (2023, 2 March). Op. cit.

3.2 CONSENSUAL DIGITAL FORENSICS

The subversive applications of forensic sciences by civil society are not new.

One of the primary records of what became known as *ciencia forense ciudadana* (citizen forensics) is the collective effort of groups like Las Buscadoras in Mexico. Faced with the state's failure to investigate disappearances (with over 100,000 unresolved cases since 2006), mothers, wives and sisters of victims began conducting independent searches using shovels, metal rods and forensic archaeological techniques in clandestine burial sites. Groups like Las Rastreadoras de El Fuerte (Sinaloa) and Colectivo Solecito (Veracruz) became experts at identifying remains, mapping graves and pressuring authorities with evidence – all while facing constant attacks and threats.

This appropriation of forensic expertise became an act of political resistance. By documenting evidence (clothing, DNA, GPS coordinates), Las Buscadoras not only filled the void left by the state but exposed its negligence. Their methods – once dismissed as amateur – are now recognised by institutions like the UN[72] and supported by forensic anthropology groups that train new searchers to become "forensic experts in their own right, while searching for their loved ones."[73] This community-based approach of *ciencia forense ciudadana* represents a courageous and vital challenge to the state's monopoly to produce evidence.

A similar logic applies to digital forensics. Faced with the need to gather evidence in cases of technology-facilitated human rights violations, independent groups are chosen over hiring companies or relying on state investigations. Organisations like Amnesty Tech and The Citizen Lab stand as notable examples, with years of experience producing forensic reports to expose technological abuses.[74]

However, not all sensitive contexts for human rights defenders involve sophisticated spyware like Pegasus or Quadream. As this issue has become more widely recognised, digital forensics applications have diversified to serve other purposes, benefiting organisations and individuals for whom government spyware is not necessarily the primary threat. Some examples:

- Forensic analysis for activists/human rights defenders. Individuals or civil society groups seeking judicial justice for human rights violations – often victims who distrust the judicial system and lack resources to hire private forensic experts.

[72] OHCHR Mexico. (2025, 9 May). Mensaje en ocasión del Día de las Madres. https://hchr.org.mx/comunicados/mensaje-en-ocasion-del-dia-de-las-madres/

[73] Schwartz-Marin, E., & Cruz-Santiago, A. (2014, 20 November). How citizens lead the search for Mexico's disappeared. *Al Jazeera*. https://www.aljazeera.com/opinions/2014/11/20/how-citizens-lead-the-search-for-mexicos-disappeared

[74] Scott-Railton J., Marczak B., Guarnieri C., & Crete-Nishihata M. (2017, 11 February). Op. cit.

- Internal investigations in non-profit organisations. Digital security audits are increasingly more popular within civil society organisations. Methodologies like SAFETAG, a well known audit framework, suggest some activities about digital forensics.[75]
- Investigations of human rights violations where the goal is not necessarily legal action but public exposure of the violations: Pegasus Project,[76] #GobiernoEspía,[77] report on cyber patrolling and open-source intelligence (OSINT) in Colombia,[78] and reports on targeted attacks against activists.[79]
- Holistic support for victims of security incidents: individualised assistance for activists, women, LGBTQIA+ individuals and other marginalised groups offered by digital security help desks for civil society.

This phenomenon of appropriating digital security methodologies and techniques is not unprecedented. Inspired by incident response procedures and risk analysis practices for NGOs, the concept of holistic security was created, integrating physical, psychosocial and digital security.[80] Nearly 10 years on, this methodological principle has been widely accepted and is prevalent in almost the entire community of DSHCS.

The incorporation of digital forensics into this field is an even newer phenomenon, making it difficult to define established practices and concepts, especially given the diversity observed among organisations. In our interviews, we found significant variations in methodologies, practices, workflows and even the objectives of these institutions. To name a few, The Citizen Lab and Amnesty Tech primarily focus on responding to advanced threats. Threat labs like Front Line Defenders and SocialTIC also conduct advanced analyses but handle a large number of cases referred by internal and external partners. Despite this, they do not prioritise producing forensic reports. Meanwhile, FemBloc is a feminist helpline whose main motivation is building capacity to offer forensic legal services for women victims of violence.

Despite this variety, it is important to name what we do to differentiate ourselves and reinforce our political stance: by centring forensics in civil society, we are not positioning ourselves within traditional forensics but rather as a counterpoint to it.

[75] https://safetag.org/activities/forensic_analysis/

[76] Forbidden Stories. (2021, 18 July). Op. cit.

[77] Articulo 19. (2017, 19 June). #GobiernoEspía a activistas, defensores de derechos humanos y periodistas en México. https://articulo19.org/gobiernoespia/

[78] Fundación Karisma. (2023). *Cuando el Estado vigila. Ciberpatrullaje y OSINT en Colombia*. https://web.karisma.org.co/wp-content/uploads/2023/02/Cartilla_Cuando_el_estado_vigila_2_V_WEB-1.pdf

[79] Amnesty International. (2020, 17 March). Targeted Surveillance Attacks in Uzbekistan: An Old Threat with New Techniques. https://www.amnesty.org/en/latest/research/2020/03/targeted-surveillance-attacks-in-uzbekistan-an-old-threat-with-new-techniques/

[80] Tactical Tech. (2016). *Holistic Security: A Strategy Manual for Human Rights Defenders*. https://holistic-security.tacticaltech.org/

Unlike corporate forensics or forensics done by police investigators, forensic analysis for human rights requires fully informed consent. The person under investigation must understand each step – what data will be collected, how it will be used, possible outcomes and limitations – before authorising the process. This approach, called consensual forensics, places the supported person at the centre, ensuring they retain control over the investigation, regardless of her technical knowledge.[81]

Beyond forensic expertise, this model requires a foundation of transparency and psychosocial support, blending technical analysis with comprehensive care. Ideally, consent should be obtained before initiating evidence collection. While many questions are addressed verbally in the early stages of an investigation, using a written document to formalise key agreements is strongly recommended. Organisations such as SocialTIC and MariaLab share adaptable consent agreement templates, which other groups can freely customise.[82]

Collaboration and technology development

The collaborative angle appeared frequently in interviews with expert interlocutors. As highlighted in these conversations, one of the main challenges faced by these organisations is the need to adapt existing tools and methodologies – originally designed for law enforcement – to effectively address the unique requirements of human rights investigations.

In response to these specific demands, some developers have taken the initiative to create custom tools that integrate existing open-source components with newly developed functions, which were previously only available in expensive proprietary tools. Examples of tools developed with free software and aimed at civil society applications are PiRogue and Colander. Both are developments of the PTS Project,[83] a platform designed to “provide accessible and powerful tools for network analysis, mobile forensics, and collaborative case management, specifically tailored for civil society, digital rights defenders, researchers, journalists, and regulatory bodies.”

- Colander: An incident management platform that organisations can instal on their own servers. It collects events (such as network traffic, alerts), artefacts (files and backups, APKs), and other technical and contextual information, turning them into navigable knowledge.
- PiRogue: A hardware device based on open-source Raspberry Pi, which functions as a network router, analysing network traffic in real time. PiRogue helps detect potential compromise of a mobile device.

[81] SocialTIC. (2025, 3 February). Explainer: Introducción a la forense digital consentida para la defensa de los Derechos Humanos. https://forensics.socialtic.org/explainers/01-explainer-introduccion-forense-digital/01-explainer-introduccion-forense-digital.html

[82] https://marialab.org/feministforensic

[83] https://pts-project.org/

In the interview with Esther Onfroy, CEO of Defensive Lab Agency, the developer of these tools, emphasises that "the main goal of PiRogue Suite is to provide people with tools that are free to use so they can equip themselves at low cost." But that is not the only key difference between PTS project and commercial tools. Before their development, Defensive Lab Agency's founder decided to deepen her understanding of the mobile device ecosystem from a human rights perspective: "I continued developing tools while staying in contact with different organisations so that I can hear from them – what are their issues, what are their needs." This relationship is not one-directional, as she is also part of a feminist organisation that provides incident response support for civil society, making her a user of her own tools.

This type of initiative also facilitates access to certain forensic capabilities for organisations with less infrastructure and advanced technical capacity. Network traffic analysis, which PiRogue is designed to facilitate, can be done in other ways – for example, by setting up a VPN server and routing users through a VPN client, as Conexo does:

> Basically, we set up a VPN that we control, capture the traffic, analyse it – more or less how it works is that we filter all the traffic and only keep the things that are unusual or uncommon. It doesn't necessarily mean they're malicious; but yes, for example, it's not Facebook, not Twitter, not Instagram, not the thousands of domains Google uses – things we know aren't suspicious.[84]

The high financial – and human – cost of using advanced digital tools is not the only barrier driving the development of custom software for our field. There are specific needs in consensual forensics that commercial tools are not designed to address. For instance, the need to perform remote mobile analysis – a less common requirement in law enforcement – led Amnesty Tech to develop Androidqf.[85] This tool combines several open-source components, including Android Debug Bridge (ADB) – the industry standard for Android extraction and manipulation – and Mobile Verification Toolkit (MVT).[86] In its interview, Amnesty Tech explained they prefer working with local partners who handle the first line of triage, collecting forensic data and sharing it through secure channels, but in many cases, they are forced to conduct extractions remotely.

> And more often than not, people can follow instructions autonomously to collect the data and upload it to us. So usually, it's pretty straightforward. Of course, there are people at different levels of risk – maybe with

[84] Interview with Conexo, 11 September 2024.
[85] https://github.com/botherder/androidqf
[86] https://github.com/mvt-project

> varying technical skills, poor internet connections, or other challenges that make the process more difficult. In those cases, we rely on someone local who speaks their language or can meet them in person to guide them through it.[87]

This is also the preferred method for Front Line Defenders, which has internal partners in different parts of the world. "Usually, those cases come to us from digital protection coordinators or general protection coordinators, so the difference lies in those internal referrals, let's say."[88]

Despite the clear advantages of in-person collections, there are many cases where it is not feasible, being almost the norm for feminist helplines. Maria d'Ajuda has not developed software for consensual forensics, but maintains secure online communication tools for its helpline and partner organisations. Instead of using popular tools like Zoom or Google Hangouts, MariaLab supports cases through a BigBlueButton[89] instance, hosted in its own server without collecting any user data or metadata. This is part of a broader feminist infrastructure project called Maria Vilani.[90]

FemBloc, on the other hand, chose to offer support through multiple channels, offering assistance via phone and WhatsApp:

> So, our communication methods keep adapting based on digital gaps, the tools people already use, and the paths they've taken to reach us – because these factors change constantly. All of this also influences which communication channels we prioritise. We've also made Telegram and Signal available, though Signal is the only encrypted option we offer – but nobody uses it.[91]

Case documentation and the ability to share threat intelligence are other motivations for developing software. Some groups, like CiviCERT,[92] has a Malware Information Sharing Platform (MISP) instance reserved to trusted members.[93] This is an attempt to exchange threat intelligence with a special focus on civil society and online activism cases. But MISP is a complete and robust platform, which often seems too complex and highly specialised in technical indicators while lacking visualisation of other relevant data, such as risk assessments and psychosocial indicators. Colander[94] has similar capabilities to

[87] Interview with Amnesty Tech, 17 October 2024.

[88] Interview with Front Line Defenders, 11 October 2024.

[89] https://bigbluebutton.org/

[90] https://mariavilani.vedetas.org

[91] Interview with FemBloc, 1 October 2024.

[92] https://www.rarenet.org/resources/

[93] https://www.misp-project.org/

MISP, but it also tries to represent knowledge in more graphical ways, allowing analysts to build documentation focused on human rights topics:

> For example, in Colander, you have only very generic types of information you can represent – so it's very flexible, and you can use your own taxonomy, your own ontology. Sometimes users struggle when starting with Colander because it's more like a sandbox – you don't really have a starting point. You start wherever you want.[95]

It is important to mention that despite the excellent quality of the tools created, digital forensic experts still rely on many other tools to perform deeper forensic analysis. During our participation in the Latin American consortium led by Fundación Acceso, we compiled a list of software that organisations were currently using.[96] Reviewing this list reinforces the conclusion that technical training remains necessary for other groups to adopt technologies for consensual forensics – whether or not they were developed specifically for this field.

[94] https://pts-project.org/docs/colander/deployment/
[95] Interview with Defensive Lab Agency, 10 October 2024.
[96] https://marialab.org/feministforensic

4.

Helplines addressing digital violations

The expert organisations interviewed for our study – identified in Section 2.1 – operate in the digital security field through three primary approaches:

- Technical independent audits and consulting
- Training and capacity-building programmes
- Development of educational materials.

While many of these digital security organisations often end up responding to emergency incidents, this does not constitute their primary activity – a role that is typically fulfilled by specialised security helplines.

Among the organisations interviewed, Access Now and Amnesty Tech have dedicated helplines with a clear mandate to support civil society organisations, journalists, human rights defenders and activists. Access Now offers 24/7 emergency support and long-term digital protection in multiple languages. The helpline offers real-time assistance for urgent threats like compromised accounts, surveillance incidents and cyberattacks, while also conducting preventative training and developing multilingual resources to strengthen digital resilience. As one of the first global initiatives of its kind, the helpline has become a critical resource for at-risk communities, combining technical expertise with human rights-centred solutions.

Amnesty International’s Security Lab provides specialised digital protection support, assisting with urgent cases such as targeted spyware attacks (e.g. Pegasus), phishing attempts and forensic analysis of compromised devices. Beyond emergency response, it offers preventive resources, including threat assessments and secure communication tools, with a focus on high-risk individuals and marginalised communities.

These helplines are focused on human rights defenders and civil society but do not cover situations outside these groups. However, when examining the human rights landscape through a broader lens, it becomes evident that digital violations against socially marginalised groups also pose a significant human rights concern, even when the affected groups do not belong to formally organised civil society structures. This is why feminist helplines – as part of the broader community of digital security help desks for civil society – play a fundamental role in providing direct assistance to victims of gender-based violence, racism and LGBTQIA+ phobia.

4.1 FEMINIST HELPLINES

The origins of feminist helplines can be traced back to solidarity networks organised by women, LGBTQIA+ individuals, and migrants to share information about reproductive rights, safe routes and resources against systemic oppression.[97] As detailed in the Feminist Helplines Index,[98] the key differentiator of feminist helplines is their survivor-centred, trauma-informed approach, which considers how gender, race and other identities exacerbate impacts of digital violence. Threats such as doxing, surveillance or non-consensual data leaks are addressed through both technical and political strategies, redefining digital safety from the perspective of marginalised experiences.

We, as part of feminist helplines, come from the understanding that human rights violations – particularly gender-based violence, racism, ableism and xenophobia – are socially structured and affect individuals not only because of their activism but because of their identities. While these groups may not be the primary targets of high-cost surveillance software, they are still impacted by a culture of digital surveillance and control that predates and extends beyond the spyware crisis.

The feminist digital helplines participating in this study are relatively new, having been established within the last decade – some during the COVID-19 pandemic.[99] Beyond the health and economic crisis, feminist organisations and advocates for women's rights warned of a surge in domestic and gender-based violence. For many individuals, particularly those residing with perpetrators, the domestic environment was not safe.

Recent scholarly literature converges on the notion that the confinement, isolation and heightened tensions engendered by the pandemic exacerbated the prevalence of violence against women and gender-dissident individuals while hindering their ability to seek assistance. Simultaneously, the widespread migration of labour, academic and social activities to online platforms, intensified during the pandemic, leading to a significant increase in time spent online. In response, the utilisation of online support networks became highly prevalent.

Despite being established independently by entities in various countries, the feminist helplines examined in this study exhibit a remarkable degree of convergence behind their creation and operational practices. We compiled a table of these helplines involved in this study to provide a clear overview of each group's scope and specialisation (see Table 2).

[97] https://feministhelplines.org/about/

[98] Ibid.

[99] Among the five helplines that are part of this study, only Navegando Libres and SOS Digital were launched before 2020; in 2018 and 2019 respectively. The others began their development during the COVID-19 pandemic, mostly motivated by an increase in the number of cases.

Table 2 Feminist helplines involved in this study

Helpline/Year founded: Navegando Libres por la Red 2018

Organisation of origin and country: Taller de Comunicación Mujer (Ecuador)

What motivated the creation of the helpline

The digital security helpline Navegando Libres por la Red was launched to address needs uncovered while monitoring gender-based violence and abortion cases in Ecuador.

In 2016, after addressing cases involving multiple forms of technology-facilitated violence simultaneously, the team from Taller de Comunicación Mujer began its transformation to promote a feminist approach to the internet and technologies.

Contact channels

Telegram

Signal

WhatsApp

Secure emai

Areas of service

Training in holistic and digital protection

Development of specific strategies to mitigate digital gender-based violence

Teams

Four people: one in charge of coordination and three follow up on cases. The team has a background in social sciences, such as anthropology and gender studies, and receives technical training in digital protection and digital care.

Supported groups

Women, children and adolescents. Members of the LGBTQIA+ community

Migrant or refugee women and LGBTQIA+ individuals

Feminist and human rights/land rights groups.

Challenges in support cases

Situations where digital violence coexists with other kinds (physical, sexual or psychological) or social vulnerability. Cases involving platforms like WhatsApp, where intervention options are limited. Cases involving suspected spyware are particularly challenging due to the team's limited forensic analysis knowledge, the inherent complexity of such cases and the myths surrounding them.

Table 2 Feminist helplines involved in this study

Helpline/Year founded: SOS Digital 2019

Organisation of origin and country:

Taller Internet Bolívia (Bolivia)

What motivated the creation of the helpline

The SOS Digital helpline was established in response to the Bolivian Government's inaction in addressing digital gender-based violence.

In 2019, amid a widespread political crisis, there was limited information on how to combat gender-based violence. The SOS Digital centre was founded to provide a feminist and intersectional response to this issue.

Contact channels

Telegram

Signal

WhatsApp

Areas of service

Emotional support

Technological support

Legal advice

Teams

The team consists of five members: three members with experience in the social field, a lawyer and a telecommunications engineer.For certain activities, they are supported by Fundación Internet Bolivia's communications team and technology specialist.

Supported groups

Adolescent girls, women experiencing any form of gender-based violence, activists, LGBTQIAPN+ individuals, journalists and women in politics.

Challenges in support cases

Cases with high risk of escalating into physical or sexual violence. Violence through WhatsApp or Telegram. Individuals who need legal support but cannot afford a lawyer. Suspected presence of spyware on phones.

Table 2 Feminist helplines involved in this study

Helpline/Year founded: Luchadoras 2020

Organisation of origin and country: Luchadoras (México)

What motivated the creation of the helpline

Before formally establishing the helpline, Luchadoras' team did a study on women's and gender-diverse individuals' experiences with digital violence in Mexico.

The research aimed to map the different forms of this violence and understand its impacts.

Their findings naturally led to supporting cases, which increased over time, becoming an institutional priority.

Contact channels

Social media

Email

Direct call via

Areas of service

Legal support

Psychological support

Technical support for digital platforms and digital care

Teams

The team consists of three psychologists: One is in charge of coordinating the helpline and two directly monitor the cases.

Supported groups

Mainly women, young people and gender dissidents, activists, feminists and human rights defenders in general

Challenges in support cases

Cases related to unauthorised access to information and accounts

Suspected intervention in devices by spyware

Table 2 Feminist helplines involved in this study

Helpline/Year founded: Linea de atención de Técnicas Rudas 2021

Organisation of origin and country:

Técnicas Rudas (México)

What motivated the creation of the helpline

Digital security support has always been one of Técnicas Rudas' core priorities.

While they had supported cases since 2017, it was only in 2021,through an Access Now project, that they established a dedicated helpline. This allowed them to provide free assistance and include emergency services (previously, their work focused on medium- and long-term monitoring).

Contact channels

Referrals and recommendations.

Email

Signal

Areas of service

Follow-ups are based on a risk analysis with emphasis on digital security and the creation of a protection plan.

Teams

The team consists of four people working in digital security, and recently one member of the group participated in a mentoring programme that enabled them to incorporate malware detection into their work plan.

Supported groups

People from the LGBTQIA+ community, land defenders, journalists and human rights defenders in general.

Challenges in support cases

Rural or hard-to-reach contexts

Time constraints and limited availability of individuals.

High levels of stress and social vulnerability.

In certain situations, the team encounters technical limitations or gaps in specific knowledge that hinder optimal intervention.

Table 2 Feminist helplines involved in this study

Helpline/Year founded: Maria d'Ajuda 2023

Organisation of origin and country:

MariaLab (Brazil)

What motivated the creation of the helpline

Since its creation, MariaLab frequently handled digital security incident cases received through its official channels or members' personal contacts.

However, during the COVID-19 pandemic, Brazil saw an increase in various forms of gender-based violence, which led the organisation to formalise a structured helpline.

Maria d'Ajuda was established in 2021, with the dual purpose of providing a dedicated channel for digital security support and systematising case management.

Contact channels

Requests are only received via a secure email address that redirects to a ticketing system.

Areas of service

Digital care training

Digital security for organisations

Digital security on social media

Teams

The permanent team consists of four people – two responsible for case triage and initial actions, one system administrator and one forensic specialist.

When cases proceed to full support or forensic analysis, they are referred to another team. This team consists of two support staff and three digital security consultants who are requested only when needed.

Supported groups

Women and the LGBTQIA+ community, feminist organisations, human rights organisations and activists.

Challenges in support cases

Continuity of medium and long-term support. Remote assistance in cases requiring more complex analysis.

The lack of response by social media platforms.

Most cases involve social media, where responses are limited. The organisation is working on a communications plan to diversify cases.

In the following paragraphs, we highlight some important findings from the comparative overview of helplines.

A foundational and common concept in feminist helplines' care approach is the ongoing support that is offered – also called *acompañamiento* in Spanish or *acompanhamento* in Portuguese. This terminology represents an ongoing collaborative process rather than a one-time service provision. Rooted in feminist principles, this approach emphasises autonomy and capacity-building for those seeking support, focusing on a learning process rooted on three interconnected goals:

- Building capacity through knowledge by providing information and facilitating discussions on how technology and the internet work and what political issues are involved.
- Developing practical skills to independent comprehension and informed decision-making about safety measures.
- Introducing secure and free alternative tools to expand communication options beyond reliance on large commercial platforms (Big Tech).

Autonomy is also related to the self-determination of the supported person. Above all, safety measures must align with and respect the individual's choices and preferences. This understanding is rooted in the longstanding practice of feminist movements in supporting victims of sexual violence. Even in technical cases, there is no single correct answer. For this reason, the initial hearing and risk assessment are essential for fully understanding each case.

Despite the many similarities, there are some important differences between the helplines mentioned:

- With the exception of Luchadoras, which was founded independently, each helpline originated as an institutional derivative project, enabling continuity and growth of existing operations.
- There are a variety of channels for contact and each organisation determines its choice based on distinct considerations. Social media and messaging applications offer advantages like widespread popularity and easy accessibility – enabling quick connections to emergency support. While email communication may not provide the same immediacy as other channels, it offers greater control over information flow and enhanced security measures.
- Contrary to initial assumptions, the helplines teams are not predominantly composed of information technology professionals. Rather, they are multidisciplinary groups that develop technical expertise primarily through hands-on experience and targeted training within the helpline work itself.

- All helplines address gender-based violence, but it is important to note that Maria d'Ajuda and Técnicas Rudas don't provide this support exclusively. Both have prior experience in digital security for human rights organisations, and they continue this work through their respective helplines.

One of the most relevant aspects of this comparison analysis is the identification of key challenges in case management. Common issues include the difficulty of holding social media platforms accountable for adequately moderating violent content, overlap of multiple forms of violence in online abuse cases, and frequent disruptions in support services due to unreliable internet access. However, the most critical finding is that all helplines (except Maria d'Ajuda) reported a need for strengthening technical capacities to effectively address cases involving digital surveillance and illegal monitoring.

4.2 THREE DAYS OF DIGITAL FORENSIC PRACTICES: COMUNIDAD. FORTALEZA. CRIANZA MUTUA AND FORRÓ

In February 2025, we held an in-person gathering with representatives from each feminist helpline participating in this project. Fourteen women and trans people from six countries (Brazil, Argentina, Canada, Ecuador, Bolivia and Mexico) were brought together and spent three days immersed in a cosy house, sharing meals, bedrooms, laughter and stories. Before the event, we facilitated online meetings where we collected reports about each helpline's experience with recurring case examples that motivated them to seek forensic knowledge. The examples were rich and remarkably similar, which helped us prepare a didactic structure to the meeting agenda.

From the beginning, we expected this space to be more than an intensive digital techniques practice session. In the first activity, we used a methodology inspired by the essay *The Carrier Bag Theory of Fiction* by author Ursula K. Le Guin.[100] This icebreaker activity served as a playful way to begin introductions, but it also laid the foundation for an open and collaborative knowledge creation process. Through this dialogue, we distilled our ideas down to three main points that became the pillars of our research process: *Comunidad. Fortaleza. Crianza mutua.*[101]

A common characteristic among participants is their view of digital care as an integral part of a capacity-building and skill development process. The group itself consists of diverse individuals, each bringing their own experiences, activism,

[100] Le Guin, U. K. (1986). *The Carrier Bag Theory of Fiction*. https://theanarchistlibrary.org/mirror/u/uk/ursula-k-le-guin-the-carrier-bag-theory-of-fiction.pdf

[101] Araujo, D., & Carl. (2025, 28 April). Bringing the energy home. *GenderIT.org*. https://genderit.org/index.php/feminist-talk/bringing-energy-home

cultures and passions. When these elements intertwine, they create a rich tapestry of knowledge that manifests best in broader discussions rather than narrowly ultra-specialised activities.

Bringing these reflections to the beginning of a meeting focused on sharing specialised practices was intentional and deeply symbolic. Thus, when we concluded our gathering with a *forró* (a Brazilian dance) workshop, it served not only as an enjoyable activity connecting us to our bodies and each other but also as a way to celebrate and experience a rhythm recognised as part of Brazil's intangible cultural heritage.[102]

The forensic practices were organised around a simulated incident, covering all steps from receiving the case to its conclusion. At each stage, we discussed how each organisation performs its work, sharing the basic principles of our approach. This was the contextualisation for the practical digital forensic sessions, which covered the following topics:

- Triage techniques for forensics: Initial case questions and Android security checks
- Android forensic extraction using Androidqf and MVT tools
- Google Takeout data extraction and analysis
- PiRogue installation and introductory network traffic analysis

To make examples more realistic and applicable, we brought pre-infected Android devices with common stalkerware whose complete forensic investigation can be reproduced with the guide *Mobile Forensic Analysis: A Case Study Walkthrough.*[103]

Beyond being a training about forensic techniques, the meeting was a moment of sharing and collaboration among us and resulted in a rich debate about what we want when applying forensic analysis with a feminist care perspective.

[102] Tolentino, I. (2019, 24 October). Forró and the Relationship between Music, Dance and Identity. *Corpuslab*. https://corpuslab.info relacoes-entre-musica-danca-e-identidade/?lang=en

[103] Greater Internet Freedom. (2024). *Mobile Forensic Analysis: A Case Study Walkthrough*. https://greaterinternetfreedom.org/course forensic-analysis-a-case-study-walkthrough-part-01-starting-a-case-and-preliminary-triage/

5.

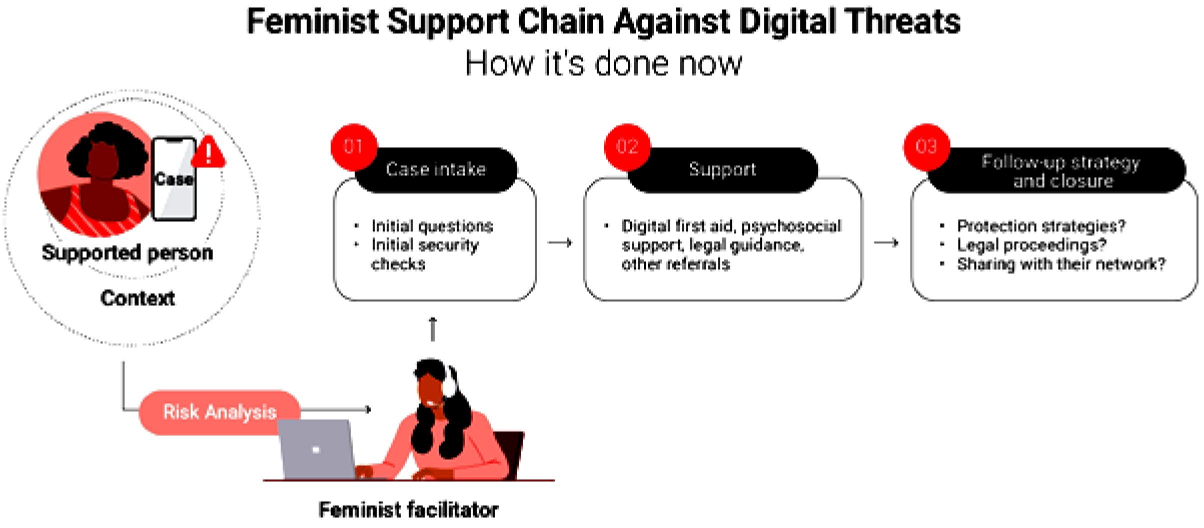
Feminist forensics

5.1 FEMINIST SUPPORT CHAIN: A VISUAL SUMMARY

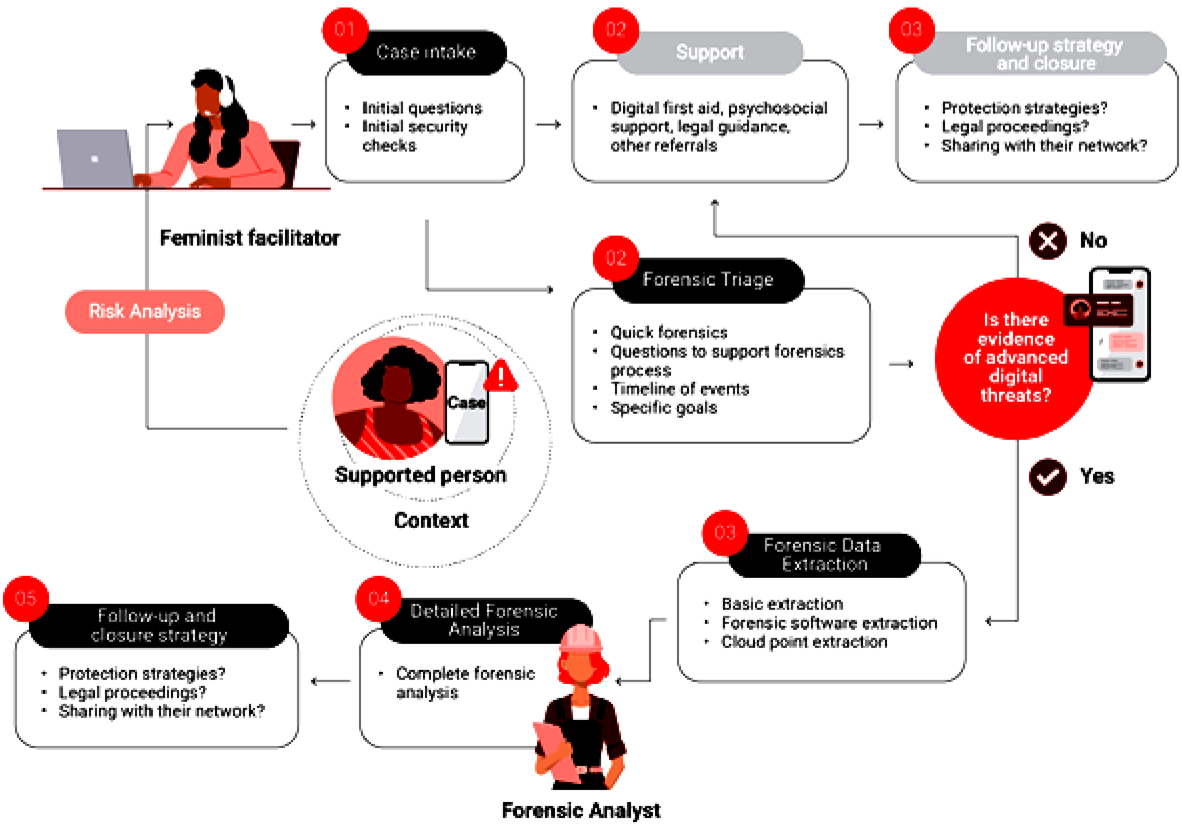
During the various phases of working with the feminist helplines, we noticed that no matter how unique each helpline is, there are many similarities in how we respond to digital incidents. Through dialogues, we designed a visual summary of our mutual support process, which we named Feminist Support Chain.

Initially this design contained no digital forensic practices or specialised triage. All investigation and triage activities conducted by the helplines were concentrated in the moment for receiving the case and doing individualised check-ups, later directed to specialised support.

To this model, we added a proposal for integration with consensual forensic analysis. Our expectation is to expand this support chain model by including partner organisations that accept referred cases, with whom the feminist facilitator would interact directly.

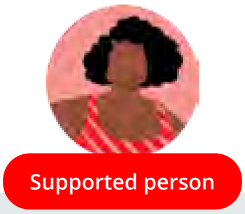

Feminist Support Chain Against Digital Threats
How it's done now
Case
Supported person
Context
Risk Analysis
Feminist facilitator
01
Case intake
• Initial questions
• Initial security checks
02
Support
• Digital first aid, psychosocial support, legal guidance, other referrals
03
Follow-up strategy and closure
• Protection strategies?
• Legal proceedings?
• Sharing with their network?

Feminist Support Chain Against Digital Threats


Feminist facilitator
Risk Analysis
01 Case intake
Initial questions
Initial security checks
02 Support
Digital first aid, psychosocial support, legal guidance, other referrals
03 Follow-up strategy and closure
Protection strategies?
Legal proceedings?
Sharing with their network?
Case
Supported person
Context
02 Forensic Triage
Quick forensics
Questions to support forensics process
Timeline of events
Specific goals
Is there evidence of advanced digital threats?
No
Yes
03 Forensic Data Extraction
Basic extraction
Forensic software extraction
Cloud point extraction
04 Detailed Forensic Analysis
Complete forensic analysis
Forensic Analyst
05 Follow-up and closure strategy
Protection strategies?
Legal proceedings?
Sharing with their network?

In this proposal there is a new key actor called the forensic specialist and two additional phases that the feminist liaison can perform before the analysis: triage for forensics and forensic data extraction.

Who participates in this chain



Supported person

“Acolhida” (PT-br), “acompañada” (es); victim, survivor,affected person.

An individual seeking support following a digital security incident, often due to their activism, human rights work, or affiliation with a marginalized group, requiring specialized help from organizations specialized in such communities.

Feminist facilitator

“Acolhedora” or “atendedora” (PT-br), “acompañante” (es)

Digital security helpline staff, supporter or consultors who work from the perspective of digital care, holistic care or protection for activists and human rights defenders. Trusted person who have already undergone security training, workshops or audits, seen as a reference within partner groups.

Forensic expert

Forensic specialist, forensic expert.

Organizations and/or people working for civil society with this objective. Digital security helpline staff who have this knowledge. Independent professionals hired for technical consultancy (depending on the context and risk analysis).

It is important to highlight that this type of cooperation between local partners and forensic specialists already occurs in the internal flow reported by expert organisations. Not all experts interviewed have a digital security helpline, but they all evolved their practices towards a holistic and organised response, working together with other digital security facilitators who are closer to the ones seeking help.

By incorporating forensic triage and forensic data collection phases into feminist helpline operations, we hope to facilitate the same type of qualified relationship that already exists between these organisations. Obviously, nothing prevents forensic analysis from being conducted internally by helplines that wish to build this capacity (as is the case with FemBloc and Maria d'Ajuda), but when looking at the support chain as a whole, we recognise that diversity is necessary since no technical practice answers all questions.

Forensic analysis alone cannot fully address the complex threat models behind surveillance, gender-based violence or the persecution of activist work. Digital forensic training of facilitators who are closer to the victims is also relevant to this chain and can contribute to more effective responses.

Which is why we felt the need to write another document parallel to this research, an informative guide detailing the Feminist Support Chain and our proposal for its integration with consensual forensics. In the document, we list procedures created by us and other groups, whose language and pedagogical approach are tailored to engage with the field of digital care – particularly in the new phases of triage for forensics and forensic data extraction.[104]

The inclusion of the triage for forensic phase in the Feminist Support Chain represents a new layer of analysis, aiming to identify evidence of more sophisticated digital threats. Unlike the initial triage – which focuses on more common causes like misconfigured dual-use applications or unauthorised access to cloud accounts – at this stage we look for patterns of suspicious activity. This analysis does not require specialised forensic software, and can be done through reviewing system settings and key indicators via the device's graphical user interface (GUI). The goal is to detect suspicious apps or configurations that may indicate stalkerware or other malware, while assessing whether a forensic analysis is necessary.

From a holistic perspective, we understand that this qualified evidence-gathering also functions as a psychosocial tool: the technical review process,

[104] https://marialab.org/feministforensics

when conducted during support with transparency and empathy, helps validate concerns and reduce the emotional impact of digital violence.

Once there is any indication of the need for forensic analysis, the feminist facilitator assumes the crucial role of informing the victim and does the data extraction. This phase is conditioned by multiple factors: the professional's technical expertise, the supported person's conscious choices, operational limitations (such as the need for remote collection and internet quality) and the potential judicial use of evidence – in which case forensic protocols must be strictly applied, including preserving the chain of custody.

Regardless of these factors, there are various extraction possibilities that are not limited to a single technical approach. The feminist facilitator can collect relevant contextual information, such as specific analysis objectives and reconstruction of an incident timeline with date and time records. Some evidence can be obtained without specialised tools, like system logs and cloud account access logs. Even when forensic software is necessary, there are options with simplified interfaces, like Androidqf, which can be used by mostly anyone after proper training.

One practice in particular stood out in our experience: extracting Google account data using Google Takeout.[105] Since Google accounts are intrinsically linked to Android devices – through app synchronisation, login credentials and system resource access – the analysis of this data can be complementary and possibly reveal unauthorised access to files, emails, security settings and other sensitive information in the Google ecosystem.

Two aspects of this technique deserve emphasis: first, this information is highly relevant for TFGBV cases commonly handled by feminist helplines, such as account theft and unauthorised access to personal files. Second, we identified a significant gap that there are few references about the forensic usage of this data, both in traditional forensics and consensual digital forensics. This void in literature and existing practices motivated us to write a full tutorial.[106]

Both the guide and the tutorials are examples of contributions that the field of consensual digital forensics can offer to improve the support of cases of TFGBV. Aimed at feminist helplines, all the knowledge that we are gathering in our repository has been created for digital security help desks for civil society and can be freely reproduced, adapted and remixed.

[105] This tool was developed by Google to enable users to download their stored data. Some of the extracted information contains forensically relevant data for Android device investigations. https://takeout.google.com

[106] https://marialab.org/feministforensic

5.2 OUR CONTRIBUTIONS FOR DIGITAL FORENSICS

Feminist digital forensics can only exist within a feminist support cycle.

This cycle begins at the first point of contact and it extends far beyond mere evidence collection or legal case-building, actively pursuing pathways to holistic repair. We recognise that the search for judicial justice must not overshadow other forms of reparation, such as restoring mental well-being and reclaiming autonomy.

The feminist approach in helplines extends beyond addressing gender-based violence cases, though this remains a core component. A distinctive feature of these helplines is their personalised support that transcends solving specific technical issues. By recognising the complexity of violence-related experiences, they provide safe spaces for affected individuals to voice their fears, insecurities and doubts. Active, empathetic listening forms a fundamental pillar of this process, fostering trust-building relationships.

Given the uniqueness of the work carried out by feminist helplines, we conclude this study by expanding our initial research question. Beyond examining how digital forensics could support the fight against TFGBV, we also find that the feminist perspective of care makes a significant contribution to the development of consensual digital forensics.

We advocate for a feminist lens to advanced digital threat response – one that acknowledges digital forensic examination as an important component of, but not equivalent to, the entire support chain. This begins with re-examining several key concepts:

1. From dead artefacts to living people

Traditional forensic analysis uses traces from past events to accurately reconstruct the facts of what occurred. In informal language, they say that forensics focuses on dead data and even call relevant traces by the name of artefacts. On the other hand, feminist digital forensics is about living people. The ones seeking support are our priority and their needs guide the process, even when they differ from what analysts or facilitators might recommend.

2. Clear language, not jargon

Demystify digital forensics by explaining it simply – what it can (and cannot) achieve, its risks and its real-world implications without technical obfuscation. Technical and specialised language creates barriers to comprehension and self-determination for those receiving support. While forensic analysis requires technical precision, the communication of findings must be clear, accessible and delivered in the individual’s own language.

3. Simple, not superficial

Offer straightforward and thorough explanations of analysis goals, limitations and possible outcomes – ensuring informed participation without oversimplifying complexities. Forensic analysis results must be contextualised to the supported person's reality, with clear connections to their daily life – making them relevant enough to be taken seriously, but not so alarming as to cause distress.

4. Data autonomy and informed control

Clarify: What data is being analysed? By whom? Where and how long is it stored? Technology-facilitated violence often entails loss of autonomy and control over personal data. The investigation and response process must therefore counteract the original violation by actively restoring the individual's control of their information. Beyond being an ethical and security requirement in forensic analysis, this approach specifically aims to prevent re-victimisation.

5. Participatory process

Where possible and desired, involve individuals in investigation steps. There are multiple stages where supported persons can meaningfully participate, such as in device data extraction or creating a timeline of case-relevant events. This approach strengthens autonomy and also fosters deeper understanding of both ongoing actions and necessary future protective measures.

6. Consent is not a checkbox; it is an ongoing conversation

Use signed forms where needed, but other forms of consent mechanisms can be developed. Consent must be freely given, informed and unequivocal, and may be withdrawn at any time. While this may sometimes hinder the analysis, the priority must always be to respect the supported person's defined priorities.

7. Minimal data is good, but it must work

Limit data collection to necessities, but ensure the entire support chain has what it needs – with clear referrals for issues beyond a facilitator's expertise. While these cases can offer valuable insights, it is critical to avoid treating their experience as a training tool; instead, focus on collaborative problem-solving that centres their needs.

8. Transparency as protocol

It is important to conduct regular check-ins to update the person on the analysis progress, jointly evaluate next steps, and collaborate on decisions if threats are confirmed. Transparency builds trust and also has a learning component, improving the understanding of the process.

9. Communication with care

Forensic work does not end with a technical report; it culminates in how findings are communicated and integrated into individuals' lives. The main objectives of a feminist support chain is to replace technical reports with ongoing dialogue – where findings are explained contextually, questions welcomed proactively, and safety plans co-created.

10. "Who watches the watch(wo)men?"

Care for caregivers' support structures is vital for responders handling trauma-heavy cases. The impact on the lives of those supporting technology-facilitated violence cases is often overlooked. Prolonged exposure to trauma narratives inevitably compromises facilitators' mental and physical health. Maintaining the support chain requires more than training and knowledge updates – it involves creating systematic decompression mechanisms and ongoing care structures for internal teams.

We believe that applying a feminist intersectional approach to digital forensics is necessary because, historically, women, gender dissidents and racialised groups have been systematically rendered invisible in the production of technological knowledge – a domain culturally constructed as masculine. This erasure produces a paradox that embodied minorities navigate daily, yet under the weight of systemic fear.

Our shared goal as helpline practitioners – and above all, as digital rights activists – is to transform digital technology and the internet into living spaces: spaces where people can chart their own paths and where technology itself can be reimagined through the prism of our identities and struggles.

Feminist digital forensics:
A study and a proposal for development

maria
[lab]

feminist
internet
research
network

APC
ASSOCIATION FOR
PROGRESSIVE
COMMUNICATIONS