por los Derechos Civiles

¿Who Searches Your Phone?

Status of mobile device forensic extraction tools in judicial and law enforcement decisions

PART 2

September 2022
adc.org.ar

Author: Luis García Balcarce
Layout and design: El Maizal - Cooperativa de Comunicación

Contents

Executive Summary

Our mobile phones contain all kinds of data that ranges from photos, videos and emails to information about our health, the places we visit and our leisure time. This data, in the case of certain crimes, allows the authorities to investigate and prove certain facts. Mobile device forensic extraction tools are used for this purpose. These tools are software and hardware supplied by private companies to security forces and prosecutors to extract and analyse the information held in our mobile phones.

This report continues the research published by the Association for Civil Rights (ADC) in December 2021: *Who Searches Your Phone?*[1] On this occasion, the research focuses on the use of forensic extraction tools by the Argentinian National Gendarmerie (GNA), the Police of the Autonomous City of Buenos Aires and public prosecutors' offices in both jurisdictions. In addition, it delves into the judicial interpretation of these tools and briefly touches on issues related to border security and migrants.

Lastly, the report offers a series of recommendations to the judiciary, the legislature and the security forces on the regulation and use of mobile device forensic extraction tools within a framework that respects due process and the right to privacy.

[1] https://adc.org.ar/wp-content/uploads/2022/01/ADC-Quien-revisa-tu-telefono.pdf

Introduction

Mobile device forensic extraction tools allow accessing information available on mobile phones. In the context of criminal investigations, these procedures are carried out by experts or computer labs that report to national and provincial security forces.

After the attempted assassination of Vice President Cristina Fernández in September of 2022, many news stories and interpretations have emerged in relation to the forensics carried out on the attacker's mobile phone to extract data[2]. At the time of this report, it is not yet clear what happened or how, but after an initial forensic examination, the seized phone was reset to factory settings.

Some versions say that it occurred after a failed decryption attempt by the Federal Police. Unable to access the information, the phone was sent to the Airport Security Police, but when it was plugged in, the message "phone factory reset" appeared, meaning there was no longer any data to extract.[3]

This type of situation and potential lack of care in the handling of digital evidence demonstrates the urgent need for specific legislation on clear and transparent protocols for using mobile phone forensic extraction tools and for training on their use for judicial operators and law enforcement.

Currently, most prosecutors are equipped with tools to conduct these procedures. For this report, we conducted a study of the current

[2] https://www.infobae.com/politica/2022/09/04/ataque-a-cristina-kirchner-las-dudas-sobre-el-celular-reseteado-del-detenido-y-el-intento-para-recuperar-la-informacion/
[3] https://www.pagina12.com.ar/479088-ataque-a-cristina-kirchner-al-borde-de-perder-una-prueba-cla

situation at the Argentinian National Gendarmerie (GNA), the Police of the Autonomous City of Buenos Aires and public prosecutors' offices in both jurisdictions.

The main focus is the Argentinian National Gendarmerie since, as the judicial police in the federal jurisdiction, it carries out functions related to border and internal security concerning criminal investigations of organized crime, complex crimes, technological crimes, cybersecurity and narco-criminality, for which forensic data extraction tools are of the utmost importance and widely used. We will also focus on the Buenos Aires Police, because as the federal capital it has a higher concentration of activities and population compared to the rest of the country[4] and it is important to report on this type of tools in this jurisdiction since they are commonly used in criminal investigations.

In terms of the tools, attention is focused on Cellebrite's UFED (Universal Forensic Extraction Device) because it is the most widely used to extract and analyse mobile device information in Argentina.[5] In some cases, the data shows tools from other providers are also used, so they will also be explained briefly.

Cellebrite is an Israeli company that, according to its Spanish-language website, offers industry-leading technology and services "trusted by law enforcement and businesses around the world to help protect communities, preserve their most valuable assets, and bring justice and peace to victims and innocent people."[6] UFED is a device from this company that is used to extract and decode data from the vast majority of mobile phones.

In recent years, information has emerged regarding the use of UFED

[4] https://www.argentina.gob.ar/sites/default/files/poblacion_urbana_dnp.pptx_.pdf
[5] https://www.clarin.com/policiales/detectives-telefonos-secretos-sistema-abre-celulares-resuelve-causas-complejas_0_U-d0fZd2m.html
[6] https://cellebrite.com/es/pagina-principal#

Cellebrite to investigate and prosecute dissidents in countries like Venezuela[7], Belarus[8], Russia[9], and Indonesia[10], which are known for adopting measures against political dissent and the LGBTIQ+ community. In response to several petitions submitted by human rights organizations to the Israeli Ministry of Defence, the company announced that it would stop selling its technology to China and Hong Kong, and more recently to Russia and Belarus.[11]

UFED Cellebrite includes commercial or proprietary software. That is, unlike open-source software,[12] the tool's source code is protected by intellectual property rights.[13] ADC's 2021 report pointed out that a crucial stage of proceedings, which involves no less than gathering evidence that may determine the guilt or innocence of a person, is conducted using tools and programs whose codes and operating algorithms are not known. This conflicts with article 18 of the Argentinian National Constitution, under which a person accused of a crime has the right to know and control the evidence used against them, particularly considering that the alleged vulnerabilities of some

---

[7] https://www.diariolasamericas.com/america-latina/regimen-maduro-hackea-celulares-software-empresa-israeli-n4235839

[8] https://www.haaretz.com/israel-news/2020-08-18/ty-article/.premium/whats-israeli-phone-hacking-firm-cellebrite-doing-in-sanctioned-belarus/0000017f-e198-d75c-a7ff-fd9dff0b0000

[9] https://www.haaretz.com/israel-news/security-aviation/2022-10-21/ty-article/.premium/russia-still-using-israeli-tech-to-hack-detainees-cellphones/00000183-eb6c-d15c-a5eb-ff6cf86e0000

[10] https://www.haaretz.com/israel-news/tech-news/2020-11-02/ty-article/.highlight/hacking-grindr-israels-cellebrite-sold-phone-spy-tech-to-indonesia/0000017f-db25-db22-a17f-ffb5bd550000

[11] https://cellebrite.com/en/cellebrite-to-stop-selling-its-digital-intelligence-offerings-in-hong-kong-china/; https://cellebrite.com/en/cellebrite-stops-selling-its-digital-intelligence-offerings-in-russian-federation-and-belarus/

[12] *El uso de software abierto para el análisis de la evidencia digital*, Gustavo Presman and Pablo A. Palazzi, available at https://docplayer.es/90297795-El-uso-desoftware-abierto-para-el-analisis-de-la-evidencia-digital.html

[13] Ibid.

tools would cast doubts on the reliability of the evidence that is collected.[14]

The sensitive nature of the information that our mobile phones store requires that the practices to conduct data extraction and analysis, as well as the regulations that allow incorporating them into judicial proceedings, respect the accused person's guarantees. These practices should conform to principles such as legality, limited purpose, accuracy and quality, limited retention, data security and confidentiality. It is important that these guarantees apply to the defendants and the third parties whose information is also on their mobile phones.

[14] *Exploiting vulnerabilities in Cellebrite UFED and Physical Analyzer from an app's perspective*, Signal, April 21, 2021 https://signal.org/blog/cellebrite-vulnerabilities/

Judicial Decisions and Mobile Forensic Data Extraction Tools

Today, mobile phones store many types of information about their owners and third parties. It includes everything from photos, videos and emails to information on banking, health and leisure time. When a phone is examined, extracting information implies, on the one hand, jeopardizing the right to privacy and, on the other, the possibility that the extracted information could be compromised, which would affect the results of the forensic analysis and, consequently, the right to a defence.[15]

There are no specific regulations on when and how to use forensic extraction tools on mobile phones in judicial proceedings. In the absence of regulation, judicial interpretation –what judges and judicial operators decide in the specific cases they are tasked with resolving– becomes especially relevant.

To discuss the use of mobile phone forensic extraction tools in judicial proceedings and how it is framed by the right of defence and the fundamental rights of the parties and third parties, we reviewed the rulings handed down on this type of technologies, in particular regarding UFED Cellebrite.

[15] For more information on the balance that should exist between state police power and the right to privacy as a result of the vast amount of information stored in mobile telephones, see *Riley v. California*, Supreme Court of the United States, review available at https://harvardlawreview.org/2014/11/riley-v-california/

The research identified references to the tools and their use in rulings and other judicial resolutions.[16] However, the judicial decisions reviewed and interviews with various judicial operators did not reveal any concerns about the data extraction tools themselves, the accuracy of what is extracted, the methodology used or the risk that the tools could be compromised.[17]

For example, in June 2022 the Federal Oral Criminal Court No. 1 resolved in the case *Shen, Yongchao s/Infracción Ley 23.73713*[18] that a second download of data from a mobile phone conducted by the police using a UFED tool does not constitute a forensic examination. The Court reasoned that the forensics took place during the first download.

It is important to underscore that the defence argued the right to privacy was violated by repeating the data extraction. In response, the Court considered that only information whose collection had been ordered, that is, information related to the facts under dispute, would be considered in the oral and public debate. At no point did the Court specify what would happen with the rest of the extracted information that would not be debated.

In September 2019, Chamber IV of the National Criminal and Correctional Court of Appeals in *AJA y otros s/ nulidad*[19] rejected a request to nullify a decision that ordered making forensic copies of two seized mobile phones without giving notice to the defence. The

---

[16] As an example, see *Vega, Diego Daniel y Otros s/Infracción Ley 23.737*, Tribunal Oral Federal de Bahía Blanca, 03/06/2022, available at https://www.cij.gov.ar/sentencias.html

[17] https://www.youtube.com/watch?v=6BjRuA5EvZ8

[18] *Shen, Yongchao s/Infraccion Ley 23.737*, Tribunal Oral en lo Criminal Federal N° 1, 27/05/2022, available at https://www.cij.gov.ar/sentencias.html

[19] *A.J.A. y otros s/nulidad*, Cámara Nacional de Apelaciones en lo Criminal y Correccional - Sala IV, 20/09/2019, available at https://www.diariojudicial.com/public/documentos/000/087/223/000087223.pdf

judges considered that unlocking the mobile devices is equivalent to obtaining a copy of the data stored on the device. The Court argued that this copy, made by the City Police Intelligence Directorate using UFED Cellebrite, does not constitute a forensic examination but rather a measure ordered to preserve the evidence. Based on this argument, the judge can obtain copies or reproductions of the seized information in order to preserve the chain of custody without having to notify the defence.

In terms of the use of the UFED Cellebrite tool, the issues in these two rulings relate to notice and the repetition of the procedure to extract information from mobile phones, not to the technologies that were used or their accuracy. Crucially, the two rulings do not consider the importance of the first extraction of digital information from a mobile phone, as this access produces the hash, an algorithm that creates a unique value that allows identifying whether the extracted information is exactly the same as the one that is stored. Therefore, if that information is modified, the bits[20] of the original file change, the hash calculation changes and, consequently, the string or algorithm is not the same as the first extraction hash. For this reason, it is important to verify the hash that resulted from the first extraction to verify the correct chain of custody of the data.[21]

These rulings and the specialists' interviews also reveal that the judiciary has yet to define with clarity basic aspects of digital

[20] A bit corresponds to a digit in the binary numbering system and represents the smallest unit of information.
[21] For additional information on these issues with a more legalistic approach, see *La extracción de prueba electrónica de teléfonos celulares y la garantía de defensa en juicio*, Carla Paola Delle Donne, available at https://www.thomsonreuters.com.ar/content/dam/openweb/documents/pdf/arg/white-paper/dossier-el-desafio-de-la-prueba-electronica.pdf

investigation. For example, it has not determined clearly whether the evidence is the hardware or the device from which the information was extracted, or if it is the extracted information itself.

Also, the judicial nature of mobile phone extraction has not been established: whether it constitutes forensics or the seizure of information, if it requires an express court order, and whether the defence should receive notice. These definitions, which appear to be mere legal categories, are important because depending on their classification various safeguards or protective measures apply to the rights of defence and due process of the affected individuals.

As far as it was possible to establish, the definition of these legal categories depends on the judicial authority's interpretation in each specific case.

It is important to mention that the reliability of the forensic extraction tools and their margin of error, which are key aspects to assess the collected data, also have not been defined.

The analysed case-law shows that judicial operators have little knowledge of mobile phone digital evidence and that judges have been timid in their approach to these issues. This gives rise to legal uncertainty that should be resolved urgently to ensure protective standards in accordance with due process and the fundamental rights of those involved, and to update the work of the judiciary regarding the forensic extraction of digital information.

Security Forces, Prosecution Authorities and Mobile Phone Forensic Extraction

This study on the use of mobile phone forensic extraction tools by public agencies focused on the Argentinian National Gendarmerie, the National Public Prosecutor's Office, the Police of the City of Buenos Aires and the Public Prosecutor's Office of the City of Buenos Aires.

As mentioned before, we consider it is important to focus on the Argentinian National Gendarmerie due to its border security and internal security functions in relation to organized crime, complex crimes, technological crimes, cybersecurity and narco-criminality, and on the City of Buenos Aires due to the high concentration of activity and population and the habitual use of these tools in criminal investigations.

The study includes requests for public information and research on official websites. Below is the information that was obtained for each agency:

Argentinian National Gendarmerie:

Cellebrite's website mentions this security force and the use of Cellebrite tools in their laboratories.[22] According to the site, National Gendarmerie officers, through the Digital Forensics Department which has five regional offices in Campo de Mayo, Córdoba, Rosario, San Miguel de Tucumán and Bahía Blanca, deliver a constant flow of digital devices to the laboratory. The objective is to conduct investigations by producing digital intelligence on issues related to border security, drug

[22] https://cellebrite.com/es/la-gendarmeria-nacional-de-argentina-esta-superando-las-barreras-de-tiempo-y-distancia-con-inteligencia-digital/

trafficking and smuggling, among other issues. In addition, it is further described that investigators and examiners use UFED to extract data from mobile devices, Cellebrite UFED Cloud to preserve and analyse data from the cloud –such as messaging app conversations and web browsing history– Cellebrite Pathfinder to create a unified forensic environment across the entire lab network and Cellebrite Physical Analyzer to generate reports.

In its response to our request for public information,[23] the Argentinian National Gendarmerie indicated that there is currently a total of 23 UFED Forensic Extraction Devices in forensic computing labs in the different Institutional Deployment Units, which operate under the Directorate of Criminalistics and Forensic Studies, as follows:

Forensic Extraction Equipment			
Nº	UNIT	EQUIPMENT	LOCALITY/ PROVINCE
1	REGION I COMMAND	UFED TOUCH ll	Campo De Mayo (Buenos Aires)
2	GROUP VII HEADQUARTERS "SALTA"	UFED TOUCH ll	Salta – Salta
3	SQUADRON 7 “PASO DE LOS LIBRES” “CBO MISAEL PEREYRA"	UFED TOUCH ll	Paso de Los Libres – Corrientes
4	SQUADRON 10 "EL DORADO"	UFED TOUCH ll	El Dorado – Misiones
5	SQUADRON 34 BARILOCHE "CABO PRIMERO MARCIANO VERON"	UFED TOUCH ll	Bariloche – Río Negro
6	TELEPHONY DIV (DICRIEFOR) CELULAR	UFED TOUCH ll	CABA

[23] The response to the information request submitted to the Argentine National Gendarmerie is in our possession.

7	GROUP IV HEADQUARTERS "MISIONES"	UFED TOUCH ll	Posadas – Misiones
8	GROUP VI HEADQUARTERS "FORMOSA"	UFED TOUCH ll	Formosa – Formosa
9	GROUP XX HEADQUARTERS "CÓRDOBA"	UFED TOUCH ll	Córdoba – Córdoba
10	CORE SQUADRON 59 "SANTIAGO DEL ESTERO"	UFED TOUCH ll	Santiago Del Estero – Santiago Del Estero
11	GROUP XV HEADQUARTERS "ROSARIO"	UFED TOUCH ll	Rosario
12	UNIPROJUVETUE	UFED TOUCH ll	Venado Tuerto – Santa Fe
13	GROUP V HEADQUARTERS "ENTRE RÍOS"	UFED TOUCH ll	Paraná – Entre Ríos
14	GROUP XVI HEADQUARTERS "SANTA CRUZ"	UFED 4 PC	Río Gallegos – Santa Cruz
15	JEFATURA DE AGRUPACIÓN ll "CORRIENTES"	UFED TOUCH ll	Corrientes - Corrientes
16	COMANDO DE REGIÓN V	UFED 4 PC	Bahía Blanca – Buenos Aires
17	GROUP XI HEADQUARTERS "MENDOZA"	UFED 4 PC	Mendoza – Mendoza
18	TELEPHONY DIV (DICRIEFOR) CELULAR	UFED 4 PC -	CABA
	TELEPHONY DIV (DICRIEFOR) CELULAR	UFED 4 PC -	CABA
	TELEPHONY DIV (DICRIEFOR) CELULAR	UFED PREMIUN	CABA
	TELEPHONY DIV (DICRIEFOR) CELULAR	UFED 4 PC-	CABA
	TELEPHONY DIV (DICRIEFOR) CELULAR	UFED 4 PC -	CABA
19	HEADQUARTERS VII "CATAMARCA"	UFED 4 PC -	San Fernando Del Valle de Catamarca – Catamarca

In its 2020-2023 institutional strategic plan, the National Gendarmerie notes that the lack of budgetary resources to maintain the UFED Touch19 software licenses up to date is a weak point[24]. Cellebrite describes this software as a comprehensive mobile forensic tool that allows police, military and intelligence forces to extract forensically sound evidence data irrespective of location[25].

An advanced search on the Official Gazette's website found that in 2022 the open tenders called for directly contracting license renewal services for UFED Premium to unlock mobile phones.[26] It was awarded to the company IAFIS Argentina SA through Public Tender 19/2022 for the total sum of 39,631,782.00 pesos.[27]

The response to our request for public information reveals that the Gendarmerie maintains contact with the providers through official email, for the sole purpose of obtaining quotes to initiate the administrative acts required to purchase forensic equipment.

The Directorate of Criminalistics and Forensic Studies applies the following protocols and manuals in cases that involve the analysis of mobile devices:

- Guidelines established in different international publications,[28] whose publishing dates are striking (all were issued between

[24] https://www.argentina.gob.ar/sites/default/files/plan-estrategico-20-23.pdf
[25] https://cellebrite.com/en/cellebrite-introduces-ufed-touch2-platform
[26] Casey, E. 2004. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. Baltimore, Maryland, USA. Elsevier.
[27] https://www.boletinoficial.gob.ar/detalleAviso/tercera/2311388/20220613
[28] Casey, E. 2004. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. Baltimore, Maryland, USA. Elsevier.

2000 and 2004) in view of technological advancements and the emergence of new types of crimes.

- Resolution 528/2021 of the National Ministry of Security: "Action Protocol for Scientific Research at the Place of the Event."[29] It specifies how the computer forensic specialist should proceed at the location of the occurrences, but it does not refer to the reliability and security of the tools used to extract information from mobile phones.

- Resolution 234/2016 of the National Ministry of Security: "General Action Protocol for Police and Security Forces in the Cybercrime Investigation and Evidence Gathering Process."[30] It does not specifically mention mobile phone forensic extraction tools, nor does it set forth any required characteristics they should fulfil in order to guarantee due process.

- ISO/IRAM Standard 27037,[31] which establishes the guidelines to identify, collect, acquire and preserve digital evidence.

In its response to the request for information, the Gendarmerie stated it does not conduct computer security audits since the tools are licensed by world-renowned companies and that it holds technical meetings with the tool suppliers where the staff that operates these computer systems are informed of new developments and updates. To this end, the operators are assigned a reserved username and password to access the technical information for each offered equipment.

---

[29] https://www.boletinoficial.gob.ar/detalleAviso/primera/253486/20211126
[30] https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-234-2016-262787
[31] https://www.iso.org/standard/44381.html

In terms of its operation, it highlighted that two different hash algorithms are applied to the collected information when the data is submitted to the requesting judicial authority in order to safeguard the integrity and authenticity of the collected digital evidence. Furthermore, it explained that extraction processes and methods differ depending on the brand, model and operating system of each mobile device. This includes:

- Advanced Logical Extraction
- Physical Extraction
- File system: ADB
  - Android Backup
  - Android Backup APK Downgrade

In turn, each forensic device has its own extraction record, but there is no distinction between successful and unsuccessful attempts. In addition, the Directorate of Criminalistic and Forensic Studies, specifically the Mobile Device Division, registers a unique forensic examination number for each forensic request, which is part of the process record of the forensic tool. As these are ongoing judicial cases, the proceedings are restricted to the parties and remain secret to third parties, and the work is performed under a confidentiality agreement.

The Gendarmerie affirmed they do not keep copies of the extracted information after it is sent to the requesting judicial authority.

National Public Prosecutor's Office:

The General Directorate of Investigations and Technological Support for Criminal Investigation (DATIP) is part of the structure of the Public Prosecutor's Office. According to information request AIP No. 379 of August 8, 2022, sent to the organization, two laboratories perform

forensic examinations within the scope of the discipline known as computer forensics, namely:

- DATIP Computer Laboratory
- DATIP Telecommunications Analysis Laboratory

One of the functions of the Telecommunications Analysis Laboratory is to manage the use and services carried out with DATIP's mobile device data extraction equipment (UFED) and any others that may be implemented in the future.[32] The Directorate's website has a publicly accessible video that is presented as a tutorial on how to download UFED.[33]

In accordance with the information ascertained on the website of the National Official Gazette and the procurement website of the Public Prosecutor's Office, on December 20, 2021, Public Tender 38/2021 approved purchasing three UFED 4PC Ultimate licenses for a term of 24 months and the renewal of one UFED 4PC Ultimate license for a term of 12 months, from the company VEC S.R.L., for 11,743,785 pesos.[34] In May of that same year, Public Tender 10/2021 approved purchasing a 24-month UFED 4PC Ultimate license from the company IAFIS Argentina SA for 2,698,748.00 pesos.[35]

In information request AIP No. 379[36] of August 8, 2022, the Public Prosecutor's Office informed that for the forensic acquisition and subsequent analysis of mobile devices, the DATIP Telecommunications Analysis Laboratory uses UFED 4PC Ultimate version software, and that presently it has four active licenses.

---

[32] https://www.mpf.gob.ar/datip/laboratorio-de-analisis-de-telecomunicaciones/
[33] https://www.mpf.gob.ar/datip/#gallery
[34] https://www.boletinoficial.gob.ar/detalleAviso/tercera/2296402/20211220
[35] https://www.boletinoficial.gob.ar/detalleAviso/tercera/2276900/20210510
[36] The response to the information request submitted to the National Public Prosecutor's Office is in our possession.

The website of the National Public Prosecutor's Office indicates that between June and August 2022, this agency held a technical legal workshop on the analysis of UFED extractions (mobile phones), forensic images (Autopsy - FTK-Encase), social networks and assistance to locate witnesses.[37] The workshop was directed at Public Prosecutor's Office employees, civil servants and magistrates, and its main objective was to acquire the fundamental notions to analyse evidence extracted from an electronic device. In addition, information request AIP No. 379 affirmed that technicians from the Telecommunications Analysis Laboratory of the National Public Prosecutor's Office have participated in demonstrations held by companies about different forensic technologies, with the active participation of local suppliers, but the Prosecutor's Office did not provide specific information on the subjects that were discussed or provide minutes of these meetings.

Regarding procedures to gather digital evidence from mobile devices, the Public Prosecutor's Office indicated they are conducted in accordance with basic guidelines and protocols, including Resolution 528/2021 of the National Ministry of Security, Resolution PGN 0756/2016 of the National Public Prosecutor's Office and ISO/IRAM 27037, among others.

Resolution 528/2021 of the National Ministry of Security is the Action Protocol for Scientific Investigation at the Place of the Event[38] and does address the reliability and security of the tools used to extract information from mobile phones.

Resolution PGN 0756/2016 of the National Public Prosecutor's Office includes a Guide to Obtaining, Preserving and Treating Digital Evidence

[37] https://www.mpf.gob.ar/capacitacion/actividad/taller-tecnico-juridico-de-analisis-de-extracciones-ufed-telefonos-celulares-imagenes-forense-autopsy-ftk-encase-redes-sociales-y-colaboracion-en-la-busqueda-de-testigos/
[38] https://www.boletinoficial.gob.ar/detalleAviso/primera/253486/20211126

published in 2014, and partially adopts the principles set forth in the standard ISO/IRAM 27037 mentioned above. It does not make any reference to mobile phone extraction tools. It only states that the actual analysis of the data extracted from computer storage devices is conducted exclusively through any internationally endorsed software tool (Encase, for example) and that at the moment local security forces use these programs due to their optimal and reliable performance, and because they are endorsed by the National Institute of Standards and Technology (NIST).[39]

Additionally, each UFED 4PC Ultimate software license has a log[40] that reports the number of forensic reports, the type of extraction performed, the result and the start and end dates of the activity, among other variables. The information provided by the National Public Prosecutor's Office shows that between September 15, 2020, and August 3, 2022, 2,483 forensic examinations were carried out by this agency. The results of the examinations are detailed in the report generated by the log and can be successful, annulled, omitted or have a read error.

Also, in information request AIP No. 379 of August 8, 2022, the Public Prosecutor's Office informed that they do not conduct internal, external or independent audits to assess the tools' computer security. This lack of audits is concerning because a system glitch in the tools can affect access to justice and fair trials.

Police Force of the Autonomous City of Buenos Aires:

The Police of the City of Buenos Aires reports to the city's Ministry of Justice and Security. In 2015, the national government transferred to

[39] https://www.fiscales.gob.ar/wp-content/uploads/2016/04/PGN-0756-2016-001.pdf
[40] Sequential recording in a file or database of all occurrences (events or actions) that affect a specific process. It is evidence of system behaviour.

the government of the City of Buenos Aires the resources to fully exercise policing functions in its territory. The Computer Intelligence Analysis Division and the Special Investigations Section are part of this security force's structure.[41]

We could not locate any institutional references to mobile phone forensic extraction tools on the websites of the Buenos Aires Police or the Buenos Aires Ministry of Justice and Security. The Official Gazette's search engine did not return any results concerning the acquisition, tenders or requests for proposals by the city's government concerning these tools for the Police or the Ministry of Justice and Security. The institutions indicated the tools are purchased [42]by the Undersecretary of Administrative Management of the Ministry of Security pursuant to procurement, acquisition and contracting of goods and services conducted through the government's electronic procurement and contracting system, and that the contracts and the tenders are public.

In its response to public information request NO-2022-30927160-GCABA-SLCC, the Buenos Aires Ministry of Justice and Security indicated it has the City Police Superintendence for the Fight against Cybercrime, which in turn has the Cybercrime Investigation Directorate. The Computer Crime Investigation Department reports to the directorate, and this department includes the Computer Analysis Division and the Special Investigations Section. These last two offices have computer forensic laboratories that work jointly on mobile phone forensics requested by the judiciary.

The reply also states that Cellebrite's UFED Touch hardware and UFED 4PC software (currently version 7.57.0.13) are used to conduct mobile

[41] https://documentosboletinoficial.buenosaires.gob.ar/publico/PE-RES-MJYSGC-SECS-34-18-ANX.pdf
[42] Public information request NO-2022-30927160-GCABA-SLCC

device forensic extractions. The acquired information is analysed using Cellebrite software Physical Analyzer (currently version 7.56.0.20).

In relation to the protocols to use these tools, the only information provided by the Ministry of Justice and Security of the Buenos Aires City Government, in September 2022, indicates that the procedures are carried out in strict compliance with "good forensic practices",[43] without providing copies or elaborating on such practices. Lastly, it affirms that there is no training or contact with UFED providers.[44]

Public Prosecutor's Office of the Autonomous City of Buenos Aires:

According to the procurement section of the Buenos Aires Public Prosecutor's Office,[45] Provision OAF 30/2022 approved Direct Contracting No. 4/2022 for the renewal of six EnCase™ Forensic SMS licenses with support service and updates for the period between June 2022 and June 2023 and the renewal of six Axiom Complete Magnet SMS licenses with support service and updates for the period between August 2022 and August 2023, for the Judicial Investigations Body of the Public Prosecutor's Office. All for the total sum of 34,635.00 dollars.[46]

EnCase™ Forensic is a tool that finds, decrypts, collects and preserves forensic data from a wide variety of devices for its use in digital investigations. Its website states that it can find digital evidence no matter where it hides to help law enforcement and government

[43] The response to the information request submitted to the City of Buenos Aires Ministry of Justice and Security is in our possession.
[44] Ibid.
[45] https://mpfciudad.gob.ar/compras/search
[46] https://mpfciudad.gob.ar/storage/archivos/1fd6b060f907ca0884d4b7ecce511fc7.pdf

agencies reduce case backlogs, close cases faster and improve public safety.[47]

Magnet Axiom is a tool to recover digital evidence from various computing devices, including smartphones, cloud services and computers. With respect to mobile phones, the tool can obtain information from devices with iOS and Android operating systems, and it analyses the evidence with integrated analytical tools, such as timelines, connections, media explorer and maps.[48]

In November 2021, Direct Contracting No. 07/2021 was approved with exclusivity, with the aim of obtaining the ENCE EnCase Certified Examiner Certification and MCFE Axiom Magnet Certified Forensic Examiner, for the use of the Judicial Investigations Body of the Public Prosecutor's Office, for the total sum of 2,700,000.00 pesos.[49]Both qualifications certify professionals from the public and private sectors in the use of certain forensic software.[50]

Also in October 2021, OAF Provision 53/2021 approved Minor Direct Contracting No. 10/2021 to renew six EnCase Forensic (SMS) licenses with support service and updates and to acquire two Magnet Outrider Computer Software, for use by the Judicial Investigations Body, for the total amount of 13,310.00 dollars.[51]

In July 2021, FGAG Resolution 178/2021 approved Public Tender No. 02/2021 for the renewal of seven UFED 4PC licenses and two KIOSK Infield licenses, to be used by the Judicial Investigation Body of the

[47] https://security.opentext.com/encase-forensic
[48] https://www.magnetforensics.com/products/magnet-axiom/
[49]https://mpfciudad.gob.ar/storage/archivos/93ed13085179966abf4250920cf6ad01.pdf
[50] https://www.opentext.com/TrainingRegistry/course/details/2687
[51]https://mpfciudad.gob.ar/storage/archivos/564a6bfdf7f8c4743da673c6fd276c63.pdf

Public Prosecutor's Office, and it was awarded to IAFIS Argentina SA for the total sum of 117,410.26 dollars.[52]

KIOSK Infield is a Cellebrite hardware platform designed to adapt to the investigation workflow that allows quickly extracting and acting on mobile data at specific locations, such as police stations and border checkpoints.[53]

Migrants and Mobile Phone Extraction Tools

Mobile phones have made the situation of migrants and border crossings even more complex than in previous times. For example, a few months ago it emerged that the U.S. government was handing out to migrants arriving from Mexico mobile phones with nothing but a tracking application installed and that could not be used to make calls or access the Internet.[54]

Cellebrite's website emphasizes the great usefulness of its technologies at border crossings and their security.[55] In Spain, for example, in August 2021, the General Police Commissariat for Immigration and Borders purchased 15 Cellebrite UDEF Touch II Ultimate mobile devices[56] to conduct judicial forensic reports at land, sea and air borders.

---

[52] https://mpfciudad.gob.ar/storage/archivos/0821ca2578b6ae2cdeab3482b4db74bd.pdf
[53] https://cellebrite.com/es/plataformas/
[54] https://cnnespanol.cnn.com/2022/06/05/telefonos-celulares-no-pueden-hacer-llamadas-ni-acceder-internet-ice-rastrear-migrantes-trax/
[55] https://cellebrite.com/es/cellebrite-responder-es
[56] https://elcierredigital.com/tecnologia/122247883/interior-usara-tecnologiaisraeli-hackear-telefonos-moviles-fronteras-espanolas.html

In Argentina, the National Gendarmerie is a security force that performs military functions as an intermediate force within the framework of internal security, national defence and foreign policy support. One of its national defence duties is the permanent control and surveillance of the country's borders.

On its website, Cellebrite states that, through its forensic tools, it supports Gendarmerie border security operations and ensures that digital intelligence becomes the pillar of current and future Gendarmerie investigations[57]. One of the initiatives supported by the company is the creation of a new laboratory network through the study of electronic devices linked to suspected criminal activities, but it does not explain how exactly it supports this initiative[58]. Thus, according to statements made by experts in the force, the company is positioned as the provider of digital intelligence solutions for future generations of National Gendarmerie officers.[59]

To learn more about the issue, we contacted people connected to defending migrants' rights in Argentina. These conversations did not yield any confirmation that these tools are being used at the Argentinian borders. Based on their experience, the procedure to enter Argentina requires fingerprinting, taking a photo, inquiring about the reason for entry and requesting an e-mail to which the National Migration Directorate sends a PDF document showing proof of entry.

Nevertheless, information did emerge on abuses involving mobile phones in Argentina´s border from the National Gendarmerie, but the

[57] https://cellebrite.com/es/la-gendarmeria-nacional-de-argentina-esta-superando-las-barreras-de-tiempo-y-distancia-con-inteligencia-digital/
[58] https://cellebrite.com/es/la-gendarmeria-nacional-de-argentina-esta-superando-las-barreras-de-tiempo-y-distancia-con-inteligencia-digital/
[59] https://cellebrite.com/es/la-gendarmeria-nacional-de-argentina-esta-superando-las-barreras-de-tiempo-y-distancia-con-inteligencia-digital/

type of abuse is about their use by migrants, and not about surveillance tools.

Proposals and Recommendations

This research shows the widespread adoption and use of forensic extraction tools, and a lack of concrete guidance and legal safeguards regarding that use. Given the technology's serious implications for due process and privacy, it is necessary to control its use and guarantee its reliability.

This conclusion has led to a series of recommendations:

Need for information on the operation of hardware and software

Although these tools are protected by trade secret, it is important that a minimum of information on how they operate is available. There should be a balance between trade secrets and the knowledge of how the tools work in order to guarantee the right of defence and the right to privacy of the individuals affected by the extracted information.

Our 2021 report emphasized that, although trade secrets are a legitimate interest protected by law, they cannot be invoked in situations that may affect fundamental rights such as the right of defence.

The admissibility of these tools in judicial proceedings should be contingent on guaranteeing a reliable methodology and that the results obtained remain unmodified. To this end, it is indispensable to promote transparency and control over how these tools operate and this should be a more important value than protecting trade secrets.

Legislation regarding information extraction

The authorities that use these tools should have specific publicly available regulations that guarantee due process and the right of defence in terms of the use of information extraction tools.

Although the Public Prosecutor's Office indicated the protocols used for the extraction of evidence in general and digital evidence in particular, it did not provide specific details on the procedural standards and operation of mobile phone forensic extraction tools.

This is central to ensuring that affected parties can exercise appropriate control over the evidence and can object to erroneous and/or illegal manipulation during the extraction of the information.

Tool providers should be selected pursuant to criteria established in the regulations, to ensure that they meet a verifiable reliability standard for judicial proceedings.

Legislation on information analysis

In this same vein, given the amount of personal and third-party information found on our mobile phones, extraction should be limited to the specific case and purpose sought, with minimum harm to third parties.

Today, mobile phones hold information on every aspect of an individual's life, concerning both the owner of the device and third parties who have a relationship with this person. For this reason, it is extremely important that the information that is analysed pertains only to the specific case and that it concerns the privacy of third parties as little as possible.

In criminal proceedings, the search for evidence cannot advance beyond what is necessary in relation to this personal data.

Legislation on the storage of extracted data

One of the issues that arose while preparing this report and for which no answers or forecasts have been found is the manner in which these tools store extracted data.

Where is it stored? Is it on a server belonging to the institution conducting the examination or does it belong to the company providing the software? What security measures exist for this information?

It is appropriate that the collected data is not stored on servers belonging to third parties that are unrelated to the investigation and that the institution storing the data has in place the security measures that are required to guarantee that the data is not altered or stolen, this in order to safeguard the right to due process and the right to privacy of the individuals involved.

Legislation on the disposal of extracted and irrelevant information

As a general principle, personal data should be retained for a limited period of time.

Information extracted through forensic mobile phone tools should not be kept longer than is necessary for the investigation.
A clear directive should be in place regarding the permanent deletion of the extracted information after a certain period of time.

It is critical to emphasize that if the information extracted in relation to the owner of the phone is not relevant to the specific case it should be deleted immediately, in particular, when it concerns and belongs to third parties.

Information about the margin of error

In general, in forensic practice, results are produced following a specific technical and methodological approach, but it is possible to have disparate criteria and a diversity of outcomes, which is why in technical disciplines it is often not possible to affirm with certainty a conclusion. Consequently, margins of error are permitted in the results.[60][51].

When using mobile device forensic extraction tools, as with other types of forensic examinations or tests, the reports should include the technology's margin of error percentage.

It is important to provide this information because it safeguards potential challenges and questioning of the evidence by the defence and the adequate assessment of the evidence by the judges.

Training of judicial operators

Case-law and expert opinion research shows that judicial operators are not only unfamiliar with the operation of these technologies but also with the procedural nature of their use in proceedings.

[60] For additional information see *Certeza pericial y margen de error,* Patricia Noemí Apesteguy, available at **https://www.lanacion.com.ar/politica/certeza-pericial-y-margen-de-error-nid1773887/**

This has a direct impact on the conduct of proceedings and the guarantees that govern them.

It is necessary to train and inform judicial operators on the operation, risks and eventualities of these forensic extraction tools to ensure that the evidence they provide is correctly assessed and that their use complies with due process and the right of defence, with all the guarantees for the person involved.

Meaningful human intervention

Replacing forensic technicians or experts with different technologies is a growing trend. For this reason, it is important to guarantee meaningful human intervention in these procedures to protect people from the arbitrary decisions that technologies often make.

It is very important that human intervention is actually meaningful and not simply a person connecting or manipulating software or hardware. The intervention should imply a concrete influence on the use and results of these tools. This prevents arbitrary decision-making by the technologies.

Migration and digital rights

The contacts that take place in the context of migrants and border crossings highlight the need for more in-depth study of cases involving police abuse and the exploitation of personal data. While we did not detect specific instances of the use of mobile phone extraction tools, other examples of irregular action suggest that further research is required before such situations can be ruled out.

It is necessary to increase the public visibility of the reality faced by migrants in order to encourage reflection that invites change in specific humanitarian and legally unprotected situations.

It is important to promote ties between different human rights organizations in the digital and migrant sphere to work together on a joint agenda regarding the respect of human rights in these types of situations.

Author

Luis García Balcarce

Mr. García Balcarce holds a law degree from the University of Buenos Aires and is experienced and trained in the management of digital content and tools in the Ibero-American legal field. He has been editorial and content director for projects to disseminate legal information with universities and public and private institutions. As project officer at ADC, his research focuses on privacy, data protection and freedom of expression.

adc.org.ar