



**INTERPOL'S FORENSIC REPORT
ON FARC COMPUTERS AND HARDWARE
SEIZED BY COLOMBIA**

MAY 2008

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

© ICPO-INTERPOL 2008

All rights reserved. No part of this report may be reproduced, copied or used by any means without prior permission in writing from ICPO-INTERPOL.

Published by:
ICPO-INTERPOL
200 Quai Charles de Gaulle
69006 Lyon
France

www.interpol.int

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

<u>TABLE OF CONTENTS</u>	<u>Page</u>
ACKNOWLEDGEMENTS	4
EXECUTIVE SUMMARY	6
PART 1: OPERATIONAL FRAMEWORK FOR INTERPOL'S INDEPENDENT EXAMINATION OF THE EIGHT SEIZED FARC COMPUTER EXHIBITS	10
1.1 Eight seized FARC computer exhibits	10
1.2 Request for assistance from Colombia	10
1.3 INTERPOL's operational support to member countries	13
PART 2: PHYSICAL HANDOVER OF THE SEIZED COMPUTER EXHIBITS BY COLOMBIAN POLICE TO INTERPOL'S INCIDENT RESPONSE TEAM AND FORENSIC ACQUISITION OF THE EXHIBITS	16
PART 3: TRANSFER OF THE IMAGE DISKS BY DIPLOMATIC POUCH FROM COLOMBIA TO SOUTHEAST ASIA	20
PART 4: INTERPOL'S INDEPENDENCE	23
PART 5: MAJOR PUBLIC FINDINGS	25
PART 6: RECOMMENDATIONS FOR INTERPOL AND ITS MEMBER COUNTRIES	35
LIST OF APPENDICES	39

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

ACKNOWLEDGEMENTS

Many representatives from INTERPOL member countries, INTERPOL's Executive Committee, INTERPOL officials and external experts devoted countless hours and resources to this endeavour.

I would first like to acknowledge INTERPOL's Senior Vice-President Arturo Herrera Verdugo and all of the members of our Executive Committee, whose support was a prerequisite for INTERPOL to provide any assistance to Colombia in this area.

The Commissioners of the Australian Federal Police, Mr Michael Keelty, and the Singapore Police Force, Mr Boon Hui Khoo, made available their computer experts to conduct the forensic examination of the eight seized FARC computer exhibits. Their immediate and unconditional support for INTERPOL demonstrated their recognition of the importance of this task and their faith in INTERPOL to carry out this task with the thoroughness, care and necessary independence it required.

None of this would have been possible without INTERPOL's two computer forensic experts from Australia and Singapore who dedicated themselves to producing such a large amount of high-quality work under great time pressure. Their willingness to take on this painstaking task – to fully immerse themselves in the examination of 609.6 gigabytes of data – and the professionalism with which they conducted their forensic examination gave INTERPOL the utmost confidence in their findings. INTERPOL also benefited greatly from the invaluable insights of the experts from academia, the private sector and police who were consulted.

At the INTERPOL General Secretariat, officials from many different services provided their expertise and manpower to produce this report within the tight timeframe agreed upon with Colombia. Rather than list all of the individuals by name, officials from the following services, listed alphabetically, made the deployment of the Incident Response Team to Colombia, INTERPOL's subsequent assistance to Colombia and the production of this report possible:

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

Administration and Budget Directorate
Americas Sub-Directorate
Cabinet
Command and Co-ordination Centre
Communications and Publications Office
Criminal Analysis Sub-Directorate
Executive Directorate for Police Services
Financial and High-Tech Crimes Sub-Directorate
Information Systems Directorate
Language Services Sub-Directorate

Management Planning and Policy Office
NCB Services and I-24/7 Development
Directorate
Office of Legal Affairs
Office of the Special Representative to the
United Nations
Operational Police Support Directorate
Protocol, Missions and Conferences Office
Security Sub-Directorate
Specialized Crime and Analysis Directorate
Training Sub-Directorate

Our National Central Bureaus in the relevant countries greatly assisted in co-ordinating the forensic examination, ensuring that the materials needed to conduct the examination were provided and serving as liaisons between the General Secretariat and the national authorities in their countries. Colombia's *Departamento Administrativo de Seguridad* and the Colombian National Police had the courage to ask INTERPOL to conduct an in-depth, independent forensic examination of the seized computer exhibits and the integrity to allow INTERPOL to do its work without attempting to influence the outcome.

I would also like to thank Mr José Miguel Insulza, Secretary General of the Organization of American States, for his endorsement of INTERPOL's ability to conduct this work independently and professionally. This confirmed that the situation required independent, international law enforcement expertise that only INTERPOL could provide.

INTERPOL is the sum of its parts. It is the belief of police in our member countries that we can assist them during a crisis situation; that we can provide specialized expertise that may be ordinarily lacking in their countries; and that we can serve as an independent law enforcement body in international investigations. It is our National Central Bureaus, our Sub-Regional Bureaus, our Liaison Offices and our member countries' law enforcement services around the world that ensure that any time and anywhere a law enforcement officer calls for assistance, that call will be answered. And it is the dedication of INTERPOL's officials, who remain committed to the ideal of international police co-operation and work in service of this ideal each and every day, who make INTERPOL's work possible.



Ronald K. Noble

INTERPOL Secretary General

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

EXECUTIVE SUMMARY

- € Colombian authorities requested INTERPOL¹ to conduct a forensic examination of three laptops, two external hard disks and three USB thumb drives seized from the *Fuerzas Armadas Revolucionarias de Colombia* (FARC) camp in the Ecuadorian border region with Colombia on 1 March 2008 (hereinafter referred to as the “eight seized FARC computer exhibits”).
- € Specifically, Colombian authorities sought INTERPOL’s independent computer forensic technical assistance to examine the user files on the eight seized FARC computer exhibits and to determine whether any of the user files had been newly created, modified or deleted on or after 1 March 2008.
- € This request from Colombia fell within the scope of one of INTERPOL’s Core Functions to provide operational police support to its member countries. A key mechanism for delivering this support is an INTERPOL Incident Response Team (IRT)², which can be deployed within hours of a request from a member country faced with (a) a crisis situation, (b) circumstances which require resources or expertise beyond the capacity of that specific country, or (c) the need for independent assistance in an international investigation.
- € After carefully considering Colombia’s request, INTERPOL proposed to deploy immediately an IRT to Colombia with a mandate to examine the technical feasibility of the Colombian request and to provide advice on how to carry out the work if judged feasible. INTERPOL’s Secretary General led the delegation to Colombia, which included the IRT members and INTERPOL’s General Counsel, to meet with Colombian authorities to define the terms and scope of the assistance to be provided.
- € The *Technical Assistance Agreement* concluded between INTERPOL and Colombia set forth the conditions for ensuring both the independence of INTERPOL and a sound legal framework for INTERPOL to provide expert and objective police assistance to Colombia.

¹ Any reference to INTERPOL in this report refers to the General Secretariat of the International Criminal Police Organization-INTERPOL, based in Lyon, France, unless otherwise indicated.

² Please see page 14 for an explanation of an Incident Response Team.

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

- € The IRT deployed to Colombia was given the working name of CompFor (from **computer forensics**), and included two forensic experts from Australia and Singapore selected by their national police administrations. The experts came from outside of the region and did not speak Spanish, which helped to eliminate the possibility that they might be influenced by the content of any data they were examining. The basis for their work was Article 30 of INTERPOL's Constitution³ which is designed to protect INTERPOL staff from outside influences in the conduct of their official duties. All of these measures were taken to safeguard their objectivity during the course of the forensic examination.
- € The scope of INTERPOL's computer forensic examination was limited to (a) determining the actual data contained in the eight seized FARC computer exhibits, (b) verifying whether the user files had been modified in any way on or after 1 March 2008, and (c) determining whether Colombian law enforcement authorities had handled and examined the eight seized FARC computer exhibits in conformity with internationally recognized principles for handling electronic evidence by law enforcement.
- € The remit of the IRT and INTERPOL's subsequent assistance to Colombia's investigation did not include the analysis of the content of documents, folders or other material on the eight seized FARC computer exhibits. The accuracy and source of the user files contained in the eight seized FARC computer exhibits are and always have been outside the scope of INTERPOL's computer forensic examination.
- € During the first phase of the examination, which took place in Bogotá, forensic experts produced physical images⁴ of the data contained in the eight seized FARC computer exhibits.
- € During the second phase of the examination, the experts each forensically examined four of the eight seized FARC computer exhibits in their working countries in Southeast Asia.
- € Upon completing their computer forensic examination, INTERPOL's experts concluded:
 - € **Finding 1:** The eight seized FARC laptop computers, USB thumb drives and external hard disks contain a total of 609.6 gigabytes of data, including documents, images and videos.

³ Please see page 16 for the text of Article 30.

⁴ For an explanation of forensic imaging see page 18.

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

- € **Finding 2:** All seized FARC computer exhibits were accessed by Colombian authorities between 1 March 2008, when they were seized, and 10 March 2008, when they were handed over to INTERPOL's computer forensic experts.

- € **Finding 2a:** Access to the data contained in the eight seized FARC computer exhibits by the *Grupo Investigativo de Delitos Informáticos* of the Colombian Judicial Police between their receipt at 11:45 a.m. on 3 March 2008 and their handover to INTERPOL's computer forensic experts on 10 March 2008 conformed to internationally recognized principles for handling electronic evidence by law enforcement.

- € **Finding 2b:** Access to the data contained in the eight FARC computer exhibits between 1 March 2008, when they were seized by Colombian authorities, and 3 March 2008 at 11:45 a.m., when they were turned over to the *Grupo Investigativo de Delitos Informáticos* of the Colombian Judicial Police, did not conform to internationally recognized principles for handling electronic evidence by law enforcement.

- € **Finding 3:** INTERPOL found no evidence that user files were created, modified or deleted on any of the eight seized FARC computer exhibits following their seizure on 1 March 2008 by Colombian authorities.

- € INTERPOL's computer forensic examination confirmed Colombian law enforcement's own admission that access to the data contained in the eight seized FARC computer exhibits between 1 March 2008, when they were seized by Colombian authorities, and 3 March 2008 at 11:45 a.m., when they were handed over to the *Grupo Investigativo de Delitos Informáticos* of the Colombian Judicial Police, did not conform to internationally recognized principles for the ordinary handling of electronic evidence by law enforcement. That is, instead of taking the time to make write-protected images of all eight seized exhibits before accessing them, they accessed the exhibits directly.

- € In contrast, access to the data contained in the eight seized FARC computer exhibits by the *Grupo Investigativo de Delitos Informáticos* of the Colombian Judicial Police after 11:45 a.m. on 3 March 2008 conformed to the highest standards of internationally recognized principles for handling electronic evidence by law enforcement. For example, none of the eight seized FARC computer exhibits was directly accessed by these experts.

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

- € The verification of the eight seized FARC computer exhibits by INTERPOL does not imply the validation of the accuracy of the user files, the validation of any country's interpretation of the user files or the validation of the source of the user files. It is well established that for law enforcement purposes, factual findings concerning the truth or accuracy of the content of any item of evidence are made in the context of a judicial process at the national or international level and/or by a specially appointed commission with jurisdiction over the matter in dispute.

- € In addition to this public report, INTERPOL has provided a classified technical report to the Colombian authorities in conformity with the *Technical Assistance Agreement*. This classified report includes electronic copies of all of the user files on the eight seized FARC computer exhibits. It also contains a detailed comparison of 18 documents provided by Colombia to the two INTERPOL experts as hard copies and 41 additional documents given in electronic format.

- € Finally, INTERPOL's CompFor IRT has identified a number of issues with regard to the conduct of international computer forensic examinations and with regard to the handling of electronic evidence by law enforcement officials, especially those who are the first to respond to a crime scene. These issues are not only directly relevant to Colombia but also for law enforcement officers in all of INTERPOL's 186 member countries. Addressing them effectively requires INTERPOL and its member countries to develop a number of initiatives which are explained in detail in Part 6 ("Recommendations for INTERPOL and its member countries") of this report.

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

**PART 1: OPERATIONAL FRAMEWORK FOR INTERPOL'S INDEPENDENT
EXAMINATION OF THE EIGHT SEIZED FARC COMPUTER EXHIBITS**

1.1 Eight seized FARC computer exhibits

1. In the early hours⁵ of Saturday, 1 March 2008, Colombian authorities conducted a narco-trafficking and counter-terrorist operation against a suspected camp of the *Fuerzas Armadas Revolucionarias de Colombia* (FARC) - Revolutionary Armed Forces of Colombia. The camp was located at co-ordinates N 00 21 45 W 76 20, 1.9km (1.2 miles) on the Ecuadorian side of the border with Colombia across from the province of Putumayo. During this operation, Colombian authorities recovered three laptop computers, two external hard disks and three USB thumb drives, hereinafter referred to as the “eight seized FARC computer exhibits⁶.”

2. The eight seized FARC computer exhibits belonged to Raúl Reyes, the *nom de guerre* of Luis Edgar Devia Silva, who was on the FARC's seven-member Secretariat and acted as the organization's chief negotiator and spokesperson. Reyes and Guillermo Enrique Torres, alias Julián Conrado, a FARC commander, were killed in the operation. FARC has been designated a terrorist organization by Colombia, other governments and INTERPOL,.

3. Within the context of the regional tensions related to this seizure, Colombian authorities sought the assistance of INTERPOL to conduct an independent forensic examination of the eight seized FARC computer exhibits⁷.

1.2 Request for assistance from Colombia

4. On 4 March 2008, three days after the operation by Colombian authorities, INTERPOL received a request via two separate channels seeking its independent computer forensic technical assistance to examine the user files on the eight seized FARC computer exhibits and to determine

⁵ According to a timeline provided by Colombian authorities, the seizure of the eight FARC computer exhibits took place between approximately 5:50 a.m. and 7:50 a.m. (local time, GMT -5:00).

⁶ The factual summary as to what occurred from 1 March 2008 until the eight seized FARC computer exhibits were turned over to INTERPOL computer forensic experts on 10 March 2008 in Bogotá for the purpose of making a forensic image of the exhibits is based on representations made by Colombian authorities to INTERPOL both in writing and orally during classified briefings, and in the computer forensic examination conducted by INTERPOL's experts.

⁷ Please refer to Appendix 1 for descriptions and images of the eight seized FARC computer exhibits.

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

whether any of the user files had been newly created, modified or deleted following the seizure by the Colombian authorities on 1 March 2008.

5. A letter⁸ was sent by Colombia's *Departamento Administrativo de Seguridad* (DAS) – the Administrative Department for Security – through INTERPOL's National Central Bureau (NCB) in Bogotá. This same letter was also sent by the Director General of the Colombian National Police, Brigadier General Oscar Adolfo Naranjo Trujillo, to Colombia's liaison officer at the headquarters of the European Police Office in The Hague, Netherlands, who then communicated this request to INTERPOL's liaison officer based there. This was forwarded to the Director of INTERPOL's National Central Bureau Services and I-24/7 Development in Lyon, France.

6. These requests went through the appropriate chain of command, reaching the INTERPOL Secretary General that same day, 4 March 2008.

7. When any member country requires assistance from INTERPOL, it can make a request bilaterally or multilaterally via INTERPOL's secure global police communications system, known as I-24/7, which is installed in the INTERPOL National Central Bureau of every member country. A country can also directly contact INTERPOL's General Secretariat in Lyon, France; any one of INTERPOL's five Sub-Regional Bureaus in Africa or the Americas; or INTERPOL's Liaison Offices in Asia and at the United Nations in New York.

8. Most frequently, at the national level, the head of the relevant National Central Bureau requests INTERPOL's assistance using I-24/7. Alternatively, the head of the agency under which the NCB is located or the head of any other law enforcement agency in a member country can request assistance from INTERPOL. The NCB is the designated point of contact between all law enforcement bodies in the country in which it is located and the INTERPOL General Secretariat. Officers working in NCBs are responsible for handling all INTERPOL issues related to transnational criminals and cross-border investigations, but they remain in the service of and completely under the authority of their national law enforcement bodies.

9. In the event of INTERPOL receiving requests for assistance from multiple channels at the national level, INTERPOL co-ordinates its assistance by working through the head of the NCB or the head of the agency under which the NCB is located.

⁸ Please refer to Appendix 2 for the full text of the letter.

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

10. Since the requests from Colombia came through two different channels, INTERPOL recommended clear and pre-defined communication channels for the purposes of this Incident Response Team (IRT). The Secretary General replied to the Director of Colombia's *Departamento Administrativo de Seguridad*, Ms Hurtado Afanador, in a letter dated 5 March 2008⁹, stating explicitly that INTERPOL would communicate directly with her – who in her capacity as Director of the DAS oversees the NCB in Bogotá – and that the NCB would be the single point of contact for INTERPOL with the Colombian authorities. A copy of this letter was also sent to the Director General of the Colombian National Police, Brigadier General Oscar Adolfo Naranjo Trujillo. The aim was to ensure that all work performed by the IRT complied with INTERPOL's rules and regulations.

11. The Secretary General's letter proposed that INTERPOL immediately deploy an IRT to Colombia with a mandate to examine the technical feasibility of the Colombian request and to provide advice on how to carry out the work if judged feasible.

12. INTERPOL's proposal was accepted by Director Hurtado Afanador in a letter addressed to the Secretary General on 6 March 2008¹⁰.

13. At the time of the requests from Colombia, INTERPOL Secretary General Ronald K. Noble was participating in INTERPOL's 20th Asian Regional Conference in Hong Kong, China. He asked the heads of delegation from Singapore (Police Commissioner Boon Hui Khoo, Singapore Police Force) and Australia (Commander Paul Osborne, Manager, International Network, Australian Federal Police) whether they would be willing to identify computer forensic experts in their national police forces who could take part in the IRT. Both agreed.

14. Identifying experts from member countries when specific expertise is needed falls within INTERPOL's standard procedures for assembling and deploying IRTs. INTERPOL sought the assistance of experts from Australia and Singapore for several practical reasons: their police services have widely recognized technological expertise in computer forensics; they have been active and generous supporters of INTERPOL's work in providing police support and training to other member countries; the selected experts did not read Spanish and could thus avoid being

⁹ Please refer to Appendix 3 for the full text of the letter.

¹⁰ Please refer to Appendix 4 for the full text of the letter.

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

influenced by the content of the data; and their being from the Asia-Pacific region reinforced their impartiality.

1.3 INTERPOL's operational support to member countries

15. Colombia has first-hand knowledge of the tools and services that INTERPOL can offer, having hosted INTERPOL's 19th Americas Regional Conference in Bogotá from 25 to 27 September 2007 and having participated actively in INTERPOL's programmes and initiatives through the National Central Bureau in Bogotá.

16. The world's largest international police organization, INTERPOL aims to facilitate cross-border police co-operation, and support and assist all organizations, authorities and services whose mission is to prevent or combat international crime. INTERPOL's four Core Functions, as approved by its supreme governing body, the General Assembly, are providing secure global police communications, operational data services and databases for police, operational police support services, and police training and development to law enforcement bodies in all of its 186 member countries¹¹.

17. One of INTERPOL's primary means for providing operational support to police globally is the deployment of Incident Response Teams to member countries faced with crisis situations, either natural or man-made, or with circumstances which require resources or expertise outside the ordinary capacity of that specific member country. Please refer to the text box on the following page for more information.

¹¹ Further details of the four Core Functions are available on INTERPOL's website: www.interpol.int

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

Incident Response Teams

Upon the request of a member country, an INTERPOL IRT can be briefed, equipped and deployed to anywhere in the world within 12 to 24 hours of an incident.

An IRT is typically composed of expert police and support staff, tailored to the specific nature of the crime or disaster and the type of assistance INTERPOL is requested to provide. When specific police expertise is not readily available at its General Secretariat, INTERPOL calls on its network of police forces in its 186 member countries to identify one or more officers with the required expertise and skills. These experts are then deployed as part of the INTERPOL IRT and work exclusively for and report to INTERPOL for the duration of their deployment.

The first IRT was deployed in October 2002 to Indonesia following a terrorist bombing in Bali. Since then, 37 teams have been deployed to 25 different countries in Africa, the Americas, Asia, and Europe.

18. At the request of its member countries, INTERPOL frequently co-ordinates multi-country police investigations or provides support on issues affecting multiple countries. This support can be as simple as linking a suspected criminal to crimes in two different countries through a search of INTERPOL's databases, or as complex as co-ordinating the year-long international effort to identify victims of the 26 December 2004 tsunami which killed hundreds of thousands of people in Southeast Asia. The types of support provided by INTERPOL and the crime issues addressed are as diverse as INTERPOL's global membership.

19. INTERPOL assisted Mauritanian authorities in 2007 with the investigation into the country's largest-ever cocaine seizure. Three major suspects were arrested by Belgian and Moroccan authorities following an operational meeting organized by INTERPOL with investigators from 10 countries on three continents. Similarly, INTERPOL supported authorities in Guinea-Bissau in identifying a major network behind the trafficking of cocaine from South America to Europe via West Africa.

20. In the same year, more than 430 individuals were arrested during an operation co-ordinated by INTERPOL which targeted illegal soccer gambling controlled by organized crime gangs in seven jurisdictions in Southeast Asia. A total of 272 underground gambling dens, which were estimated to have handled more than US\$680 million in illegal bets worldwide, were identified and shut down by police in participating countries during the five-month operation.

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

21. Another operation conducted in 2007 in partnership with police and customs authorities in Argentina, Brazil, Chile, Paraguay and Uruguay significantly disrupted the activities of organized crime networks involved in pharmaceutical and consumer-product counterfeiting in the region, with more than 120 criminals arrested, goods worth approximately US\$30 million seized, and main trafficking routes and modus operandi identified.

22. Fingerprints submitted by Spain and checked against INTERPOL's database by Serbia helped identify and locate a suspect in the 11 March 2004 train bombings in Madrid who had fled Spain and travelled through at least six different countries in Europe before finally being arrested by police in Serbia.

23. INTERPOL has successfully conducted two worldwide public appeals for assistance in identifying individuals who appeared in images of child sexual abuse on the Internet. The first, in October 2007, led to the arrest of the suspect 11 days later in Thailand, while the suspect in the second global appeal was arrested in the United States 48 hours after the launch of the appeal.

24. Additionally, as in the case with Colombia, INTERPOL, when requested, provides independent law enforcement support in international investigations. At the request of the United Nations, specialized officers from INTERPOL supported the UN International Independent Investigation Commission in Beirut with its investigation into the assassination of former Lebanese Prime Minister Rafik Hariri in 2005. INTERPOL also supported the UN Independent Inquiry Committee which investigated alleged corruption connected to the Oil-for-Food Programme for Iraq.

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

**PART 2: PHYSICAL HANDOVER OF THE SEIZED COMPUTER EXHIBITS BY
COLOMBIAN POLICE TO INTERPOL'S INCIDENT RESPONSE TEAM AND
FORENSIC ACQUISITION OF THE EXHIBITS**

25. After the conditions for the deployment of the IRT to Colombia had been finalized, INTERPOL's management nominated officers from the General Secretariat to participate in the IRT along with the experts from Australia and Singapore. A team leader and one computer forensic specialist from INTERPOL were assigned to the IRT.

26. It was determined that during the course of their forensic examination of the eight seized FARC computer exhibits, the experts from Australia and Singapore would function as INTERPOL officials for all purposes related to their expert technical work, which meant they would report to INTERPOL staff in the discharge of their official duties and not their national administrations. This also meant that they would not report on any aspect of the forensic examination to their national administrations. Australian and Singaporean authorities agreed to these conditions by virtue of allowing their experts to become INTERPOL officials.

27. The legal basis for this request is enshrined in Article 30 of INTERPOL's Constitution, which states:

"In the exercise of their duties, the Secretary General and the staff shall neither solicit nor accept instructions from any government or authority outside the Organization. They shall abstain from any action which might be prejudicial to their international task.

Each Member of the Organization shall undertake to respect the exclusively international character of the duties of the Secretary General and the staff, and abstain from influencing them in the discharge of their duties.

All Members of the Organization shall do their best to assist the Secretary General and the staff in the discharge of their functions."

28. The INTERPOL delegation arrived in Bogotá, Colombia, on Sunday, 9 March 2008¹². Led by INTERPOL's Secretary General, the six-person delegation included the four IRT members mentioned above and INTERPOL's General Counsel, to provide the appropriate legal framework for INTERPOL's work.

¹² Members of the IRT arrived at different dates and times between 8 and 9 March, but by Sunday, 9 March, all team members had arrived in Bogotá.

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

29. During this initial deployment, the Secretary General and the General Counsel met with relevant Colombian authorities and concluded a *Technical Assistance Agreement* which defined the terms and scope of the assistance to be provided. Please refer to Part 4 (“INTERPOL’s independence”) for more information and to Appendix 5 for the full text of the agreement.

30. The IRT began its work on 10 March 2008 by identifying the precise technical requirements of Colombia’s request. Officers from the Colombian Judicial Police’s computer forensics unit (*Grupo Investigativo de Delitos Informáticos*) briefed the IRT about the chain of custody, equipment and software used, and the procedures the officers had followed in the handling of the eight seized FARC computer exhibits up to this point.

31. According to the Colombian authorities, all of the items had been seized from a FARC camp between approximately 5:50 a.m. and 7:50 a.m. (local time at location of seizure, GMT -5:00) on Saturday, 1 March 2008.

32. On 3 March 2008, at 11:45 a.m. local time, the exhibits were handed over to the Colombian Judicial Police’s computer forensics unit, which kept the eight seized FARC computer exhibits in its custody until they were provided to the IRT.

33. After obtaining custody of the exhibits, the IRT first made a detailed inventory of all of the equipment that had been handed over, including a digital photograph and description of the trademark, model and serial number of each item, in accordance with internationally recognized principles for handling electronic evidence by law enforcement¹³. A duly executed chain of custody documented whenever any of the eight seized FARC computer exhibits were accessed.

34. Using their own laptops, equipment and software, the experts began the forensic acquisition of the data contained in the eight seized FARC computer exhibits. This is known as “imaging” in computer forensic terminology. To determine whether the imaging succeeded, the IRT checked and validated the integrity of the images by confirming that the hash values of the eight seized FARC computer exhibits and the images matched. Please refer to the text box on the next page for more information on the “imaging” process and an explanation of hash values.

¹³ Please refer to Appendix 6, “General Principles,” *Seizure of e-Evidence*, Version 1.01, 15.12.2003, European Union Project from the Programme OISIN II managed by the Directorate-General of Justice and Home Affairs in partnership and co-operation with INTERPOL.

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

35. The data were successfully imaged to two disk drives – each image involved two disk drives, because the data were too voluminous for one disk; this is in line with internationally recognized principles for handling electronic evidence by law enforcement. This process was repeated a second time to obtain a second image of the data, so in all, two forensic images of all of the material were generated.

Forensic acquisition of computer data

“Imaging” is the process whereby an exact duplicate of the hard disk of electronic equipment or digital storage media is made. The process of imaging in the context of computer forensics is very different from an “electronic copy” of a file that an average computer user can make.

Firstly, there is a methodological difference. Imaging requires dedicated forensic software operated by individuals with computer forensic skills. The computer should not be booted (i.e., turned on). For a user to make a copy of a file, the computer needs to be switched on. Regardless of the operating system installed on the computer, booting the computer leads to modifications of certain data on its hard drive. While these may be invisible and irrelevant to the user, these system operations matter to forensic experts, because the latter will not only analyze the user files such as written documents, images and sound files, but also look at hidden data and information contained in system files, i.e., information that is generated “automatically” by the computer while processing information.

Secondly, the nature of the copying is different. Imaging makes an exact duplicate of the hard disk content: a forensic image is a 1:1 mirror containing the complete contents and structure of a data storage medium or device, such as a hard drive, a USB thumb drive, a CD or a DVD. An image file is usually created based upon the sectors on the medium (bit stream copy), ignoring its file system. As such, an image contains all of the information necessary to replicate exactly the structure and all contents of a storage device. Imaging requires proper precautions, by using write-blockers, to ensure that during the process, nothing is modified on the original exhibit.

The third difference is that forensic imaging involves a validation process to determine if the image is completely identical to the original. This is done through the comparison of hash values. A hash value is a string of numbers and characters generated by using a specific algorithm. The hash value is generated according to the data on the computer and is absolutely unique to each storage device. By comparing the hash value generated from the original with those from the image, forensic examiners can determine whether or not the imaging was successful. If they match, the imaging was successful; if they do not match, the process must be repeated from the beginning.

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

36. On Wednesday, 12 March 2008, the eight seized FARC computer exhibits were returned to the attorney leading the investigation. The receipt and return of each item by the IRT to the Colombian authorities were recorded on chain-of-custody stickers, which were affixed to the sealed pouches containing each item.

37. By Thursday, 13 March 2008, the first set of disk drives had been sealed in uniquely identified pouches and placed in an evidence safe. The second set of disk drives was used for the actual analysis of the data by the INTERPOL experts, who followed internationally recognized principles for handling electronic evidence by law enforcement¹⁴.

¹⁴ Ibid.

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

**PART 3: TRANSFER OF THE IMAGE DISKS BY DIPLOMATIC POUCH FROM
COLOMBIA TO SOUTHEAST ASIA**

38. It quickly became apparent that the IRT could not complete its work during the initial deployment period to Colombia because of the volume and complexity of the data to be examined. The data contained in the eight seized FARC computer exhibits amounted to approximately 609.6 gigabytes, which if converted to full-page text documents would equal 39.5 million pages. It was estimated that the forensic examination would take approximately four to six weeks, with the two experts each independently examining images of four of the eight seized FARC computer exhibits.

39. Given the scale of the task, the INTERPOL Secretary General and the Colombian authorities agreed that the computer forensic experts would continue with the actual forensic examination in their usual workplaces in Southeast Asia.

40. This decision added to the complexity of INTERPOL's work. Firstly, the Secretary General had to secure the agreement of the Commissioners of the Australian Federal Police and the Singapore Police Force to extend the secondment of both experts for the period necessary to complete their work. Secondly, agreement had to be obtained from the competent Colombian police and prosecutorial authorities that data classified as "ULTRA SECRETO" could be possessed by non-Colombian law enforcement officials outside of Colombia. Thirdly, diplomatic and logistical arrangements needed to be made to transport this classified data from Colombia to Southeast Asia.

41. On 18 March 2008, the Secretary General wrote to the Australian and Singaporean police Commissioners to ask them to authorize the officers concerned to continue their missions. The letter explicitly requested that the two officers continue to be assigned to INTERPOL on a full-time basis and, even more importantly, that their work should be considered confidential and independent. As a result, the analysis performed by the experts for the purpose of this report would be communicated to INTERPOL and the Colombian authorities only and not to their national administrations, nor would they take instructions from their national administrations as to how to carry out their work.

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

42. The Australian Federal Police and Singapore Police Force both formally confirmed their agreement to the Secretary General's request in writing.

43. The Colombian authorities, after consultation with the competent national governmental authorities, agreed to allow the classified data to leave the country, which meant a legal basis for preserving the confidentiality of the data from access by any country during the data's transit to Southeast Asia had to be established.

44. It was agreed that the best and most secure way to transport the image disks was via diplomatic pouch by authorized Colombian government officials, ensuring the data were protected by diplomatic immunity. The IRT took all of the necessary steps to mark and seal the image disks produced by the INTERPOL experts of the eight seized FARC computer exhibits that would be delivered to the offices of the experts, and a chain of custody was duly established.

45. INTERPOL's Command and Co-ordination Centre (CCC) in Lyon actively monitored the transportation of the materials until their safe arrival in Southeast Asia. The CCC is designed to provide immediate police assistance to any INTERPOL member country around the clock and in any of INTERPOL's four official languages (Arabic, English, French and Spanish). This allowed INTERPOL to know at all times the exact location of the image disks produced by the INTERPOL experts of the eight seized FARC computer exhibits and, if necessary, to intervene if any problems were encountered during the journey.

46. The IRT left Bogotá between 14 and 16 March 2008. On Tuesday, 25 March at 6:30 p.m. (local time), the pouches left Bogotá accompanied by two Colombian police officers. They arrived safely at their respective destinations on 27 March 2008.

47. In addition to the image disks, Colombian authorities delivered two white binders, one to each expert, containing hard copies of 18 documents, under 13 separate headings, selected by them. These documents had been marked "*ULTRA SECRETO*" by Colombian authorities. They requested that INTERPOL's experts locate these documents among the 609.6 gigabytes of data contained in the images of the eight seized FARC computer exhibits. They asked that INTERPOL determine and report whether any data had been added to or deleted from these documents, i.e. whether these selected documents had been modified in any way.

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

48. The Colombian authorities also provided a single disk containing soft copies of documents that Colombian experts were using as part of their ongoing investigation into the FARC. These documents contained annotations made by Colombian authorities as part of their investigation. Unlike the hard copies of the documents contained in the white binder, INTERPOL was simply asked to find these documents so that Colombian authorities would know in how many locations and in how many of the eight seized FARC computer exhibits these documents could be found. Please refer to Part 5 (“Major Public Findings”) for more information.

49. After the receipt of their working copies of the eight seized FARC computer exhibits on 27 March 2008, INTERPOL’s computer forensic experts were able to begin their examination in earnest.

50. The forensic examination was completed on Friday, 9 May 2008. The two experts from Australia and Singapore travelled to the INTERPOL General Secretariat from 11 to 12 May 2008 to brief a working group of external forensic experts and INTERPOL officials on the methodology used and steps taken to reach their conclusions.

51. The full results of the INTERPOL experts’ forensic examination are described in Part 5 (“Major Public Findings”). Each INTERPOL expert produced a full, in-depth forensic analysis report which was delivered to Colombian authorities as part of the *Technical Assistance Agreement* concluded between the Colombian authorities and INTERPOL.

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

PART 4: INTERPOL'S INDEPENDENCE

52. While it was clear from the outset that Colombia's request was well within the scope of INTERPOL's mission¹⁵, there were a number of elements surrounding Colombia's operation on 1 March 2008 that needed to be explicitly clarified by INTERPOL as part of its independent examination of the eight seized FARC computer exhibits. INTERPOL was sensitive to the multi-country controversy surrounding the operation and took great care to avoid the appearance of partiality in a dispute involving countries which are members of INTERPOL in good standing.

53. INTERPOL took a number of steps to clearly assert its independence. On Friday, 7 March 2008, the Secretary General sent a message to INTERPOL's Senior Vice-President Arturo Herrera Verdugo and to all members of its Executive Committee, as well as to all 186 INTERPOL National Central Bureaus, to clearly explain what had been agreed with the Colombian authorities and to emphasize that INTERPOL's role was exclusively technical¹⁶. In addition, the Secretary General expressed his willingness and availability to travel to any INTERPOL member country that requested a meeting to discuss this matter.

54. The Secretary General also informed INTERPOL's membership that he would personally travel to Colombia with the IRT "to ensure that there is no misunderstanding about the team's tasks and responsibilities; to ensure that the working conditions will permit them to function in an independent atmosphere; and to ensure that any last-minute questions or issues can be efficiently dealt with and resolved."¹⁷

¹⁵ The Colombian authorities specifically asked for computer forensic assistance in the framework of a law enforcement investigation. Not only is this in line with INTERPOL's global mission as defined in its Constitution, but providing operational police support to member countries is also an inherent part of INTERPOL's strategy and is one of the organization's four Core Functions explicitly endorsed by its General Assembly.

¹⁶ Please refer to Appendix 7 for the full text of the message transmitted via INTERPOL's I-24/7 global police communications network to all 186 National Central Bureaus on 7 March 2008.

¹⁷ Ibid.

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

55. On Saturday, 8 March 2008, while the IRT was making final preparations for its deployment the next day, the INTERPOL Secretary General spoke by telephone with Mr José Miguel Insulza, Secretary General of the Organization of American States (OAS) to advise him of the exclusively technical expertise to be provided by INTERPOL. Secretary General Insulza stated that he strongly and publicly supported INTERPOL's providing an independent examination to determine whether any user files had been newly created, modified or deleted from the eight seized FARC computer exhibits following their seizure by Colombian authorities on 1 March 2008.

56. In addition, during INTERPOL's 4th Heads of NCBs meeting held in Lyon, France, from 2 to 4 April 2008, the Secretary General met with the heads of delegation from Colombia, Ecuador and Venezuela to explain the exclusively technical remit of INTERPOL's assistance to Colombia and to reiterate his offer from 7 March 2008 to travel to any INTERPOL member country that had concerns about INTERPOL's deployment of the IRT. The Secretary General followed this up with separate letters to the national police commissioners of Colombia, Ecuador and Venezuela and to the Director of Colombia's *Departamento Administrativo de Seguridad*¹⁸. Colombia was the only INTERPOL member country that asked to meet with INTERPOL's Secretary General and no country objected to INTERPOL's examination of the eight seized FARC computer exhibits.

¹⁸ Please refer to Appendix 8 for the full text of the letters sent to the relevant Colombian, Ecuadorian and Venezuelan officials.

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

PART 5: MAJOR PUBLIC FINDINGS

This section of the report contains INTERPOL's findings upon completion of its forensic analysis¹⁹. The accuracy and source of the content of the data remain outside the scope of INTERPOL's computer forensic evaluation.

**Amount and type of data contained in the eight seized FARC
computer exhibits**

Finding 1: The eight seized FARC laptop computers, USB thumb drives and external hard disks contain a total of 609.6 gigabytes of data, including documents, images and videos.

57. INTERPOL was asked to forensically examine a total of eight seized FARC computer exhibits: three laptop computers, two external hard disks and three USB thumb drives. Each exhibit was given a unique reference number by Colombia²⁰. The three laptops are referenced as exhibits 26, 27 and 28. The two external hard disks are exhibits 30 and 31, and the three seized USB thumb drives are exhibits 32, 33 and 34²¹.

58. All the data were indexed by INTERPOL's computer forensic experts to enable them to perform keyword searches in order to locate documents that could be relevant to the investigation. This is a labour-intensive and time-consuming process. The imaging²² of the data took three days and the indexing of the exhibits took one week in total. This index will also enable the Colombian investigators to easily retrieve any user files from the eight seized exhibits at a later stage if or when their investigation identifies other documents of law enforcement value.

59. In total, these eight exhibits contain 609.6 gigabytes of data.

¹⁹ The classified report contains additional findings that provide more detail on the comparison of specific documents found on the exhibits. As this information is classified, the contents of these findings cannot be revealed in this public report. However, it should be noted that all of the classified findings are consistent with the public findings contained in this report.

²⁰ Each exhibit was given a unique reference number for the purpose of accurately and comprehensively documenting the chain of custody.

²¹ It should be noted that exhibit 29 was not provided to INTERPOL for its forensic examination as it was not an electronic data storage device and therefore required no computer forensic analysis. This explains the gap in the sequential numbering of the exhibits.

²² For an explanation of forensic imaging see page 18.

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

60. In non-technical terms, the volume of 609.6 gigabytes of data would correspond to 39.5 million filled pages in Microsoft Word²³ and, if all of the seized data were in Word format, it would take more than 1,000 years to read it all, at a rate of 100 pages per day.

61. For the purposes of this report, we have classified the files found on the exhibits referred to in three categories:

1. Operating system²⁴ files
2. Application files
3. User files

62. Operating system files are used by a computer in the course of normal operations, such as start-up, running and shutdown. These files are frequently created, accessed and modified without the user being aware.

63. Application files are associated with software installed on the computer over and above the operating system. Applications include word processors, media players and anti-virus software. Anti-virus programs are particularly active by design in order to ensure that all files present on the computer are free of malicious code. Application files are attributable to the application and are outside the direct control of the user. For example, when a user opens an existing document with Microsoft Word, a temporary back-up copy is created on the hard drive.

64. User files are directly attributable to the user and the user is responsible for and has control of the content. User files include word processing documents, spreadsheets and music files. For example, when a user saves a document using Microsoft Word, the resulting file stored on the hard drive or other device is a user file.

65. For the purpose of this report, the term "system files" is used to collectively describe operating system files and application files.

66. The 609.6 gigabytes include both system files and user files. INTERPOL's classified report contains all of the user files that were stored on the eight seized exhibits. It is the sovereign decision of the Colombian authorities to decide which of that data should be declassified.

²³ Calculations based on information found on the website of Setec Investigations, "How Many Pages per Gigabyte and Megabyte", www.setecinvestigations.com

²⁴ It should be noted that all three laptop computers that were seized (exhibits 26, 27 and 28) had Microsoft operating systems installed on them.

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

67. Without revealing the content of the data, INTERPOL can state the following with regard to the user files contained in the eight seized FARC computer exhibits:

- € 109 document files were found on more than one of the exhibits
- € 452 spreadsheets
- € 7,989 e-mail addresses
- € 10,537 multimedia files (sound and video)
- € 22,481 web pages
- € 37,872 written documents (such as Word documents, PDF files, text format documents)
- € 210,888 images

Of the above, 983 files were found to be encrypted.²⁵

**Verification of nature of access to the eight FARC computer exhibits
between their seizure on 1 March 2008 and their handover to
INTERPOL's computer forensic experts
on 10 March 2008**

68. Given that Colombia seized the eight FARC computer exhibits on 1 March 2008, and that there were questions in the media about whether Colombia had altered or tampered with the seized exhibits, INTERPOL was called in to independently determine whether any files had been created, accessed, modified or deleted on or after the 1 March 2008 seizure date.

69. Each file on a computer or an electronic storage device has an electronic timestamp that specifies the date and time on which the file was created, last accessed, last modified or deleted. Using forensic software, INTERPOL's experts extracted the timestamp information for the files on each exhibit, distinguishing between system files and user files. They also verified the system time settings on each of the three seized laptop computers, as these settings provided a baseline for the timestamps. For files on external hard disks or USB thumb drives, the date and time settings are usually taken from the computer to which they were connected when the files were created, accessed, modified or deleted.

²⁵ Encryption is a method of scrambling and encoding data to prevent anyone except the intended recipient from reading that data.

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

Finding 2: All seized FARC computer exhibits were accessed by Colombian authorities between 1 March 2008, when they were seized, and 10 March 2008, when they were handed over to INTERPOL's computer forensic experts.

70. INTERPOL will explain in layperson's terms the two primary ways in which data contained in laptop computers, USB thumb drives and external hard disks can be accessed. One way is in conformity with internationally recognized principles for handling electronic evidence by law enforcement²⁶, and the other way is in non-conformity with these principles.

Finding 2a: Access to the data contained in the eight seized FARC computer exhibits by the *Grupo Investigativo de Delitos Informáticos* of the Colombian Judicial Police between their receipt at 11:45 a.m. on 3 March 2008 and their handover to INTERPOL's computer forensic experts on 10 March 2008 conformed to internationally recognized principles for handling electronic evidence by law enforcement.

71. Handling electronic evidence in conformity with internationally recognized principles requires adherence to a rigorous methodology. In co-operation with its member countries and regional governmental and law enforcement institutions, INTERPOL has co-authored a set of international principles for the handling of electronic data evidence²⁷. These principles were formally presented to the INTERPOL Cybercrime Conference in Cairo, Egypt, in 2004 and are available to law enforcement officers in all 186 INTERPOL member countries through the Organization's secure website.

72. Colombia's National Police has qualified and trained computer forensic experts. Its expert unit is called the *Grupo Investigativo de Delitos Informáticos* (hereinafter referred to as "Colombia National Police's computer forensic experts") and is located within the *Dirección de Investigación Criminal* (Colombian Judicial Police). The Head of the Colombia National Police's Computer Forensic Experts Unit was Vice-President of the training subgroup of INTERPOL's Latin America Working Party on Information Technology Crime from January 2007 to April 2008. He is still the permanent representative for Colombia on the Working Party.

²⁶ See Findings 2a and 2b for an explanation of the internationally recognized principles for handling electronic evidence by law enforcement.

²⁷ *Seizure of e-Evidence*, Version 1.01, 15.12.2003, EU Project from the Programme OISIN II managed by the Directorate-General Justice and Home Affairs (co-authored and partnered by INTERPOL).

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

73. As part of INTERPOL's forensic examination of the eight seized FARC computer exhibits, INTERPOL reviewed the process followed by the Colombia National Police's computer forensic experts to handle the electronic evidence seized on 1 March 2008. The Colombia National Police's computer forensic experts took custody of the eight seized FARC computer exhibits on 3 March 2008 at 11:45 a.m. (local time in Bogotá)²⁸.

74. The procedures used by the Colombian Judicial Police for recording, documenting, photographing and labelling, imaging²⁹ and copying each of the exhibits were found by INTERPOL's experts to conform to internationally recognized principles for the handling of electronic evidence by law enforcement, thus ensuring that none of the data contained in the seized exhibits had been altered, damaged or destroyed during the handling of the evidence.

75. The precise technical details of all of the steps taken by Colombia National Police's computer forensic experts to examine the eight seized computer exhibits are set forth in great detail by INTERPOL's experts in their classified technical report. It is absolutely clear that the Colombia National Police's computer forensic experts conformed to the fundamental principle that law enforcement should not, under ordinary circumstances, directly access seized electronic evidence. Instead, law enforcement should make a physical image of the data on the computer hardware in question, using a write-blocking device to avoid having any impact on the operating system files of the computer and to avoid the necessity for a detailed and time-consuming examination of the seized electronic evidence in order to prove that there was no tampering with or effect on the actual content of the user files at the time that direct access occurred.

76. Because the Colombia National Police's computer forensic experts handled the eight seized FARC computer exhibits in compliance with internationally recognized principles for conducting computer forensic examinations, no data were created, added, modified or deleted on any of the these exhibits between 3 March 2008 at 11:45 a.m.³⁰ and 10 March 2008, when the exhibits were handed over to INTERPOL's experts to make their image disks.

²⁸ The actual seizure of the eight computer exhibits occurred between 5:50 a.m. and 7:50 a.m. (local time at the place of seizure, GMT -5:00) on Saturday, 1 March. However, it was not until more than 48 hours later that the eight seized exhibits were given to the computer forensic specialists of the Colombian Judicial Police. This occurred on Monday, 3 March 2008 at 11:45 a.m. local time in Bogotá, Colombia (GMT -5:00).

²⁹ For an explanation of forensic imaging, see page 18.

³⁰ Local time in Bogotá, Colombia (GMT -5:00).

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

Finding 2b: Access to the data contained in the eight FARC computer exhibits between 1 March 2008, when they were seized by Colombian authorities, and 3 March 2008 at 11:45 a.m., when they were turned over to the *Grupo Investigativo de Delitos Informáticos* of the Colombian Judicial Police, did not conform to internationally recognized principles for handling electronic evidence by law enforcement.

77. When law enforcement directly accesses seized electronic evidence without first making physical images of the data, such access leaves traces of the relevant law enforcement officer's accessing and viewing of the evidence. Direct access may complicate validating this evidence for purposes of its introduction in a judicial proceeding, because law enforcement is then required to demonstrate or prove that the direct access did not have a material impact on the purpose for which the evidence is intended.

78. Using forensic tools, law enforcement computer experts can determine the different types of temporary and permanent system files that were created in the computer as a result of it either being turned on or off. For law enforcement investigative purposes, INTERPOL will not disclose the specific forensic tools that were used to make this determination during INTERPOL's examination of the eight seized FARC computer exhibits.

79. Colombian law enforcement authorities have openly stated to INTERPOL's computer forensic experts that an officer in their anti-terrorist unit directly accessed the eight seized FARC computer exhibits under exigent and time-sensitive circumstances between 1 March 2008, when they were seized by Colombian authorities, and 3 March 2008.

80. As stated above, using forensic tools, law enforcement computer experts can reconstruct what happens when seized electronic evidence is directly accessed and INTERPOL's experts have done so in their forensic examination.

81. As a result of this, INTERPOL's experts found that:

82. The operating systems of the three seized laptops all showed that the laptops had been shut down on 3 March 2008 (at different times, but all three prior to 11:45 a.m.³¹, the time of receipt by the forensic computer examiners of the Colombian Judicial Police). The two external hard disks and the three USB thumb drives had all been connected to a computer between

³¹ Local time in Bogotá, Colombia (GMT -5 :00).

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

1 and 3 March 2008, without prior imaging of their contents and without the use of write-blocking hardware.

83. Seized exhibit 26, a laptop computer, showed the following effects on files on or after 1 March 2008:

- € 273 system files were created
- € 373 system and user files were accessed
- € 786 system files were modified
- € 488 system files were deleted

84. Seized exhibit 27, also a laptop computer, showed the following effects on files on or after 1 March 2008:

- € 589 system files were created
- € 640 system and user files were accessed
- € 552 system files were modified
- € 259 system files were deleted

85. Seized exhibit 28, also a laptop computer, showed the following effects on files on or after 1 March 2008:

- € 1,479 system files were created
- € 1,703 system and user files were accessed
- € 5,240 system files were modified
- € 103 system files were deleted

86. Seized exhibit 30, an external hard disk, showed the following effects on files on or after 1 March 2008:

- € 1,632 system files were created
- € 11,579 system and user files were accessed
- € 532 system files were modified
- € 948 system files were deleted

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

87. Seized exhibit 31, also an external hard drive, showed the following effects on files on or after 1 March 2008:

- € 3,832 system files were created
- € 13,366 system and user files were accessed
- € 2,237 system files were modified
- € 1,049 system files were deleted

88. Seized exhibit 32, a USB thumb drive, showed the following effects on files on or after 1 March 2008:

- € 8 system files were created
- € 12 system and user files were accessed
- € 5 system files were modified
- € 6 system files were deleted

89. Seized exhibit 33, also a USB thumb drive, showed the following effects on files on or after 1 March 2008:

- € 54 system files were created
- € 168 system and user files were accessed
- € 28 system files were modified
- € 52 system files were deleted

90. Seized exhibit 34, also a USB thumb drive, showed the following effects on files on or after 1 March 2008:

- € 1 system file was created
- € 60 system and user files were accessed
- € 1 system file was modified

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

Finding 3: INTERPOL found no evidence that user files were created, modified or deleted on any of the eight seized FARC computer exhibits following their seizure on 1 March 2008 by Colombian authorities.

91. The direct access to the eight seized FARC computer exhibits between 1 March 2008 and 3 March 2008 left traces in the system files, as explained above. However, INTERPOL's experts found not a single user file on any of the eight exhibits had been created, modified or deleted following their seizure on 1 March 2008. Using their forensic tools, they found a total of 48,055 files for which the timestamps indicated that they had either been created, accessed, modified or deleted as a result of the direct access to the eight seized exhibits by Colombian authorities between the time of their seizure on 1 March 2008 and 3 March 2008 at 11:45 a.m.

92. INTERPOL's experts also found that one laptop computer (exhibit 28) and the two seized external hard disks (exhibits 30 and 31) contained files with erroneous date stamps, set in the future.

93. Exhibit 28 contains:

- € One file that was shown as created on 17 August 2009

94. Exhibit 30 contains:

- € 668 files with creation dates that range from 7 March 2009 to 26 August 2009
- € 31 files which show as having been last modified between 14 June 2009 and 26 August 2009
- € These files contained either music, video or images

95. Exhibit 31 contains:

- € 2,110 files with creation dates ranging from 20 April 2009 to 27 August 2009
- € 1,434 files which show as having been last modified between 5 April 2009 and 16 October 2010

96. Based on analysis of the characteristics of these files, INTERPOL's experts concluded that these files were originally created prior to 1 March 2008 on a device or devices with incorrect system time settings. The appearance of these files on exhibits 30 and 31 indicates that they were either created while the exhibits were connected to a device with incorrect system time settings or the files were later transferred – after their initial creation – to exhibits 30 and 31 and the 2009 timestamps were transferred with the files.

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

97. As for the single file present on exhibit 28 with a 2009 creation date, INTERPOL's experts concluded that this file was transferred to exhibit 28 after the file's initial creation and the 2009 creation date was transferred with the file.

98. Based on the above, INTERPOL's experts concluded that Colombian authorities should not rely on the time stamping of the files with future dates in these three exhibits (28, 30 and 31).

99. Taking into account all of the above and based on a comprehensive forensic examination, INTERPOL's experts conclude that no user files have been created, modified or deleted on any of the eight FARC computer exhibits following their seizure on 1 March 2008.

PART 6: RECOMMENDATIONS FOR INTERPOL AND ITS MEMBER COUNTRIES

Recommendation 1: Enhanced training for first-responder police units encountering electronic evidence during criminal investigations.

100. It is widely accepted as a problem within police forces around the world that first-responder police units – the law enforcement officers who first find the electronic evidence – do not as a general rule have adequate training with regard to how to handle and access electronic evidence contained in computers and electronic data storage devices.

101. The contents of INTERPOL's *IT Crime Manual* already provide a comprehensive basis for the content of such training programmes. In addition, the European Commission's AGIS project, '*Cybercrime Investigation – developing an international training programme for the future*³²,' has already outlined the need for and the contents of such training programmes.

102. Furthermore, a Resolution adopted at the 6th INTERPOL International Conference on Cybercrime, held in Cairo, Egypt, from 13 to 15 April 2004 stated that "*training and technical assistance should remain a priority for international efforts against cybercrime [...]*".

103. It is worth noting here that training in this area should not only be aimed at computer forensic experts, but particularly at first responders. It is clear that technology will continue to play an ever-increasing role in everyone's lives and, in the years to come, electronic evidence will be encountered increasingly in investigations.

104. INTERPOL has collaborated in the development of a series of cybercrime training courses that have been delivered by its trainers globally. INTERPOL will further enhance the capabilities of investigators to combat cybercrime and other forms of crime where electronic evidence is encountered, by delivering scheduled training courses and in particular training for first responders.

³² AGIS PROJECTS: 036/2003 and 167/2004 Final Report. Published by NSLEC, United Kingdom, September 2005.

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

Recommendation 2: Creation of a properly trained, dedicated and equipped computer forensic and Internet investigation unit at INTERPOL.

105. There are currently 1.3 billion Internet users worldwide³³. By 2010, the number of users will reach 1.8 billion³⁴. International travel will double between now and 2020, by which year there will be 1.4 billion international arrivals³⁵. Many international travellers will be carrying devices with electronic data stored in them. This will lead to significant increases in the number of multi-country investigations involving electronic evidence. In light of this, it is essential that INTERPOL has its own dedicated, fully trained and fully equipped unit to provide member countries with computer forensic training and assistance.

106. Both INTERPOL and Colombia were fortunate that within hours of INTERPOL's request, the Commissioners of the Australian Federal Police and the Singapore Police Force were willing to make a computer forensic expert available to work on an INTERPOL-led examination of eight seized FARC computer exhibits. Removing these experts from their day-to-day work for their respective police services at short notice placed a burden on their respective units, which already face heavy workloads, and meant neither police service was able to prepare properly for this deployment. Finally, at the time of the request by INTERPOL, it was apparent that INTERPOL and its experts would come under close scrutiny and could become the target of unfair or ill-considered politically motivated criticism.

107. Colombia's request to INTERPOL in this particular investigation highlights the importance for member countries to be able to call upon an independent and international organization such as INTERPOL to assist them with dealing with large amounts of electronic evidence.

108. It is noteworthy that such an endeavour is consistent with the Council of Europe's Convention on Cybercrime, which provides at Article 35 that *trained and equipped personnel are available [...] on a twenty-four-hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence*. This Convention has so far been ratified by 22 countries and signed by another 22 countries. However, in the long term, INTERPOL believes that the "around-the-clock

³³ <http://www.internetworldstats.com/stats.htm>

³⁴ <http://www.clickz.com/>

³⁵ Statistics from the World Tourism Organization

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

network” as envisaged in the Convention on Cybercrime should include all of INTERPOL’s 186 member countries. Currently, INTERPOL has already established National Central Reference Points on IT crime in 111 countries.

109. Such a unit should also build much-needed relationships with the private sector and the academic world. It would be crucial for the success of an INTERPOL computer forensic unit to be able to draw upon, when needed, specific expertise from the private sector and academia, because law enforcement alone will never be able to keep abreast of the fast pace of IT developments and changes.

110. For all of the above reasons, INTERPOL needs to prepare itself for the future in this regard by creating its own in-house expertise and specialized unit. As a direct result of the work on this case and the identified need for a specialist incident response centre, utilizing the resources of law enforcement, academia and the private sector, INTERPOL will, with the Centre for Cybercrime Investigations at the University College of Dublin (Ireland), explore the possibility of hosting such a centre on a pilot basis until INTERPOL is able to consult its member countries about the importance of establishing such a centre on a permanent basis.

Recommendation 3: Review of INTERPOL’s provision of computer forensic assistance to Colombia in order to identify lessons learned.

111. Any major international investigation, no matter how professionally and independently conducted, requires a thorough review in order to identify any lessons learned. This is particularly true in this case, where computer forensic experts from two INTERPOL member countries have been given access to classified documents seized by a third country and where the work was carried out on three different continents (the Americas, Asia and Europe) and in different languages.

112. None of these unprecedented factors has prevented INTERPOL from carrying out an independent and comprehensive review within the timeframe agreed upon by both parties. Yet, there were no standard operating procedures in place to deal with issues that will no doubt recur in the future – if not for INTERPOL, then for its member countries on a bilateral or multilateral basis. A candid, thorough and critical review will ensure that both INTERPOL and its member countries will benefit in the future.

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

113. INTERPOL will conduct such a critical review of its own involvement to identify areas for improvement as part of its standard management practices. Representatives from both the Colombian *Departamento Administrativo de Seguridad (DAS)* and the Colombian National Police, the two lead agencies in this investigation, will be invited to participate in that effort, as well as representatives from other INTERPOL member countries. INTERPOL will propose that its Executive Committee oversee its internal review.

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

LIST OF APPENDICES

- Appendix 1: Descriptions and photographs of the eight seized FARC computer exhibits
- Appendix 2: Letter sent to INTERPOL from the Director General of the Colombian National Police requesting assistance dated 4 March 2008
- Appendix 3: The INTERPOL Secretary General's response, dated 5 March 2008, to Colombia's request for assistance
- Appendix 4: Letter sent to INTERPOL Secretary General from the Director of Colombia's Departamento Administrativo de Seguridad (DAS) dated 6 March 2008
- Appendix 5: *Technical Assistance Agreement* between Colombia and INTERPOL
- Appendix 6: "General Principles," *Seizure of e-Evidence*, Version 1.01, 15.12.2003, European Union Project from the Programme OISIN II managed by the Directorate-General of Justice and Home Affairs in partnership and co-operation with INTERPOL
- Appendix 7: Message from INTERPOL Secretary General informing all National Central Bureaus of INTERPOL's assistance to Colombia dated 7 March 2008
- Appendix 8: Letters from the INTERPOL Secretary General to the relevant Colombian, Ecuadorian and Venezuelan officials dated 4 April 2008
- Appendix 9: Photographs of the FARC camp raided by Colombian authorities on 1 March 2008 and some images retrieved from seized FARC computer exhibits

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

This page has been intentionally left blank

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

Appendix 1: Descriptions and photographs of the eight seized FARC computer exhibits

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

This page has been intentionally left blank

Descriptions and photographs of the eight seized FARC computer exhibits

Images produced by INTERPOL's experts on 10 March 2008

<p>Item 26: Toshiba Satellite M55-5331 bearing serial number 16239763K</p> 	<p>Item 27: One Laptop Toshiba Satellite M55-5331 bearing serial number 16238282K</p> 	<p>Item 28: One Laptop Toshiba Satellite U205-S5057 bearing serial number 17040828H</p> 
<p>Item 30: One external hard drive LACIE bearing serial number JJ86708J60054QR</p> 	<p>Item 31: One external hard disk LACIE bearing serial number SJHHRDMH</p> 	<p>Item 32: One USB thumb drive SANDISK SDCZ6-2048RB bearing serial number BE0707AAFB</p> 
<p>Item 33: One USB thumb drive Cruzer Micro 2 GB bearing serial number 33</p> 	<p>Item 34: One USB thumb drive KINSTONCN J02907 04223- 3171002F</p> 	

Computer forensic product created from the eight exhibits





Photos provided to INTERPOL by Colombian authorities of the seized FARC computer exhibits.



Nine exhibits seized by the Colombian authorities bearing exhibit numbers 26, 27, 28, 29, 30, 31, 32, 33 and 34. (Number 29 did not form part of the analysis).

© The Colombian National Police



© The Colombian National Police



© The Colombian National Police

The underside of laptop exhibits 26, 27 and 28 showing their serial numbers.

© The Colombian National Police



The three seized USB thumb drives (exhibits 32, 33, 34) along with exhibit number 29.

© The Colombian National Police



Two external hard disks bearing exhibit numbers 30 and 31.

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

Appendix 2: Letter sent to INTERPOL from the Director General of the Colombian National Police requesting assistance dated 4 March 2008

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

This page has been intentionally left blank



NATIONAL POLICE OF COLOMBIA
GENERAL DIRECTION



Bogotá D.C.,

No. 00824 DIPON - DIPOL


MATTER : Requeriment technical forensic expert

TO : Doctor
RONALD KENNETH NOBLE
INTERPOL General Secretary
Bogotá.

With all respect, I require your helpful collaboration with the support of a technical forensic expert in order to practice an official evaluation of three (3) computers and three (3) USB devices, which were found during an operation developed by the Public Forces against drug trafficking and terrorism and against Luis Edgar Devia Silva, AKA Raúl Reyes, member of FARC's Secretariat.

Appreciating your attention to this requirement, I inform that the official contact for this matter will be the Colonel Cesar Augusto Pinzón Arana, Criminal Investigation Director, with contact on the movil phone numer [REDACTED]

Cordially,


Brigadier General **OSCAR ADOLFO NARANJO TRUJILLO**
General Director Colombian National Police

This page has been intentionally left blank

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

**Appendix 3: The INTERPOL Secretary General's response, dated 5 March 2008,
to Colombia's request for assistance**

Original version in Spanish and translation in English

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

This page has been intentionally left blank

200, quai Charles de Gaulle
69006 LYON - FRANCE

INTERPOL

The Secretary General
Le Secrétaire Général
El Secretario General
الأمين العام

Ronald K. Noble

5 de marzo de 2008

S/Referencia:

00266/DIPON-DIPOL

N/Referencia:

SG/2008/C096/037090/COL-NCB/RKN-mp

Objeto:

Ayuda de INTERPOL a Colombia

Estimada Sra. Hurtado Afanador:

Le escribo para confirmar la conversación que mantuvimos hoy en relación con una solicitud remitida por Colombia a INTERPOL acerca de la ayuda especializada que necesita su país en materia de investigación informática forense, en el marco de las pesquisas que llevan a cabo sus autoridades sobre la organización terrorista FARC. La solicitud de su país fue formulada por Vd. en su condición de Directora del D.A.S. y, por consiguiente, como máxima responsable de la Oficina Central Nacional de INTERPOL en Bogotá. La misma solicitud nos ha sido remitida asimismo por el Brigadier General Óscar Adolfo Naranjo Trujillo, en su calidad de Director General de la Policía Nacional colombiana. Para garantizar que todas nuestras actuaciones son conformes con el Estatuto y otros textos reglamentarios de INTERPOL, la Organización se comunicará directamente con usted, en su condición de Jefa de la OCN de Bogotá. Confiamos en que su OCN actúe como punto de contacto único con nosotros y en que se asegure de que toda la información adecuada se comunica del modo necesario a los organismos pertinentes colombianos encargados de la aplicación de la ley. (Enviaré asimismo una copia de la presente al Sr. Naranjo Trujillo).

Concretamente, han pedido Vds. a INTERPOL que les proporcione ayuda especializada en materia de investigación informática forense en relación con los datos almacenados en tres (3) ordenadores y tres (3) llaves USB que fueron decomisados en el marco de una operación contra el narcotráfico y el terrorismo centrada específicamente en las FARC y en uno de sus principales dirigentes. Tras debatir su solicitud con la Secretaría General de INTERPOL y con varios países miembros que poseen los conocimientos especializados necesarios en el ámbito de investigación citado, me complace poder informarla de que INTERPOL va a poder prestarles la ayuda solicitada.

.../...

He aquí mi propuesta. INTERPOL enviará a un equipo integrado por cinco personas: el Subdirector en funciones para esta misión ([REDACTED]) como jefe del equipo contará con el apoyo de tres especialistas en investigación informática forense (procedentes, respectivamente, de Australia, Corea y Singapur) y de un asistente operativo del Centro de Mando y Coordinación de INTERPOL. Si pudiera alcanzarse rápidamente un acuerdo sobre los puntos que figuran a continuación, INTERPOL haría todo lo posible para constituir el equipo, reunirlo y facilitar a sus miembros la información pertinente de forma que pudiera estar en Bogotá a principios de la semana que viene. A fin de cumplir este plazo necesitaríamos su ayuda para conseguir rápidamente los visados correspondientes. En esta primera fase todos los gastos de viaje, alojamiento y dietas correrían por cuenta de INTERPOL.

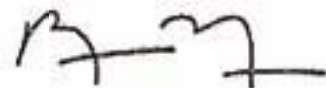
Se encomendaría al equipo el siguiente mandato:

- 1) determinar en términos técnicos precisos lo que Colombia necesita y establecer si lo que se pide es técnicamente posible;
- 2) en el caso de que lo que se pide sea técnicamente posible, informar a INTERPOL y a Colombia sobre el modo en que el equipo de INTERPOL pretende llevar a cabo tales tareas y realizar una estimación sobre el tiempo necesario para ello;
- 3) si tanto INTERPOL como Colombia estuvieran de acuerdo con la propuesta formulada por el equipo de INTERPOL, se daría a éste la autorización para proceder.

Tengo la esperanza de que este plan ofrecerá tanto a INTERPOL como a Colombia la oportunidad de asegurarse de que se lleve a cabo una evaluación adecuada de la situación y de encontrar la vía más útil para prestarles la asistencia solicitada. Como siempre, INTERPOL estará abierta a cualquier comentario o sugerencia que deseen realizar sobre la manera más eficaz en que INTERPOL podría aportar dicha ayuda.

Dado que hasta el viernes, 7 de marzo de 2008, estaré de misión oficial en Hong Kong (China) con ocasión de la Conferencia Regional Asiática, le ruego se sirva del Centro de Mando y Coordinación para comunicarse conmigo o con INTERPOL en relación con este asunto.

Le saluda atentamente,



Ronald K. Noble
Secretario General

Copia a: Brigadier General Óscar Adolfo Naranjo Trujillo
Director General de la Policía Nacional de Colombia

Sra. Dña. María del Pilar Hurtado Afanador
Directora del Departamento Administrativo de Seguridad
Carrera 28 n° 17A - 00 - Piso 9
Bogotá (Colombia)

TRANSLATION OF THE LETTER

5 March 2008

Your Ref.:

00266/DIPON-DIPOL

Our Ref:

SG/2008/C096/037090/COL-NBC/RKN-mp

Subject:

INTERPOL support to Colombia

Dear Mrs Hurtado Afanador:

This is to confirm our conversation today concerning a request that INTERPOL has received from Colombia concerning its need for expert computer forensic assistance in relation to Colombia's investigation of the terrorist organization FARC. Colombia's request has been made by you in your capacity as the Director of D.A.S. and thus the ultimate person responsible for Bogota's INTERPOL's National Central Bureau. We also have received the same request from Brigadier General Oscar Adolfo NARANJO TRUJILLO in his capacity as Director General of Colombia's National Police. In order to ensure that we are operating consistent with INTERPOL's Constitution and Rules, INTERPOL will communicate directly with you in your capacity as the Head of NCB Bogota'. We trust that NCB Bogota' will act as a single point of contact for us and that it will ensure that all appropriate information is communicated as necessary to the other relevant law enforcement agencies in Colombia. (I will send a copy of this letter to Director General NARANJO TRUJILLO as well.)

Specifically, INTERPOL has been asked to provide expert computer forensic assistance concerning the data stored in three (3) computers and three (3) USB keys that were seized in a narco-trafficking and terrorism operation targeting FARC and one of its key leaders. After having discussed your request within INTERPOL's General Secretariat and with several member countries possessing the necessary computer forensic expertise, I am happy to report that INTERPOL will be able to assist you.

Here is what I propose: INTERPOL will deploy a 5-person team comprising our Acting Assistant Director for purposes of this mission (██████████) as team leader supported by three computer forensic experts (one each from Australia, Korea and Singapore) and an operational assistant from INTERPOL's Command and Coordination Center. If agreement can be quickly reached on what follows, then INTERPOL would do all in its power to have its team identified, assembled and briefed so that it could be in Bogota' early next week. We will need your assistance in ensuring that visas will be promptly provided in order to meet this deadline. All travel, hotel, and per diem expenses would be absorbed by INTERPOL for this initial phase.

./.

The team's mandate will be:

- 1) to determine in precise technical terms what Colombia needs done and to say whether what is being requested is technically possible;
 - 2) if what is requested is technically possible, to advise INTERPOL and Colombia how INTERPOL's team intends to perform these tasks and to give an estimation as to how much time would be required for performing them;
- and
- 3) if both INTERPOL and Colombia agree to what INTERPOL's team proposes, then the team would be authorized to proceed.

It is my hope that the above approach will give both INTERPOL and Colombia the opportunity to ensure that the proper assessment of the situation can be made and to find the most effective way for providing the requested assistance. As always, INTERPOL welcomes any comments or suggestions that you might have as to how INTERPOL could most effectively assist you in this matter.

Since I will be on mission at INTERPOL's Asian Regional Conference in Hong Kong, China until Friday, 7 March 2008, please use INTERPOL's Command and Coordination Center for communicating with me or with INTERPOL relating to this matter.

Yours sincerely,

Ronald K. Noble
Secretary General

cc:

Brigadier General Oscar Adolfo Naranjo Trujillo
Director General de Policía Nacional de Colombia

Mrs María del Pilar Hurtado Afanador
Directora del Departamento Administrativo de Seguridad
Carrera 28 N° 17A – 00 - Piso 9
Bogotá - Colombia

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

Appendix 4: Letter sent to INTERPOL Secretary General from the Director of Colombia's Departamento Administrativo de Seguridad (DAS) dated 6 March 2008

Original version in Spanish and translation in English

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

This page has been intentionally left blank



Departamento Administrativo
de Seguridad D.A.S.

República de Colombia



DIR. 039550

Bogotá, D.C. 06 MAR. 2008

Señor
RONALD K. NOBLE
Secretario General OIPC INTERPOL
Lyon - Francia

Referencia: Solicitud asistencia técnica

Estimado señor Noble:

En atención a su comunicación del 5 de marzo de 2008, de la manera más atenta agradezco la atención prestada a nuestro requerimiento de asistencia técnica enviado a su Despacho el día 4 del presente mes y año.

El marco general del apoyo que requerimos es el siguiente:

1. Establecer el origen y manejo técnico dado a la información obtenida de los procesos de búsqueda de los archivos almacenados en los tres computadores portátiles, tres memorias USB, y dos discos externos, que son objeto de análisis por parte de la Policía Nacional de Colombia y que fueron incautados en desarrollo de una operación dirigida contra un cabecilla de la organización terrorista de las FARC.
2. Validar los hallazgos realizados por funcionarios del laboratorio de Informática Forense de la Dirección de Investigación Criminal de la Policía Nacional de Colombia, relacionados con archivos contenidos en los dispositivos de almacenamiento de información objeto de análisis.

Adicionalmente, en atención a los numerales 2 y 3 de su comunicación, consideramos que el tiempo es de una semana para su realización. En cuanto al modo, el desarrollo de la misión es autónomo y el Gobierno de Colombia se compromete a garantizar las condiciones de acceso y seguridad de la misma.

Finalmente, el Gabinete de Informática Forense de la Dirección de Investigación Criminal de la Policía Nacional de Colombia, será la dependencia en la que se adelantará la mencionada misión.

Cordialmente,

MARÍA DEL PILAR HURTADO AFANADOR
Directora Departamento Administrativo de Seguridad

TRANSLATION OF THE FAX FROM COLOMBIA

Departamento Administrativo de Seguridad

Our ref.: 39550

6 March 2008

Dear Mr Noble,

Further to your correspondence of 5 March 2008, I should like to thank you very much for examining our request for technical assistance which we sent to your office on 4 March 2008.

The general framework of the support we require is as follows:

1. Establish the origin of, and any technical processing applied to, the information obtained during the searches of the files on the three lap-top computers, the three USB keys and two hard-disk drives, which are currently being analysed by the Colombian national police after they were seized during an operation carried out against one of the leaders of the FARC terrorist organization.
2. Validate the findings made by officials of the Colombian criminal investigation department's computer forensics laboratory, in connection with the data contained in the storage devices being analysed.

Furthermore, with reference to paragraphs Nos. 2 and 3 of your letter, we estimate that one week will be required to carry out this work. As far as working methods are concerned, the team will be entirely independent and the Colombian Government undertakes to ensure that the team will be granted the necessary access and security.

Finally, the team will be able to carry out its work in the Colombian criminal investigation department's computer forensics offices.

Yours sincerely,
Maria del Pilar Hurtado Afanador
Director, D.A.S.

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

Appendix 5: *Technical Assistance Agreement* between Colombia and INTERPOL

Original version in Spanish and translation in English

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

This page has been intentionally left blank

**ACUERDO EN MATERIA DE ASISTENCIA TÉCNICA ENTRE LA REPÚBLICA DE
COLOMBIA Y LA SECRETARÍA GENERAL DE LA ORGANIZACIÓN INTERNACIONAL
DE POLICÍA CRIMINAL-INTERPOL**

Considerando que el Director General de la Policía Nacional de la República de Colombia, Brigadier General Óscar Adolfo Naranjo Trujillo, solicitó asistencia técnica de la Organización Internacional de Policía Criminal-INTERPOL en relación con una operación contra el narcotráfico y el terrorismo;

Considerando asimismo que dicha solicitud fue atendida favorablemente según carta de fecha 5 de marzo de 2008 suscrita por el Secretario General de la Organización Internacional de Policía Criminal-INTERPOL;

Teniendo en cuenta la resolución 1373 (2001) del Consejo de Seguridad de las Naciones Unidas, sobre las amenazas a la paz y la seguridad internacionales creadas por actos de terrorismo;

Recordando la cooperación entre el Consejo de Seguridad de las Naciones Unidas y la Organización Internacional de Policía Criminal-INTERPOL en la lucha contra el terrorismo, aprobada por la Asamblea General de INTERPOL en su 74ª reunión, celebrada en Berlín en 2005, mediante la resolución AG-2005-RES-05;

Actuando con arreglo al artículo 26(c) del Estatuto de la Organización Internacional de Policía Criminal-INTERPOL;

La República de Colombia, por una parte, representada por delegación del señor Álvaro Uribe Vélez, Presidente, por el Director General de la Policía Nacional de la República de Colombia y la Directora del Departamento Administrativo de Seguridad y por otra parte la Secretaría General de la Organización Internacional de Policía Criminal-INTERPOL, representada por el Secretario General, han convenido lo siguiente:

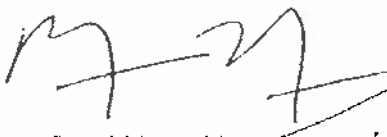
1. La asistencia proporcionada por INTERPOL consiste en los servicios de expertos en materia de investigación informática forense (en adelante denominados los expertos de INTERPOL) a fin de asesorar y prestar asistencia a la República de Colombia.
2. Para tal efecto, los expertos de INTERPOL realizarán las siguientes tareas:
 - a) proporcionar una experticia independiente sobre los datos técnicos almacenados en computadores portátiles, memorias USB, y discos externos que fueron hallados en una operación contra el narcotráfico y el terrorismo;
 - b) prestar cualquier otra forma de asistencia técnica en que puedan convenir la Secretaría General y la República de Colombia.
3. En el desempeño de sus tareas, los expertos de INTERPOL actuarán en estrecha consulta con las personas autorizadas al efecto por la República de Colombia y cumplirán sus instrucciones siempre que estén en consonancia con la asistencia que se debe prestar y con la índole internacional de sus funciones. Los expertos de INTERPOL serán responsables ante la Secretaría General.

4. La República de Colombia se compromete a:
 - a) gestionar, si es necesario, el visado correspondiente para facilitar y agilizar el ingreso, permanencia y desplazamiento en Colombia de los expertos de INTERPOL;
 - b) garantizar a los expertos de INTERPOL durante su permanencia en Colombia los servicios de transporte y de seguridad, tanto de las personas como de las instalaciones;
 - c) brindar el apoyo en materia de equipos, personal y logística que sea necesario para el éxito de la asistencia técnica prestada;
 - d) garantizar que los nombres, fotografías, voces o identidad de los expertos de INTERPOL no sean comunicados a los medios de comunicación.
5. La Secretaría General entregará los resultados de la experticia a la República de Colombia. Dichos resultados y los datos objeto de esta experticia serán propiedad de la República de Colombia.
6. La República de Colombia y la Secretaría General se consultarán entre sí sobre la publicación de tal asistencia técnica en los medios de comunicación.
7. La Secretaría General cubrirá los gastos de viaje, alojamiento, y viáticos que genere la misión de los expertos de INTERPOL durante su permanencia en Colombia.
8. La asistencia técnica prestada por INTERPOL es en beneficio exclusivo de la República de Colombia; en consecuencia, la República de Colombia conviene en asumir la entera responsabilidad de la misma y en mantener indemnes a INTERPOL o sus funcionarios de cualesquiera reclamaciones de terceros o de las obligaciones que resulten de actividades emprendidas en el desempeño de las tareas relativas a la presente asistencia.
9. La Policía Nacional y el Departamento Administrativo de Seguridad de la República de Colombia actuarán como vocero oficial de la República de Colombia ante la Secretaría General.
10. La Secretaría General prestará tal asistencia técnica a la República de Colombia siempre que se disponga de los fondos necesarios.

En fe de lo cual la República de Colombia y la Secretaría General suscriben el presente Acuerdo en dos ejemplares del mismo tenor, que entre en vigor en este día en la ciudad de Bogotá, a los 12 días del mes de marzo del año dos mil ocho.

Por la Secretaría General:

Por la República de Colombia:



Ronald K. Noble
Secretario General



Óscar Adolfo Narángo Trujillo
Director General de la Policía Nacional
de la República de Colombia,



Maria Pilar Hurtado Afandor
Directora del Departamento
Administrativo de Seguridad

AGREEMENT ON TECHNICAL ASSISTANCE BETWEEN THE REPUBLIC OF COLOMBIA AND THE GENERAL SECRETARIAT OF THE INTERNATIONAL CRIMINAL POLICE ORGANIZATION - INTERPOL

Considering that Brigadier General Óscar Adolfo Naranjo Trujillo, Director General of the National Police of the Republic of Colombia, requested technical assistance from the International Criminal Police Organization-INTERPOL in relation to an operation against drug trafficking and terrorism,

Also considering that that request was granted in a letter dated 5 March 2008, signed by the Secretary General of the International Criminal Police Organization-INTERPOL,

Bearing in mind United Nations Security Council Resolution 1373 (2001) on threats to international peace and security caused by terrorist acts,

Recalling the co-operation between the United Nations Security Council and the International Criminal Police Organization-INTERPOL in the fight against terrorism approved in Resolution AG-2005-RES-05 by the INTERPOL General Assembly at its 74th session held in Berlin in 2005,

Acting in accordance with Article 26(c) of the Constitution of the International Criminal Police Organization-INTERPOL,

The Republic of Colombia, represented by its delegation composed of President Álvaro Uribe Vélez, the Director General of the National Police of the Republic of Colombia and the Director of the Administrative Security Department, and the General Secretariat of the International Criminal Police Organization-INTERPOL, represented by its Secretary General, have agreed as follows:

1. The assistance provided by INTERPOL shall consist of the services of experts in forensic computer investigations (hereinafter referred to as INTERPOL experts) to advise and provide assistance to the Republic of Colombia;
2. For this purpose, the INTERPOL experts shall perform the following tasks:
 - (a) provide an independent expert appraisal of the technical data stored in laptop computers, USB keys and external hard drives found during an operation carried out against drug trafficking and terrorism;
 - (b) provide any other form of technical assistance agreed between the General Secretariat and the Republic of Colombia.
3. In performing their tasks, the INTERPOL experts shall act in close consultation with the persons duly authorized by the Republic of Colombia and shall comply with such instructions that are in keeping with the assistance to be provided and with the international nature of their functions. The INTERPOL experts shall be responsible to the General Secretariat;

4. The Republic of Colombia shall undertake to:
 - (a) deal, if necessary, with any visas required to enable the INTERPOL experts to enter, remain and travel in Colombia;
 - (b) ensure transport and security for the INTERPOL experts during their stay in Colombia, both for their personal security and for that of the installations;
 - (c) provide any support in terms of equipment, personnel and logistics that may be necessary for the technical assistance to be successfully provided;
 - (d) guarantee that the names, photographs, voices and/or identities of the INTERPOL experts will not be communicated to the media.
5. The General Secretariat shall provide the Republic of Colombia with the results of the expert appraisal. Those results and the data subject of the appraisal shall be the property of the Republic of Colombia.
6. The Republic of Colombia and the General Secretariat shall consult each other over the publication of such technical assistance in the media.
7. The General Secretariat shall cover the costs of travel, accommodation and expenses generated by the INTERPOL experts' mission for the duration of their stay in Colombia.
8. The technical assistance provided by INTERPOL shall be for the exclusive benefit of the Republic of Colombia; consequently, the Republic of Colombia agrees to assume full responsibility for the assistance and shall hold INTERPOL and its officials harmless in respect of any claims by third parties or liabilities resulting from activities undertaken in the performance of the tasks relating to the assistance provided.
9. The National Police and the Administrative Security Department of the Republic of Colombia shall act as official contacts for the Republic of Colombia vis-à-vis the General Secretariat.
10. The General Secretariat shall provide the technical assistance to the Republic of Colombia provided the necessary funds are available.

In witness hereof the Republic of Colombia and the General Secretariat shall sign the present Agreement in two equally authentic copies which shall enter into force on the twelfth day of March two thousand and eight in the city of Bogota.

For the General Secretariat

For the Republic of Colombia

Ronald K. Noble
Secretary General

Óscar Adolfo Naranjo Trujillo
Director General of the
National Police of the
Republic of Colombia

María Pilar Hutardo Afandor
Director of the Administrative
Security Department

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

Appendix 6: “General Principles,” *Seizure of e-Evidence*, Version 1.01, 15.12.2003, European Union Project from the Programme OISIN II managed by the Directorate-General Justice and Home Affairs in partnership and co-operation with INTERPOL

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

This page has been intentionally left blank

Seizure of e-evidence

Deliverable V1.01 (15.12.2003)

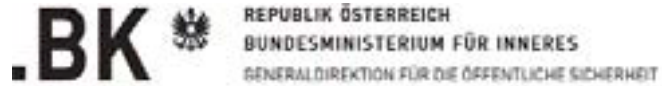
EU Project from the Programme Oisin II
managed by the Directorate-General Justice and Home Affairs

Participating organizations:

A-SIT Secure Information
Technology Center – Austria



Austrian Federal Ministry of the
Interior



National Specialist Law
Enforcement Centre (UK)



Bundesministerium des Innern
vertreten
durch MI / Landeskriminalamt
Niedersachsen (DE)



Landeskriminalamt Niedersachsen

O.I.P.C. – INTERPOL
Sécretariat général



EUROPOL



National Criminal Investigation
Department (SE)



Foreword

Modern criminals utilize and exploit information technology to an enormous extent. The effective seizure of e-evidence plays an important role in combating the challenge of crime.

In order to guarantee the correct forensic handling of e-evidence, it is necessary to issue suitable guidelines and instructions. Such rules not only ensure that evidence is accepted in court, but also reduce the opportunity for claims for damages.

This guide on seizure of e-evidence, which conforms to the relevant EU directives, provides all frontline officers with a valuable aid for preventing and fighting crime.

Preface

This document can be applied to all cases in which e-evidence should be seized.

Each Member State should take its own legal documents and regulations into consideration when interpreting the measures proposed in this document. In addition, each Member State should add its own expert units' contact information.

An organization or agency wishing to apply the recommended procedures should determine the responsibilities for individual steps/actions according to its internal structure.

Table of contents

1	INTRODUCTION	5
2	GENERAL PRINCIPLES	6
2.1	On site witnessing	6
2.2	Data integrity	6
2.3	Audit trail	6
2.4	Expert support	6
2.5	Officer training	7
2.6	Legality and adherence to principles	7
3	REFERENCES	8

1 INTRODUCTION

Information and data of investigative value stored on or transmitted by an electronic device or by digital storage media is referred to as the **electronic evidence** or **e-evidence** or **computer based evidence**. E-evidence is [5]

fragile and can be easily altered, damaged or destroyed and therefore must be handled with great care,

often latent in a similar way as fingerprints or DNA,
easy to be quickly transferred across borders, and
sometimes time-sensitive.

When processed in IT¹ systems, information is no longer “tangible” as it was before IT became widely used. There are two main difficulties that crime investigators and investigation officers are faced with when trying to seize e-evidence [3]:

There are huge amounts of electronic information that can be created, modified, removed and deleted very rapidly.

IT systems appear in a great variety and can consist not only of devices that are easily recognizable as computers, but also of less easily recognizable devices, such as mobile phones, pagers, organisers, faxes, or answering machines. The same applies to the digital storage media that can be not only a floppy disk or a CD, but also a USB pen or a SIM card.

The primary target groups for this Guide are first responders – i.e., the initial responding law enforcement officer and/or other public safety official arriving at the crime scene [5] – and other non-IT experts. It should help them recognize, collect and preserve e-evidence when expert support is not available. The first responders may not always be able to obtain the expert assistance when handling e-evidence. They therefore need to be trained how to correctly seize and preserve e-evidence. The adoption of good practices can minimize the risk of losing or damaging e-evidence due to the lack of expert availability at the crime scene. The purpose of this document is to recommend such good practices in search for, recognition of, collection of, and documentation of e-evidence [1].

¹ Information Technology

2 GENERAL PRINCIPLES

When handling e-evidence, it is crucially important to follow the general principles, i.e., [1-3]:

- on site witnessing,
- data integrity,
- audit trail,
- expert support,
- officer training, and
- legality and adherence to principles.

The principles are explained in the following sections.

2.1 On site witnessing

Principle: *The officer in charge should never attend the scene alone* [2].

At least two officers should be involved in this type of activity. This provides self-protection on the one hand, and helps to catch more details at the scene on the other. The officers should plan and coordinate their actions. If unexpected problems occur, it is easier to solve them because “two heads are better than one”.

2.2 Data integrity

Principle: *No action taken by law enforcement or their officers should change electronic devices or media which may subsequently be relied upon in court* [1].

When handling electronic devices and data, they must not be changed, either in relation to hardware or software. The officer in charge is responsible for the integrity of the material recovered from the scene and thus for commencing a forensic chain of custody [2].

2.3 Audit trail

Principle: *An audit trail or other record of all actions taken when handling electronic evidence should be created and preserved. An independent third party should be able to examine those actions and achieve the same result* [1].

It is imperative to accurately record all activities to enable a third party to reconstruct the first responder’s actions at the scene in order to ensure probative value in court. All activity relating to the seizure, access, storage or transfer of e-evidence must be fully documented, preserved and available for review [4].

2.4 Expert support

Principle: *If it is assumed that electronic evidence may be found in the course of a police operation, the officer in charge should notify experts/external advisers in time* [2].

For investigations involving search and seizure of e-evidence it may be necessary to consult external experts. All external experts should be familiar with the principles laid down in this or similar relevant documents. An expert is supposed to have [1]

- the necessary specialist expertise and experience in the field,
- the necessary investigative and legal knowledge,
- the necessary contextual and legal knowledge, and
- the appropriate communication skills (for both oral and written explanations).

2.5 Officer training

Principle: *The first responders must be appropriately trained to be able to search for and seizure e-evidence if no experts are available at the scene [3].*

In exceptional circumstances where it is necessary that a first responder collects e-evidence and/or access original data held on an electronic device or digital storage media, the first responder must be trained to do it properly and to explain the relevance and implications of his/her actions [1].

2.6 Legality and adherence to principles

Principle: *The officer and agency in charge of the case are responsible for ensuring that the law, the general forensic and procedural principles, and the above listed principles are adhered to. This applies to the possession of and access to electronic evidence [1, 4].*

Each Member State should take its own legal documents and regulations into consideration when interpreting the measures proposed in this document.

One of the internationally important legal documents, the Convention on Cybercrime by the Council of Europe, is currently (as of July 2003) open for signature by the Member States and the states which have participated in its elaboration, and for accession by other states [6].

3 References

[1] Association of Chief Police Officers (United Kingdom), "Good Practice Guide for Computer Based Evidence," V2.0: June 1999, V3.0: August 2003.

[2] Federal Ministry of the Interior (Austria), "Guide for Seizure and Evaluation of Electronic Evidence," (in German), Version 1.0, November 2001.

[3] Police Cooperation Working Party (Council of the European Union), "Information Technology and Good Practice for Search & Seizure," 2001.

[4] International Organization on Computer Evidence, "First responders good practice guide template," *Proc. OCE 2000 Conference*, Rosny sous Bois, France, December 2000.

[5] U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, Technical Working Group for Electronic Crime Scene Investigation, "Electronic Crime Scene Investigation: A Guide for First Responders," July 2001, <http://www.ncjrs.org/pdffiles1/nij/187736.pdf>.

[6] Council of Europe, "Convention on Cybercrime," European Treaty Series No. 185, November 2001, <http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=185&CM=8&DF=11/07/03>.

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

Appendix 7: Message from INTERPOL Secretary General informing all National Central Bureaus of INTERPOL's assistance to Colombia dated 7 March 2008

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

This page has been intentionally left blank

NCB Message

English version

From: IPSTG

Our Ref.: SG/2008/C109/MIS-SG-COL/MPP-CB/mfb

Dear Heads of NCB,

INTERPOL has been requested by NCB Bogota to provide technical computer expertise for the examination of certain laptops, USB keys and hard drives recovered by Colombia in connection with a narco-trafficking and terrorist operation conducted by the Colombian National Police. In light of the sensitive nature of this mission, INTERPOL has exchanged formal letters with Dra. Maria del Pilar Hurtado Afanador, Director of Colombia's Departamento Administrativo de Seguridad (DAS), to whom NCB Bogota reports. These letters make it clear that INTERPOL's requested contribution is technically focused. (Three letters are attached for your information). In order to ensure that INTERPOL provides the best technical support to NCB Bogota, INTERPOL has asked NCB Canberra (Australia) and NCB Singapore to identify computer forensic experts in their law enforcement agencies who would become part of an INTERPOL team that would also include IPSTG's General Counsel, Legal Affairs, and a Specialized Officer from IPSTG's Financial and High Tech Crime Sub-Directorate.

I will lead this team to Colombia to ensure that there is no misunderstanding about the team's tasks and responsibilities; to ensure that the working conditions will permit them to function in an independent atmosphere; and to ensure that any last-minute questions or issues can be efficiently dealt with and resolved.

Not surprisingly, despite our care in drafting a clear and technically focused set of responsibilities for INTERPOL's team, there has been widespread speculation and misreporting in the media about the scope of INTERPOL's work. It is for this reason that I have taken the decision to inform you directly as to what has been agreed to. At this point, I am planning to travel only to Colombia because no other INTERPOL member country has requested a meeting in connection with this matter. If such a request were to be received, I would do all in my power to meet with the requesting countries' authorities.

As you know, Article 3 of INTERPOL's Constitution strictly forbids the Organization from undertaking any intervention or activities of a political, military, religious or racial character. In interpreting Article 3, our General Assembly has made clear that even a matter which begins as a non-political matter can be turned into a predominantly political matter. Therefore, if at any point during INTERPOL's efforts to assist a member country's request for technical assistance the matter takes on a predominantly political character in violation of INTERPOL's Constitution, then I will withdraw INTERPOL's team immediately.

In closing, having served as your Secretary General for over 7 years now and having been unanimously re-elected by the 2005 General Assembly, you can rest assured that I will continue to carry out my duties in full compliance with our Constitution.

Sincerely,

Ronald K. Noble
Secretary General

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

Appendix 8: Letters from the INTERPOL Secretary General to the relevant Colombian, Ecuadorian and Venezuelan officials dated 4 April 2008

Original versions in Spanish and translations in English

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

This page has been intentionally left blank

200, quai Charles de Gaulle
69006 LYON - FRANCE

INTERPOL

The Secretary General
Le Secrétaire Général
El Secretario General
الأمين العام

Ronald K. Noble

Lyon, 4 de abril de 2008

N/Referencia:

SG/2008/C133/COL-CP/RKN-RAA/mfb

Asunto:

Declaración de la neutralidad de INTERPOL en
la investigación de las pruebas extraídas de los
ordenadores intervenidos a las FARC en Colombia

Estimados Sra. Hurtado Afanador y Brigadier General Naranjo Trujillo:

Me permito comunicarle que he tenido el cuidado de aprovechar la ocasión brindada por la 4ª Conferencia Anual de Jefes de OCN de INTERPOL, que se celebra en Lyon (Francia) del 2 al 4 de abril de 2008, para organizar una reunión con los representantes de los tres países interesados por la investigación emprendida tras la operación policial que las autoridades colombianas efectuaron contra las FARC el 1 de marzo de 2008.

Han asistido a la reunión los Sres. Henry Coba Santos, Jefe de la OCN, y Joaquín Fernando Buitrago, Teniente Coronel, Jefe de la Oficina de Asuntos Internacionales, así como los jefes de las delegaciones de Ecuador y Venezuela.

En el encuentro he reiterado la neutralidad de INTERPOL y mi disposición a colaborar por igual con Colombia, Ecuador y Venezuela para reforzar la cooperación policial y prestar toda la ayuda necesaria a las autoridades nacionales competentes. Deseo especialmente insistir en el carácter técnico de la ayuda prestada a las autoridades colombianas para analizar el material decomisado en la operación efectuada contra las FARC.

Se espera que el informe final esté terminado a más tardar a mediados de mayo. Es mi intención presentarlo personalmente a las autoridades colombianas para dar cuenta con toda claridad de su contenido y sus conclusiones.

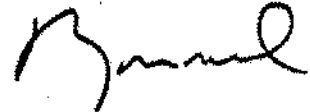
.../...

Asimismo, en la reunión he hecho constar claramente mi convencimiento de que Colombia tiene la intención de hacer público el contenido del informe de INTERPOL. Estoy de acuerdo con que, si procede, el informe sea comunicado al público.

Quedo a su disposición para reunirme con usted si lo considera conveniente o si cree que puede ser útil para facilitar la cooperación policial y la asistencia judicial en una investigación tan delicada.

Le saluda muy atentamente,

Un abrazo



Ronald K. Noble
Secretario General

cc: Sr. D. Henry Cobas Santos
Coronel, Jefe de la OCN de Bogotá

Sra. D^a María del Pilar Hurtado Afanador
Directora del Departamento Administrativo de Seguridad, y
Brigadier General Óscar Adolfo Naranjo Trujillo
Director General de la Policía Nacional de Colombia

4 April 2008

Our Ref.:

SG/2008/C133/COL-CP/RKN-RAA/mfb

Subject:

INTERPOL asserts neutrality in seized
FARC computer evidence investigation in Colombia

Dear Sra. Hurtado Afanador and Brigadier General Naranjo Trujillo,

I would like to inform you that I paid special attention to seize the opportunity presented by INTERPOL's 4th Annual Heads of NCB Conference, held in Lyon, France, from 2 to 4 April 2008, to organize a meeting with the representatives of the three countries concerned by the investigation in relation to the police operation carried out by Colombian authorities against the FARC on 1 March 2008.

The meeting was attended by Sres. Henry Coba Santos, Jefe de la OCN, y Joaquín Fernando Buitrago, Teniente Coronel, Jefe de la Oficina de Asuntos Internacionales, and by the heads of delegation from Ecuador and Venezuela.

During the meeting, I reiterated the neutrality of INTERPOL and my readiness to collaborate with Colombia, Ecuador and Venezuela equally to enhance police co-operation and lend all necessary assistance to the competent national authorities. In particular, I wish to reassert the technical nature of the assistance lent to date to the Colombian authorities for the analysis of the material seized during the operation against the FARC.

The final report is expected to be ready by mid-May at the latest. It is my intention to present it personally to the Colombian authorities in order to clearly illustrate its contents and conclusions.

.../...

I also have made clear to all parties of my belief that Colombia intends to make the contents of INTERPOL's report public. I do support the eventual public release of INTERPOL's report.

I remain at your disposal for any meeting that you might deem appropriate and that could prove helpful to facilitate police co-operation and judicial assistance in such a sensitive investigation.

Yours sincerely,

Ronald K. Noble
Secretary General

cc: Sr. D. Henry Cobas Santos
Coronel, Jefe de la OCN de Bogotá

Sra. D^a María del Pilar Hurtado Afanador
Directora del Departamento Administrativo de Seguridad, y
Brigadier General Óscar Adolfo Naranjo Trujillo
Director General de la Policía Nacional de Colombia

200, quai Charles de Gaulle
69006 LYON - FRANCE

INTERPOL

The Secretary General
Le Secrétaire Général
El Secretario General
الأمين العام

Ronald K. Noble

Lyon, 4 de abril de 2008

N/Referencia:

SG/2008/C134/ECU-CP/RKN-RAA/mfb

Asunto:

Declaración de la neutralidad de INTERPOL en
la investigación de las pruebas extraídas de los
ordenadores intervenidos a las FARC en Colombia

Estimado Sr. Bolivar Cisneros:

Me permito comunicarle que he tenido el cuidado de aprovechar la ocasión brindada por la 4ª Conferencia Anual de Jefes de OCN de INTERPOL, que se celebra en Lyon (Francia) del 2 al 4 de abril de 2008, para organizar una reunión con los representantes de los tres países interesados por la investigación emprendida tras la operación policial que las autoridades colombianas efectuaron contra las FARC el 1 de marzo de 2008.

Han asistido a la reunión el Lcdo. Miguel Oswaldo Cisneros Miranda, Teniente Coronel, Jefe de la OCN de Quito, y los jefes de las delegaciones de Colombia y Venezuela.

En el encuentro he reiterado la neutralidad de INTERPOL y mi disposición a colaborar por igual con Colombia, Ecuador y Venezuela para reforzar la cooperación policial y prestar toda la ayuda necesaria a las autoridades nacionales competentes. Deseo especialmente insistir en el carácter técnico de la ayuda prestada a las autoridades colombianas para analizar el material decomisado en la operación efectuada contra las FARC.


Se espera que el informe final esté terminado a más tardar a mediados de mayo. Es mi intención presentarlo personalmente a las autoridades colombianas para dar cuenta con toda claridad de su contenido y sus conclusiones.

.../...

Asimismo, en la reunión he hecho constar claramente mi convencimiento de que Colombia tiene la intención de hacer público el contenido del informe de INTERPOL. Estoy de acuerdo con que, si procede, el informe sea comunicado al público.

Quedo a su disposición para reunirme con usted si lo considera conveniente o si cree que puede ser útil para facilitar la cooperación policial y la asistencia judicial en una investigación tan delicada.

Le saluda muy atentamente,

Un abrazo,


Ronald K. Noble
Secretario General

cc: Sr. General de Distrito Dr. Juan Sosa Bonano
Director Nacional de la Policía Judicial e Investigaciones
Lcdo. Miguel Oswaldo Cisneros Miranda
Teniente Coronel, Jefe de la OCN de Quito

Sr. General Inspector Lcdo. Bolivar Cisneros
Comandante General de la Policía de Ecuador

4 April 2008

Our Ref.:

SG/2008/C134/ECU-CP/RKN-RAA/mfb

Subject:

INTERPOL asserts neutrality in seized
FARC computer evidence investigation in Colombia

Dear Mr Bolivar Cisneros,

I would like to inform you that I paid special attention to seize the opportunity presented by INTERPOL's 4th Annual Heads of NCB Conference, held in Lyon, France, from 2 to 4 April 2008, to organize a meeting with the representatives of the three countries concerned by the investigation in relation to the police operation carried out by Colombian authorities against the FARC on 1 March 2008.

The meeting was attended by Lcdo. Miguel Oswaldo Cisneros Miranda, Teniente Coronel, Jefe de la OCN INTERPOL Quito, and by the heads of delegation from Colombia and Venezuela.

During the meeting, I reiterated the neutrality of INTERPOL and my readiness to collaborate with Colombia, Ecuador and Venezuela equally to enhance police co-operation and lend all necessary assistance to the competent national authorities. In particular, I wish to reassert the technical nature of the assistance lent to date to the Colombian authorities for the analysis of the material seized during the operation against the FARC.

The final report is expected to be ready by mid-May at the latest. It is my intention to present it personally to the Colombian authorities in order to clearly illustrate its contents and conclusions.

.../...

I also have made clear to all parties of my belief that Colombia intends to make the contents of INTERPOL's report public. I do support the eventual public release of INTERPOL's report.

I remain at your disposal for any meeting that you might deem appropriate and that could prove helpful to facilitate police co-operation and judicial assistance in such a sensitive investigation.

Yours sincerely,

Ronald K. Noble
Secretary General

cc: Sr. General de Distrito Dr. Juan Sosa Bonano
Director Nacional de la Policía Judicial e Investigaciones
Lcdo. Miguel Oswaldo Cisneros Miranda
Teniente Coronel, Jefe de la OCN de Quito

Sr. General Inspector Lcdo. Bolivar Cisneros
Comandante General de la Policía de Ecuador

200, quai Charles de Gaulle
69006 LYON - FRANCE

INTERPOL

The Secretary General
Le Secrétaire Général
El Secretario General
الأمين العام

Ronald K. Noble

Lyon, 4 de abril de 2008

N/Referencia:

SG/2008/C135/VEN-CP/RKN-RAA/mfb

Asunto:

Declaración de la neutralidad de INTERPOL en
la investigación de las pruebas extraídas de los
ordenadores intervenidos a las FARC en Colombia

Estimado Dr. Chávez:

Me permito comunicarle que he tenido el cuidado de aprovechar la ocasión brindada por la 4ª Conferencia Anual de Jefes de OCN de INTERPOL, que se celebra en Lyon (Francia) del 2 al 4 de abril de 2008, para organizar una reunión con los representantes de los tres países interesados por la investigación emprendida tras la operación policial que las autoridades colombianas efectuaron contra las FARC el 1 de marzo de 2008.

Han asistido a la reunión la Sra. D^a María Isabel Jiménez Duran, Abogada, Comisario Jefe, Directora de Policía Internacional, Jefe de la OCN de Caracas, y el Sr. Rodolfo McTurk, Jefe de la División de Investigaciones de la OCN de Caracas, así como los jefes de las delegaciones de Colombia y Ecuador.

En el encuentro he reiterado la neutralidad de INTERPOL y mi disposición a colaborar por igual con Colombia, Ecuador y Venezuela para reforzar la cooperación policial y prestar toda la ayuda necesaria a las autoridades nacionales competentes. Deseo especialmente insistir en el carácter técnico de la ayuda prestada a las autoridades colombianas para analizar el material decomisado en la operación efectuada contra las FARC.


Se espera que el informe final esté terminado a más tardar a mediados de mayo. Es mi intención presentarlo personalmente a las autoridades colombianas para dar cuenta con toda claridad de su contenido y sus conclusiones.

.../...

Asimismo, en la reunión he hecho constar claramente mi convencimiento de que Colombia tiene la intención de hacer público el contenido del informe de INTERPOL. Estoy de acuerdo con que, si procede, el informe sea comunicado al público.

Quedo a su disposición para reunirme con usted si lo considera conveniente o si cree que puede ser útil para facilitar la cooperación policial y la asistencia judicial en una investigación tan delicada.

Le saluda muy atentamente,

Un abogado

Ronald K. Noble
Secretario General

cc: Lic. Ramón Rodríguez Chacín
Ministro del Poder Popular para Relaciones Interiores y Justicia

Sra. D^a María Isabel Jiménez Durand
Abogada, Comisario Jefe, Directora de Policía Internacional,
Jefe de la OCN de Caracas

Dr. Marcos José Chávez
Comisario General
C.I.C.P.C.
Av. Urdaneta Ed. Banco Italo Venezolano-Mesanina
Caracas 1010
Venezuela

4 April 2008

Our Ref.:

SG/2008/C135/VEN-CP/RKN-RAA/mfb

Subject:

INTERPOL asserts neutrality in seized
FARC computer evidence investigation in Colombia

Dear Dr. Chávez,

I would like to inform you that I paid special attention to seize the opportunity presented by INTERPOL's 4th Annual Heads of NCB Conference, held in Lyon, France, from 2 to 4 April 2008, to organize a meeting with the representatives of the three countries concerned by the investigation in relation to the police operation carried out by Colombian authorities against the FARC on 1 March 2008.

The meeting was attended by Sra. D^a María Isabel Jiménez Duran, Abogada, Comisario Jefe, Directora de Policía Internacional, Jefe de la OCN de Caracas, y el Sr. Rodolfo McTurk, Jefe de la División de Investigaciones de la OCN de Caracas and by the heads of delegation from Colombia and Ecuador.

During the meeting, I reiterated the neutrality of INTERPOL and my readiness to collaborate with Colombia, Ecuador and Venezuela equally to enhance police co-operation and lend all necessary assistance to the competent national authorities. In particular, I wish to reassert the technical nature of the assistance lent to date to the Colombian authorities for the analysis of the material seized during the operation against the FARC.

The final report is expected to be ready by mid-May at the latest. It is my intention to present it personally to the Colombian authorities in order to clearly illustrate its contents and conclusions.

.../...

I also have made clear to all parties of my belief that Colombia intends to make the contents of INTERPOL's report public. I do support the eventual public release of INTERPOL's report.

I remain at your disposal for any meeting that you might deem appropriate and that could prove helpful to facilitate police co-operation and judicial assistance in such a sensitive investigation.

Yours sincerely,

Ronald K. Noble
Secretary General

cc: Lic. Ramón Rodríguez Chacín
Ministro del Poder Popular para Relaciones Interiores y Justicia

Sra. D^a María Isabel Jiménez Durand
Abogada, Comisario Jefe, Directora de Policía Internacional,
Jefe de la OCN de Caracas

Dr. Marcos José Chávez
Comisario General
C.I.C.P.C.
Av. Urdaneta Ed. Banco Italo Venezolano-Mesanina
Caracas 1010
Venezuela

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

Appendix 9: Photographs of the FARC camp raided by Colombian authorities on 1 March 2008 and some images retrieved from seized FARC computer exhibits

INTERPOL'S FORENSIC REPORT ON FARC COMPUTERS
AND HARDWARE SEIZED BY COLOMBIA

This page has been intentionally left blank

Photographs of the FARC camp raided by Colombian authorities on 1 March 2008 and some images retrieved from seized FARC computer exhibits



FARC camp raided by Colombian authorities on 1 March 2008



Pictures produced by Colombian authorities of the briefcases holding the seized computers.



Cases recovered from the camp containing two of the laptops.

Some images retrieved from seized FARC computer exhibits



Luis Edgar Devia Silva *alias* Raúl Reyes working on a laptop computer.



FARC insignia



This page has been intentionally left blank