RAPPORT D'EXPERTISE D'INTERPOL SUR LES ORDINATEURS ET LE MATÉRIEL INFORMATIQUE DES FARC SAISIS PAR LA COLOMBIE

MAI 2008

RESUME ET CONCLUSIONS

RAPPORT D'EXPERTISE D'INTERPOL SUR LES ORDINATEURS ET LE MATÉRIEL INFORMATIQUE DES FARC SAISIS PAR LA COLOMBIE

Publié par :
O.I.P.C.-INTERPOL
200, quai Charles de Gaulle
69006 LYON
France

www.interpol.int

TABLE DES MATIÈRES **Page**

Le présent document est une version abrégée du rapport public (original anglais). La numérotation des paragraphes dans la partie « Conclusions » correspond à celle de la version d'origine.

RÉSUMÉ

- Les autorités colombiennes ont demandé à INTERPOL de procéder à une expertise sur trois ordinateurs portables, deux disques durs externes et trois clés USB (ci-après dénommés « les huit pièces à conviction informatiques saisies aux mains des FARC ») saisis dans un camp des Forces armées révolutionnaires de Colombie (FARC) en Équateur, dans la région frontalière avec la Colombie, le 1er mars 2008.
- Ces autorités ont plus spécifiquement sollicité de la part d'INTERPOL qu'il leur apporte une assistance indépendante et technique en matière d'informatique légale en analysant les fichiers utilisateur se trouvant dans les huit pièces à conviction informatiques saisies aux mains des FARC et en déterminant si l'un quelconque des fichiers utilisateur avait été créé, modifié ou supprimé le 1er mars 2008 ou après cette date.
- Cette demande de la Colombie entrait dans le cadre de l'une des fonctions essentielles d'INTERPOL, à savoir apporter un appui opérationnel de police aux pays membres. Parmi les principaux moyens d'apporter cet appui figurent les Cellules de crise INTERPOL (IRT), qui peuvent être déployées en quelques heures lorsque le demande un pays membre devant faire face à : a) une situation de crise, b) des circonstances nécessitant des ressources ou des compétences spécialisées dépassant les capacités de ce pays, ou c) le besoin d'une assistance indépendante dans une enquête internationale.
- Après avoir soigneusement examiné la demande de la Colombie, INTERPOL a proposé d'envoyer immédiatement sur place une Cellule de crise avec pour mission d'établir s'il était possible, sur le plan technique, d'accéder à la demande colombienne, et de prodiguer des conseils sur la façon de mener à bien la tâche en question si elle était jugée réalisable. Le Secrétaire Général d'INTERPOL a conduit en Colombie une délégation composée des membres de la Cellule de crise et du Conseiller juridique de l'Organisation afin de rencontrer les autorités colombiennes en vue de définir les conditions et le champ exact de l'assistance à apporter.
- L'accord d'assistance technique conclu entre INTERPOL et la Colombie énonçait les conditions nécessaires tant à l'indépendance d'INTERPOL qu'à la mise en place d'un cadre juridique rigoureux permettant à INTERPOL d'apporter à la Colombie une assistance policière spécialisée et objective.

- La Cellule de crise envoyée en Colombie a reçu le nom de CompFor (pour ***comp****uter* ***for****ensics* – informatique légale), et comptait deux experts, d'Australie et de Singapour, sélectionnés par leur administration policière nationale. Ces experts ne venaient pas de la région des Amériques et ne parlaient pas l'espagnol, ce qui a aidé à éliminer la possibilité qu'ils soient influencés par le contenu des données à examiner. A présidé à leur tâche l'article 30 du Statut de l'Organisation, qui a pour but de protéger le personnel d'INTERPOL contre les influences extérieures dans l'exercice de leurs fonctions officielles. Toutes ces mesures ont été prises pour préserver leur objectivité au cours de leur travail d'analyse.

- Le champ de l'expertise d'INTERPOL se limitait à : a) établir quelles données contenaient les huit pièces à conviction informatiques saisies aux mains des FARC, b) vérifier si les fichiers utilisateur avaient été modifiés de quelque façon que ce soit le 1er mars 2008 ou après cette date, et c) déterminer si les autorités colombiennes chargées de l'application de la loi avaient traité et examiné les huit pièces à conviction informatiques saisies aux mains des FARC conformément aux principes reconnus au niveau international pour ce qui est du traitement des éléments de preuve électroniques par les services chargés de l'application de la loi.

- La mission confiée à la Cellule de crise et l'assistance ensuite apportée par INTERPOL à l'enquête menée par la Colombie n'incluait pas l'analyse du contenu des documents, dossiers ou autres éléments se trouvant dans les huit pièces à conviction informatiques saisies aux mains des FARC. L'exactitude et la provenance des fichiers utilisateur contenus dans ces huit pièces à conviction sont et ont toujours été exclues du champ de l'expertise réalisée par INTERPOL, qui porte sur les aspects d'informatique légale.

- Au cours de la première phase de l'analyse, qui s'est déroulée à Bogota, les experts ont produit des images physiques des données contenues dans les huit pièces à conviction informatiques saisies aux mains des FARC.

- Au cours de la seconde phase de cette analyse, chacun des experts a examiné quatre des huit pièces à conviction informatiques saisies aux mains des FARC dans le pays où il travaille, en Asie du Sud-Est.

- Les conclusions des experts d'INTERPOL, à l'issue de leur analyse, ont été les suivantes :

  - **Conclusion 1** : Les huit pièces à conviction saisies aux mains des FARC – ordinateurs portables, clés USB et disques durs externes – contiennent en tout 609,6 gigaoctets de données, comprenant des documents, des images et des vidéos.

  - **Conclusion 2** : Toutes les pièces à conviction informatiques saisies aux mains des FARC ont fait l'objet d'accès par les autorités colombiennes entre le 1er mars 2008, date à laquelle elles ont été saisies, et le 10 mars 2008, jour où elles ont été remises aux experts en informatique légale d'INTERPOL.

    - **Conclusion 2a** : L'accès aux données contenues dans les huit pièces à conviction saisies aux mains des FARC par le *Grupo Investigativo de Delitos Informáticos* (Groupe d'enquête sur les infractions informatiques) de la Police judiciaire colombienne entre leur réception, le 3 mars 2008 à 11 h 45, et leur remise aux experts en informatique légale d'INTERPOL, le 10 mars 2008, a été effectué conformément aux principes reconnus au niveau international en matière de traitement des éléments de preuve électroniques par les services chargés de l'application de la loi.

    - **Conclusion 2b** : L'accès aux données contenues dans les huit pièces à conviction informatiques provenant des FARC entre le 1er mars 2008, date à laquelle elles ont été saisies par les autorités colombiennes, et le 3 mars 2008 à 11 h 45, lorsqu'elles ont été remises au *Grupo Investigativo de Delitos Informáticos* de la Police judiciaire colombienne, n'a pas été effectué conformément aux principes reconnus au niveau international en matière de traitement des éléments de preuve électroniques par les services chargés de l'application de la loi.

  - **Conclusion 3** : INTERPOL n'a trouvé aucun élément attestant la création, la modification ou la suppression de fichiers utilisateur sur l'ensemble des huit pièces à conviction informatiques postérieurement à leur saisie aux mains des FARC, le 1er mars 2008, par les autorités colombiennes.

- L'analyse effectuée par INTERPOL a confirmé ce qu'ont eux-mêmes reconnu les services chargés de l'application de la loi colombiens, à savoir que l'accès aux données contenues dans les huit pièces à conviction saisies aux mains des FARC entre le 1er mars, date de leur saisie par les autorités colombiennes, et le 3 mars 2008 à 11 h 45, lorsqu'elles ont été remises au *Grupo Investigativo de Delitos Informáticos* de la Police judiciaire colombienne, n'était pas conforme aux principes reconnus au niveau international en matière de traitement ordinaire des éléments de preuve électroniques par les services chargés de l'application de la loi. En d'autres termes, au lieu de prendre le temps de créer des images des contenus de chacune des huit pièces à conviction saisies en les protégeant contre l'écriture avant d'y accéder, ils ont accédé directement aux données en question.

- En revanche, l'accès aux données contenues dans les huit pièces à conviction saisies aux mains des FARC, effectué le 3 mars 2008 après 11 h 45 par le *Grupo Investigativo de Delitos Informáticos* de la Police judiciaire colombienne, l'a été de manière totalement conforme aux principes reconnus au niveau international en matière de traitement des éléments de preuve électroniques par les services chargés de l'application de la loi. Par exemple, aucune des huit pièces à conviction informatiques en question n'a fait l'objet d'un accès direct de la part de ces experts.

- La vérification par INTERPOL des huit pièces à conviction informatiques saisies aux mains des FARC n'implique ni la validation de l'exactitude des fichiers utilisateur, ni la validation de l'interprétation de quelque pays que ce soit relativement à ces fichiers utilisateur, ni la validation de la source des fichiers utilisateur. Il est bien établi que pour les besoins des services chargés de l'application de la loi, les constatations factuelles sur la vérité ou sur l'exactitude du contenu de tout élément de preuve sont opérées dans le contexte d'une procédure judiciaire de niveau national ou international et/ou par une commission spécialement désignée à cet effet et ayant compétence quant à l'objet du différend.

- Outre le rapport public, INTERPOL a remis aux autorités colombiennes un rapport technique confidentiel, conformément à ce que prévoyait l'accord d'assistance technique. Ce rapport confidentiel contient des copies électroniques de tous les fichiers utilisateur existant sur les huit pièces à conviction informatiques saisies aux mains des FARC. Il contient également une comparaison détaillée des 18 documents remis par la Colombie aux deux experts d'INTERPOL sous la forme d'exemplaires papier ainsi que 41 autres documents remis sous format électronique.

- Enfin, la Cellule de crise CompFor a recensé un certain nombre de problèmes ayant trait à la conduite des expertises d'informatique légale internationales et au traitement des éléments de preuve électroniques par les agents des services chargés de l'application de la loi, en particulier ceux qui prennent les premières mesures sur une scène de crime. Ces problèmes ne concernent pas uniquement la Colombie ; ils concernent tous les fonctionnaires des services chargés de l'application de la loi des 186 pays membres d'INTERPOL. Pour leur apporter une solution efficace, INTERPOL et ses pays membres doivent prendre un certain nombre d'initiatives qui sont présentées et expliquées en détail dans le rapport public complet.

PRINCIPALES CONCLUSIONS PUBLIQUES

Cette partie du rapport contient les conclusions auxquelles est parvenu INTERPOL à l'issue de son travail d'analyse[1]. L'exactitude et la provenance du contenu des données en question n'entrent pas dans le champ de l'expertise réalisée par INTERPOL, qui porte sur les aspects d'informatique légale.

Quantité et types de données trouvées dans les huit pièces à conviction informatiques saisies aux mains des FARC

Conclusion 1 : Les huit pièces à conviction saisies aux mains des FARC – ordinateurs portables, clés USB et disques durs externes – contiennent en tout 609,6 gigaoctets de données, comprenant des documents, des images et des vidéos.

57. Il a été demandé à INTERPOL d'analyser en tout huit pièces à conviction à caractère informatique saisies aux mains des FARC : trois ordinateurs portables, deux disques durs externes et trois clés USB. Chaque pièce s'est vue attribuer un numéro de référence unique par la Colombie[2]. Les trois portables sont référencés sous les numéros 26, 27 et 28. Les deux disques durs externes sont les pièces N^{os} 30 et 31, et les trois clés saisies les N^{os} 32, 33 et 34[3].

58. Toutes les données ont été indexées par les experts en informatique légale d'INTERPOL, afin de leur permettre d'effectuer des recherches par mots-clés pour retrouver les documents susceptibles d'être utiles à l'enquête. Cette tâche a demandé beaucoup de travail et beaucoup de temps. La copie des données par création d'images-disques a pris trois jours, et l'indexation mentionnée une semaine en tout. Cette indexation permettra aussi aux enquêteurs colombiens, par la suite, de retrouver facilement tout fichier utilisateur contenu par les huit pièces saisies, si d'autres documents présentant un intérêt pour les services chargés de l'application de la loi se font jour au cours de leur enquête.

59. En tout, ces huit pièces à conviction contiennent 609,6 gigaoctets de données.

---

[1] La version confidentielle du rapport contient en plus de celle-ci des conclusions qui donnent davantage d'informations sur la comparaison effectuée entre certains documents découverts dans les pièces à conviction. Dans la mesure où ces informations sont confidentielles, la teneur de ces conclusions supplémentaires ne peut être portée à la connaissance du public.

[2] Chaque pièce à conviction a reçu un numéro de référence unique afin de rendre compte de façon précise et complète de la « chaîne de garde » (historique de la conservation des pièces en question).

[3] Il convient de noter que la pièce N° 29 n'a pas été transmise à INTERPOL pour examen dans la mesure où il ne s'agit pas d'un support de stockage de données électroniques et qu'aucune analyse relevant de l'informatique légale n'est donc nécessaire. Ceci explique qu'il manque un chiffre dans la séquence de numérotation des pièces.

60. En termes non techniques, le volume que représentent ces 609,6 gigaoctets correspondrait à 39,5 millions de pages pleines au format Word de Microsoft[4] et, si la totalité des données saisies étaient au format Word, il faudrait plus de mille ans pour prendre connaissance de toutes à raison de 100 pages de lecture par jour.

61. Aux fins du présent rapport, nous avons classé les fichiers découverts à l'intérieur des pièces mentionnées en trois catégories :

1. les fichiers système d'exploitation[5] ;
2. les fichiers application ;
3. les fichiers utilisateur.

62. Les fichiers système d'exploitation sont utilisés par un ordinateur lors des opérations normales comme son démarrage, son fonctionnement et son arrêt. Il est donc fréquent que de tels fichiers soient créés, fassent l'objet d'accès ou soient modifiés à l'insu de l'utilisateur.

63. Les fichiers application sont associés aux logiciels installés sur un ordinateur, en plus du système d'exploitation. Les applications sont notamment les outils de traitement de texte, les lecteurs média et les antivirus. Les programmes antivirus sont particulièrement actifs par nature, afin de garantir que tous les fichiers présents dans l'ordinateur soient exempts de codes malveillants. Les fichiers application sont liés à l'application en question, et l'utilisateur n'a sur eux aucune action directe. Ainsi, lorsqu'un utilisateur ouvre un document existant avec le traitement de texte Word, de Microsoft, une copie de sauvegarde temporaire est créée sur le disque dur.

64. Les fichiers utilisateur sont directement générés par l'utilisateur, qui est responsable des contenus, sur lesquels il a tout contrôle. Comptent au nombre des fichiers utilisateur les documents créés au moyen d'outils de traitement de texte, de tableurs, et les fichiers musique. Ainsi, lorsqu'un utilisateur enregistre un document au moyen de Word, le fichier qui en résulte stocké sur le disque dur ou un autre support est un fichier utilisateur.

---

[4] Le calcul a été effectué à partir des informations trouvées sur le site Web de *Setec Investigations*, « How Many Pages per Gigabyte and Megabyte », *www.Setecinvestigations.com*

[5] Le système d'exploitation installé sur les trois ordinateurs portables qui ont été saisis (pièces N^{os} 26, 27 et 28) était un produit Microsoft.

65. Toujours aux fins du présent rapport, le terme « fichiers système » désigne à la fois les fichiers systèmes d'exploitation et les fichiers application.

66. Les 609,6 gigaoctets de données examinés comportent à la fois des fichiers système et des fichiers utilisateur. La version confidentielle du rapport d'INTERPOL traite de tous les fichiers utilisateur stockés dans les huit pièces à conviction saisies. Il appartient aux seules autorités colombiennes, qui sont souveraines à cet égard, de décider lesquelles de ces données devraient être rendues publiques.

67. Sans révéler la teneur des données, INTERPOL peut indiquer ce qui suit en ce qui concerne la nature des fichiers utilisateur que contiennent les huit équipements informatiques saisis aux mains des FARC :

- 109 fichiers document ont été découverts dans plus d'un des équipements ;
- 452 étaient des feuilles de calcul ;
- 7 989 des adresses e-mail ;
- 10 537 des fichiers multimédia (son et vidéo) ;
- 22 481 des pages web ;
- 37 872 des documents écrits (tels que des documents Word, des fichiers PDF, des documents au format texte) ; et
- 210 888 étaient des images.

Sur ce qui précède, 983 fichiers se sont révélés chiffrés[6].

Vérification de la nature des accès aux huit équipements informatiques appartenant aux FARC entre leur saisie, le 1er mars 2008, et leur remise aux experts en informatique légale d'INTERPOL le 10 mars 2008

68. Étant donné que la Colombie a saisi les huit équipements informatiques aux mains des FARC le 1er mars 2008 et que les médias se sont posé la question de savoir si la Colombie avait altéré ou manipulé les matériels saisis, il a été fait appel à INTERPOL pour déterminer de façon indépendante si des fichiers avaient été créés, avaient fait l'objet d'accès, avaient été modifiés ou supprimés le 1er mars, jour de la saisie, ou après cette date.

[6] Le chiffrement est un moyen utilisé pour rendre des données inintelligibles et les encoder afin d'empêcher quiconque sauf le destinataire prévu de les lire.

69. À chaque fichier à l'intérieur d'un ordinateur ou d'un support de stockage électronique est associé un tampon d'horodatage qui précise la date et l'heure auxquelles il a été créé, a fait l'objet d'un accès pour la dernière fois, a été modifié pour la dernière fois ou a été supprimé. Au moyen d'un logiciel spécial, les experts en informatique légale d'INTERPOL ont extrait les données d'horodatage relatives aux fichiers présents dans chacune des pièces à conviction, en distinguant fichiers système et fichiers utilisateur. Ils ont également vérifié les paramètres de l'horloge système sur chacun des trois ordinateurs portables saisis, étant donné que ces paramètres fournissent les données de départ pour l'horodatage. En ce qui concerne les fichiers présents dans les disques durs externes ou les clés USB, la date et l'heure proviennent généralement de l'horloge système de l'ordinateur auquel ils étaient connectés lors de leur création, des accès dont ils ont fait l'objet, de leur modification ou de leur suppression.

Conclusion 2 : Toutes les pièces à conviction informatiques saisies aux mains des FARC ont fait l'objet d'accès par les autorités colombiennes entre le 1er mars 2008, date à laquelle elles ont été saisies, et le 10 mars 2008, jour où elles ont été remises aux experts en informatique légale d'INTERPOL.

70. INTERPOL expliquera en termes simples les deux principales façons dont il est possible d'accéder aux données contenues dans les ordinateurs portables, les clés USB et les disques durs externes. L'une est conforme aux principes reconnus au niveau international pour ce qui est du traitement des éléments de preuve électroniques par les services chargés de l'application de la loi[7], l'autre n'est pas conforme à ces principes.

[7] Cf. Conclusions 2a et 2b pour une explication des principes reconnus au niveau international en matière de traitement des éléments de preuve électroniques par les services chargés de l'application de la loi.

Conclusion 2a : L'accès aux données contenues dans les huit pièces à conviction saisies aux mains des FARC par le *Grupo Investigativo de Delitos Informáticos* (Groupe d'enquête sur les infractions informatiques) de la Police judiciaire colombienne entre leur réception, le 3 mars 2008 à 11 h 45, et leur remise aux experts en informatique légale d'INTERPOL, le 10 mars 2008, a été effectué conformément aux principes reconnus au niveau international en matière de traitement des éléments de preuve électroniques par les services chargés de l'application de la loi.

71. Le traitement des éléments de preuve électroniques conformément aux principes reconnus au niveau international exige le respect d'une méthodologie rigoureuse. En collaboration avec ses pays membres ainsi qu'avec plusieurs organismes gouvernementaux régionaux et travaillant dans le domaine de l'application de la loi, INTERPOL a défini une série de principes internationaux relatifs au traitement des éléments de preuve électroniques[8]. Ces principes ont été officiellement présentés en 2004 lors de la Conférence INTERPOL sur la cybercriminalité qui s'est tenue au Caire (Égypte). Ils peuvent être consultés par tous les services de police des 186 pays membres de l'Organisation dans la partie sécurisée du site Web d'INTERPOL.

72. La Police nationale colombienne a formé et habilité des experts en informatique légale. Son service d'informatique légale porte le nom de *Grupo Investigativo de Delitos Informáticos* (ci-après dénommés « experts en informatique légale de la Police nationale colombienne ») et fait partie de la *Dirección Judicial de Investigaciones* (Police judiciaire colombienne). Le chef du service d'informatique légale de la Police nationale colombienne a été vice-président du sous-groupe sur la formation du Groupe de travail d'INTERPOL sur la criminalité liée aux technologies de l'information pour l'Amérique latine de janvier 2007 à avril 2008. Il est toujours le représentant permanent de la Colombie au sein de ce groupe de travail.

73. Dans le cadre de l'analyse des huit pièces à conviction informatiques provenant des FARC qu'il a effectuée, INTERPOL a examiné le processus suivi par les experts en informatique légale de la Police nationale colombienne pour traiter les éléments de preuve électroniques saisis le 1er mars 2008. Les experts en informatique légale de la Police nationale colombienne ont pris possession des huit pièces à conviction en question le 3 mars 2008 à 11 h 45 (heure locale de Bogota)[9].

[8] « Seizure of e-evidence », version 1.01 du 15 décembre 2003, projet de l'UE s'inscrivant dans le cadre du Programme OISIN II géré par la Direction générale de la Justice et des Affaires intérieures (INTERPOL a participé en tant que co-auteur et partenaire).

[9] La saisie proprement dite des huit pièces à conviction informatiques a été opérée le samedi 1er mars entre 5 h 50 et 7 h 50 (heure locale du lieu de la saisie, GMT – 5 heures). Ce n'est cependant que plus de 48 heures après que les huit pièces en question ont été remises aux experts en informatique légale de la Police judiciaire colombienne, soit le lundi 3 mars 2008 à 11 h 45 heure locale de Bogota (Colombie) (GMT – 5 heures).

74. Les experts d'INTERPOL ont jugé conformes aux principes reconnus sur le plan international en matière de traitement des éléments de preuve électroniques par les services chargés de l'application de la loi les procédures utilisées par la Police judiciaire colombienne pour enregistrer, photographier et étiqueter chacune des pièces, en créer une copie-image[10] et élaborer tous les documents nécessaires, garantissant ainsi qu'aucune des données contenues dans ces pièces n'a été modifiée, endommagée ou détruite lors du traitement.

75. Les détails techniques précis de toutes les mesures prises par les experts en informatique légale de la Police nationale colombienne pour examiner les huit pièces à conviction informatiques saisies sont expliqués de manière très approfondie par les experts d'INTERPOL dans leur rapport confidentiel. Il ne fait aucun doute que les experts en informatique légale de la Police nationale colombienne se sont conformés au principe fondamental selon lequel, dans des circonstances ordinaires, les services chargés de l'application de la loi ne doivent pas accéder de façon directe au contenu d'éléments de preuve électroniques saisis : ils doivent obtenir une image physique des données qui se trouvent dans le matériel en question en utilisant un système de blocage en écriture, afin d'éviter toute incidence sur les fichiers du système d'exploitation de l'ordinateur et de ne pas se trouver dans l'obligation de procéder à un examen long et approfondi des éléments de preuve électroniques en vue de prouver qu'il n'y a eu ni modification du contenu réel des fichiers utilisateur au moment de l'accès direct, ni conséquence d'aucune sorte.

76. Parce que les experts en informatique légale de la Police nationale colombienne ont traité les huit pièces à conviction informatiques saisies aux mains des FARC conformément aux principes reconnus au niveau international en matière d'informatique légale, aucune donnée n'a été créée, ajoutée, modifiée ou supprimée sur aucune de ces pièces entre le 3 mars 2008 à 11 h 45[11] et le 10 mars 2008, lorsque ces pièces ont été remises aux experts d'INTERPOL afin de créer des images-disques.

[10] La création d'images-disques est le procédé par lequel est effectuée une copie exacte du disque dur d'équipements électroniques ou de supports de stockage numériques.
[11] Heure locale de Bogota (Colombie) (GMT – 5 heures)

Conclusion 2b : L'accès aux données contenues dans les huit pièces à conviction informatiques provenant des FARC entre le 1er mars 2008, date à laquelle elles ont été saisies par les autorités colombiennes, et le 3 mars 2008 à 11 h 45, lorsqu'elles ont été remises au *Grupo Investigativo de Delitos Informáticos* de la Police judiciaire colombienne, n'a pas été effectué conformément aux principes reconnus au niveau international en matière de traitement des éléments de preuve électroniques par les services chargés de l'application de la loi.

77. Lorsque les services chargés de l'application de la loi accèdent directement au contenu d'éléments de preuve électroniques saisis sans avoir créé au préalable une image physique des données, les opérations d'accès et de visualisation laissent des traces. L'accès direct peut compliquer la validation des éléments de preuve en vue de leur utilisation dans le cadre d'une procédure judiciaire : en effet, il incombe ensuite aux services chargés de l'application de la loi de démontrer ou de prouver que l'accès direct en question n'a pas eu d'incidence matérielle sur l'objectif dans lequel on a l'intention d'utiliser l'élément de preuve.

78. Grâce à des outils de police scientifique, les experts en informatique légale des services chargés de l'application de la loi peuvent déterminer les différents types de fichiers système temporaires et permanents qui ont été créés dans l'ordinateur lorsque celui-ci a été allumé ou éteint. Pour des raisons tenant à l'enquête, INTERPOL ne précisera pas quels outils de police scientifique il a utilisé pour parvenir à ce résultat lorsqu'il a analysé les huit pièces à conviction informatiques saisies aux mains des FARC.

79. Les autorités chargées de l'application de la loi colombiennes ont explicitement déclaré aux experts en informatique légale d'INTERPOL qu'un agent de leur unité antiterroriste avait accédé directement au contenu des huit pièces à conviction informatiques saisies aux mains des FARC dans des conditions d'extrême urgence entre le 1er mars 2008, date de la saisie de ces pièces par les autorités colombiennes, et le 3 mars 2008.

80. Comme cela a déjà été mentionné ci-dessus, divers outils de police scientifique permettent aux experts en informatique légale des services chargés de l'application de la loi de reconstituer ce qui s'est produit lorsque des éléments de preuve électroniques ont fait l'objet d'accès directs. C'est précisément ce qu'ont fait les experts d'INTERPOL lors de leur analyse.

81. À la suite de cette analyse, les experts d'INTERPOL ont établi que :

82. Les systèmes d'exploitation des trois ordinateurs portables saisis ont tous révélé que lesdits ordinateurs ont été arrêtés le 3 mars 2008 (à des heures différentes mais tous les trois avant 11 h 45[12], heure de leur réception par les spécialistes en informatique légale de la Police judiciaire colombienne). Les deux disques durs externes et les trois clés USB ont tous été connectés à un ordinateur entre le 1er et le 3 mars 2008, sans création préalable d'une image de leur contenu et sans utilisation de matériel de blocage en écriture.

83. L'examen de la pièce à conviction N° 26 – un ordinateur portable – a révélé les incidences suivantes sur les fichiers le 1er mars 2008 ou après cette date :

- ∉ 273 fichiers système ont été créés ;
- ∉ 373 fichiers système et utilisateur ont fait l'objet d'accès ;
- ∉ 786 fichiers système ont été modifiés ;
- ∉ 488 fichiers système ont été supprimés.

84. L'examen de la pièce à conviction N° 27, un ordinateur portable elle aussi, a révélé les incidences suivantes sur les fichiers le 1er mars 2008 ou après cette date :

- ∉ 589 fichiers système ont été créés ;
- ∉ 640 fichiers système et utilisateur ont fait l'objet d'accès ;
- ∉ 552 fichiers système ont été modifiés ;
- ∉ 259 fichiers système ont été supprimés.

85. L'examen de la pièce à conviction N° 28, un ordinateur portable elle aussi, a révélé les incidences suivantes sur les fichiers le 1er mars 2008 ou après cette date :

- ∉ 1 479 fichiers système ont été créés ;
- ∉ 1 703 fichiers système et utilisateur ont fait l'objet d'accès ;
- ∉ 5 240 fichiers système ont été modifiés ;
- ∉ 103 fichiers système ont été supprimés.

86. L'examen de la pièce à conviction N° 30 – un disque dur externe – a révélé les incidences suivantes sur les fichiers le 1er mars 2008 ou après cette date :

- ∉ 1 632 fichiers système ont été créés ;
- ∉ 11 579 fichiers système et utilisateur ont fait l'objet d'accès ;
- ∉ 532 fichiers système ont été modifiés ;
- ∉ 948 fichiers système ont été supprimés.

[12] Heure locale de Bogota (Colombie) (GMT – 5 heures)

87. L'examen de la pièce à conviction N° 31, également un disque dur externe, a révélé les incidences suivantes sur les fichiers le 1er mars 2008 ou après cette date :

- 3 832 fichiers système ont été créés ;
- 13 366 fichiers système et utilisateur ont fait l'objet d'accès ;
- 2 237 fichiers système ont été modifiés ;
- 1 049 fichiers système ont été supprimés.

88. L'examen de la pièce à conviction N° 32 – une clé USB – a révélé les incidences suivantes sur les fichiers le 1er mars 2008 ou après cette date :

- 8 fichiers système ont été créés ;
- 12 fichiers système et utilisateur ont fait l'objet d'accès ;
- 5 fichiers système ont été modifiés ;
- 6 fichiers système ont été supprimés.

89. L'examen de la pièce à conviction N° 33, également une clé USB, a révélé les incidences suivantes sur les fichiers le 1er mars 2008 ou après cette date :

- 54 fichiers système ont été créés ;
- 168 fichiers système et utilisateur ont fait l'objet d'accès ;
- 28 fichiers système ont été modifiés ;
- 52 fichiers système ont été supprimés.

90. L'examen de la pièce à conviction N° 34, encore une clé USB, a révélé les incidences suivantes sur les fichiers le 1er mars 2008 ou après cette date :

- 1 fichier système a été créé ;
- 60 fichiers système et utilisateur ont fait l'objet d'accès ;
- 1 fichier système a été modifié.

Conclusion 3 : INTERPOL n'a trouvé aucun élément attestant la création, la modification ou la suppression de fichiers utilisateur sur l'ensemble des huit pièces à conviction informatiques postérieurement à leur saisie aux mains des FARC, le 1er mars 2008, par les autorités colombiennes.

91. Comme il a été expliqué ci-dessus, l'accès direct entre le 1er et le 3 mars 2008 aux huit pièces à conviction informatiques saisies aux mains des FARC a laissé des traces dans les fichiers système. Toutefois, les experts d'INTERPOL ont constaté qu'aucun fichier utilisateur n'a été créé, modifié ou supprimé sur l'ensemble des huit pièces à conviction postérieurement à leur saisie, le 1er mars 2008. À l'aide de leurs outils de police scientifique, ils ont découvert un total de 48 055 fichiers dont l'horodatage indiquait qu'ils avaient été créés, ouverts, modifiés ou supprimés par suite de l'accès direct par les autorités colombiennes aux huit pièces à conviction entre le moment de leur saisie, le 1er mars 2008, et le 3 mars 2008 à 11 h 45 du matin.

92. Les experts d'INTERPOL ont également constaté qu'un ordinateur portable (pièce à conviction N° 28) ainsi que les deux disques durs externes qui ont été saisis (pièces à conviction Nos 30 et 31) contenaient des fichiers à l'horodatage erroné (dates dans le futur).

93. La pièce à conviction N° 28 contient :

- ∉ Un fichier dont la date de création est le 17 août 2009.

94. La pièce à conviction N° 30 contient :

- ∉ 668 fichiers dont les dates de création vont du 7 mars 2009 au 26 août 2009 ;
- ∉ 31 fichiers dont les dates de dernière modification vont du 14 juin 2009 au 26 août 2009 ;
- ∉ Ces fichiers contenaient de la musique, de la vidéo ou des images.

95. La pièce à conviction N° 31 contient :

- ∉ 2 110 fichiers dont les dates de création vont du 20 avril 2009 au 27 août 2009 ;
- ∉ 1 434 fichiers dont les dates de dernière modification vont du 5 avril 2009 au 16 octobre 2010.

96. En se fondant sur l'analyse de ces fichiers, les experts d'INTERPOL ont conclu que ceux-ci ont été créés à une date antérieure au 1er mars 2008 sur une ou plusieurs machines dont les paramètres de date et d'heure système étaient incorrects. Les caractéristiques de ces fichiers contenus dans les pièces à conviction Nos 30 et 31 indiquent qu'ils ont soit été créés pendant que les pièces à conviction étaient connectées à une machine dont les paramètres de date et d'heure système étaient incorrects, soit été transférés sur les pièces à conviction 30 et 31 après avoir été créés et que les informations d'horodatage en 2009 ont été transférées avec les fichiers.

97. En ce qui concerne la pièce à conviction N° 28, qui contient un seul fichier dont la date de création est en 2009, les experts d'INTERPOL ont conclu que ledit fichier a été transféré sur la pièce à conviction 28 après avoir été créé et que la date de création (2009) a été transférée avec le fichier.

98. En s'appuyant sur ces éléments, les experts d'INTERPOL ont conclu que les autorités colombiennes ne devraient pas tenir compte de l'horodatage pour les fichiers auxquels sont associées des dates futures dans ces trois pièces à conviction (28, 30 et 31).

99. En tenant compte de l'ensemble des éléments qui précèdent et en s'appuyant sur un examen complet de police technique et scientifique, les experts d'INTERPOL concluent qu'aucun fichier utilisateur n'a été créé, modifié ou supprimé sur l'ensemble des huit pièces à conviction informatiques postérieurement à leur saisie aux mains des FARC, le 1er mars 2008.