CNEJITA
Compagnie Nationale des Experts de Justice en Informatique et Techniques Associées

Journée technique du 11/06/2013

Jean-Arnaud Causse, Toulouse

SMARTPHONE
QUELLES INVESTIGATIONS

INVESTIGATIONS SMARTPHONE

- Les types de Smartphone
- Les données récupérables
- La carte SIM facile
- La carte Micro SD trop facile
- La mémoire interne ça se gâte
- Les deux acteurs majeurs
- Les backups / Le Cloud
- S'isoler du monde
- La PNIJ

LES TYPES DE SMARTPHONE

Le marché s'organise autour de 2 ou 3 OS « *standards* »

mais avec de multiples versions / variantes

(parts de marché France avril 2013)

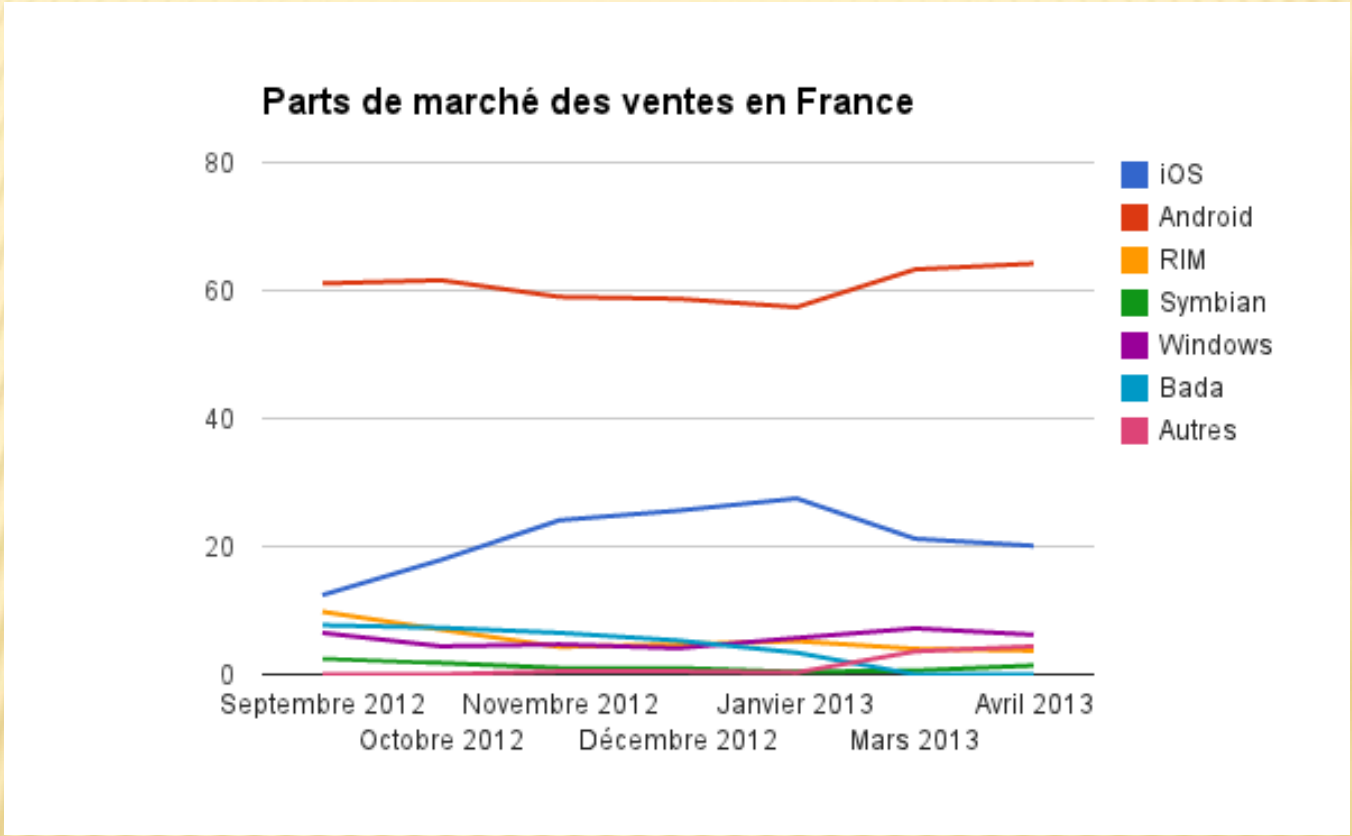
- Google Android 64 %
- Apple iOS 20 %

- Microsoft Windows Phone 6 %
- RIM BlackBerry OS 3,7 %
- Nokia Symbian 1,4 %
- Samsung Bada 0,3 %

- Firefox OS et Tizen *bientôt*

Source : http://www.kantarworldpanel.com

LES TYPES DE SMARTPHONE



Source : http://www.kantarworldpanel.com et http://www.frandroid.com

LES TYPES DE SMARTPHONE

iOS (dérivé de Mac OS X / système APPLE)

- Plusieurs versions
  - v3.x (2009 - 2010) pour iPhone 3G et 3GS
  - v4.x (2010 - 2011) pour iPhone 3GS et 4
  - v5.x (2011 - 2012) pour iPhone 3GS, 4 et 4S
  - v6.x (2012 -2013) pour iPhone 3GS, 4, 4S et 5
- Magasin officiel d'applications : App Store

ANDROID (noyau Linux / open source GOOGLE)

- Plusieurs versions
  - v1.x (2008 - 2010)
  - v2.x (2009 - 2012) beaucoup de téléphones
  - v4.x (2011 - 2013) les modèles les plus évolués et les tablettes
- Magasin officiel d'applications : Google Play
- Plusieurs surcouches développées par les constructeurs
  - HTC / Sony / LG / Samsung

« L'ORDIPHONE »

Contact / Appel / SMS / MMS

Photo, Vidéo, Son

ICCID / IMSI / MCC-MNC-LAC

Email / iMessage / Tchat

Système d'exploitation
Système de fichiers

Document

Application

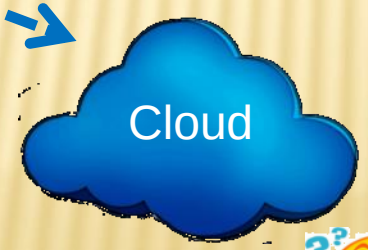
Historique accès Internet

LES DONNÉES RÉCUPÉRABLES

ICCID / IMSI / MCC-MNC-LAC
Contact / Appel / SMS

Photo, Vidéo, Son, Document
Fichiers des Applis : SQLite, Log …

Contact / Appel / SMS / MMS
Email / iMessage / Tchat
Photo, Vidéo, Son, Document
Fichiers de l'OS et des Applis



Sauvegarde de tous çà
et plus encore

LA CARTE SIM

Simple

- Si code PIN, récupérer l'ICCID pour requérir le code PUK
  - Particulier dans le cas des opérateurs virtuels MVNO
- Lecture de la référence de l'abonné : IMSI
- Lecture des Contacts / Liste Appels / SMS
- Lecture des SMS effacés

de moins en moins d'info dans le cas des Smartphones

Matériel / Logiciel

- Logiciels : TULP2G gratuit, MobilEdit, Paraben, XRY, UFED ...
- Rque: Oxygen Forensic ne lit pas les SIM

- Lecteur de carte USB : format SIM ou carte bancaire
- Adaptateur Micro et Nano SIM
- Trombone pour les iPhone

LA CARTE MICRO SD

Très simple

- Penser à la chercher car parfois cachée
- L'extraire pour la cloner avec un lecteur / bloqueur
- L'analyser comme un support amovible
- Récupération des fichiers effacés

généralement de 1 à 2 Go
existe en 64 Go

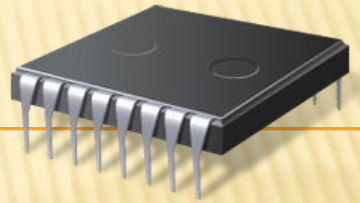
ne perdez pas de temps
à la chercher sur un iPhone !

Matériel / Logiciel

- Logiciels d'analyse : XWays / FTK / Encase ...
  - + Formatage en FAT : PhotoRec, Recuva, GetData ...
- Lecteur de fichier SQLite : SQLite Database Browser / Oxygen SQLite Viewer
- Lecteur de vidéo 3GP : VLC et plein d'autres

- Lecteur de carte avec bloqueur intégré
- Lecteur de carte avec bloqueur USB : Tableau T8R2

LA MÉMOIRE INTERNE (1/2)



jusqu'à 64 Go actuellement

Plus compliqué

- Les protections d'accès (code ou schéma)
- Les protections du constructeur
- La récupération de fichiers / du système de fichiers
  - avec une liaison data (câble, Bluetooth, infrarouge)
  - différents niveaux d'accès: logique / physique / file system
  - Android : rooting v1.6 / v2.3.4 / v3.0 / 4.1.2
  - iOS : recovery mode / jailbreak 

Attention à la méthode

- Récupération des fichiers effacés parfois impossible (iPhone)
- Récupération de données effacées dans les bases (SQLite / cache / ITHMB)

Matériel / Logiciel

- Logiciels spécialisés : XRY / Cellebrite / Oxygen / MobilEdit / Lantern / ElcomSoft / Passware (mot de passe backup)
- Lecteurs de fichier : SQLite / Plist / 3GP …
- Câbles Data / Connexion Bluetooth / Connexion Infrarouge

LA MÉMOIRE INTERNE (2/2)

Le volume des données / Le nombre d'application

- SMS, MMS, iMessage et eMail parfois par dizaine de milliers
- Des milliers d'applications différentes
  - Avec leurs propres données : sqlite, log …
  - Avec des copies de documents: Acrobat Reader / Pages / Evernote / Gmail …
- Pléthore d'applications de partage de fichiers
  - Sur des services commerciaux
  - Sur des NAS personnels
- Pléthore d'applications de communication
  - Facebook, Twitter, Twinkle, Foursquare, Skype
  - Facebook Messenger, WhatsApp, Kik, Touch/PingChat!, Textie, HeyTell
  - Yahoo! Messenger, Yahoo! Mail, Google Mail, Google Maps, Google Calendar

Remarque

- Les logiciels ne récupèrent pas tous → examen manuel du téléphone
- Certaines applications ne démarrent que s'il y a une connexion Internet
- Certains logiciels d'analyse peuvent laisser des traces !

LES DEUX ACTEURS MAJEURS

MICRO SYSTEMATION

Forensic Method	v6.5	Total
XRY Logical	286	3,956
XRY Physical Dumping	211	1,806
XRY Physical Decoding	247	1,615
Security Code Only	78	725
Smartphone Apps	8	118
XRY Untested	62	684
Total	**892**	**8,904**

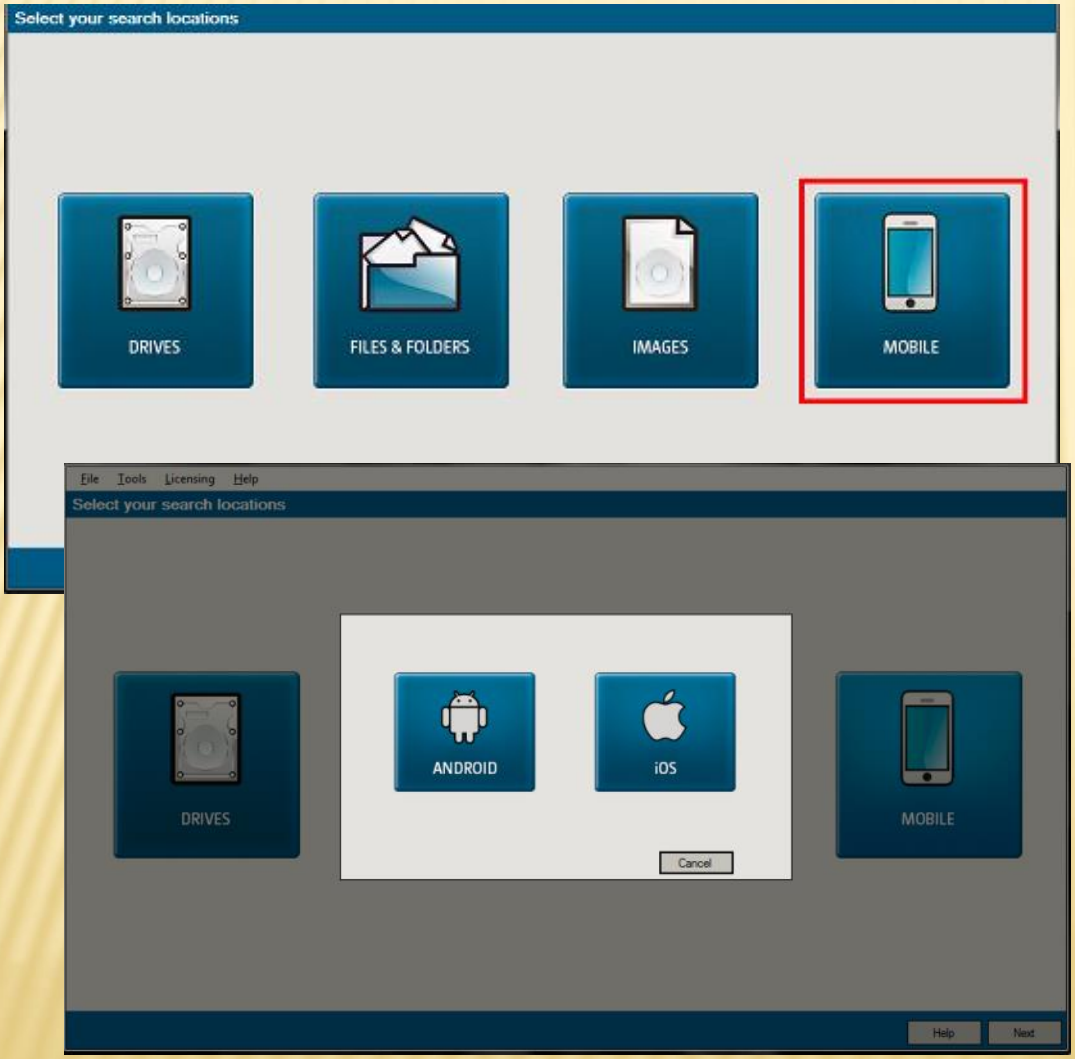
cellebrite
delivering mobile expertise

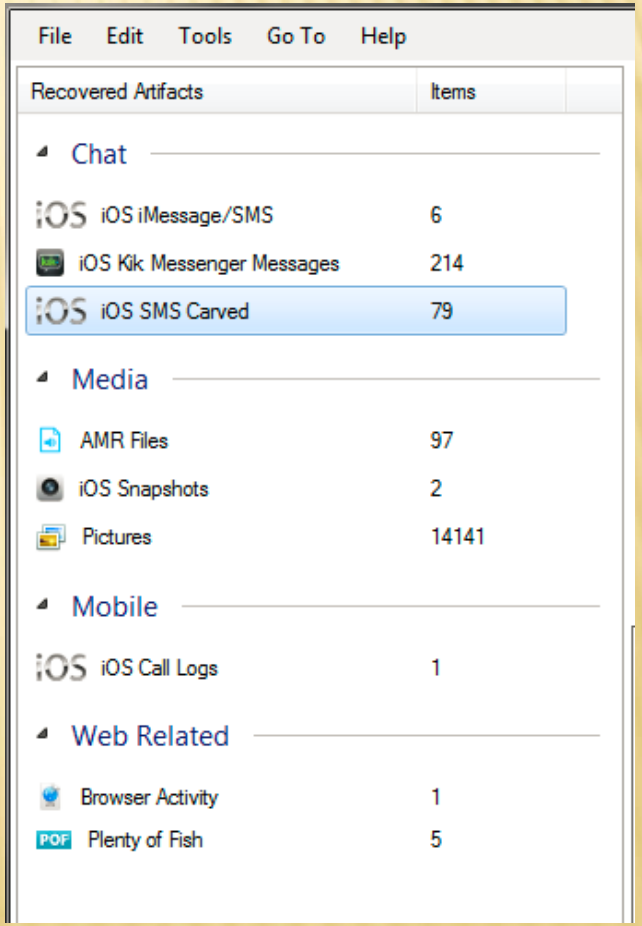
Method	New	Total
Logical Extraction	144	5,064
Physical Extraction*	258	2,580
File System Extraction	207	2,131
Password Extraction	20	1,072
Total	**629**	**10,847**

*including GPS Extraction

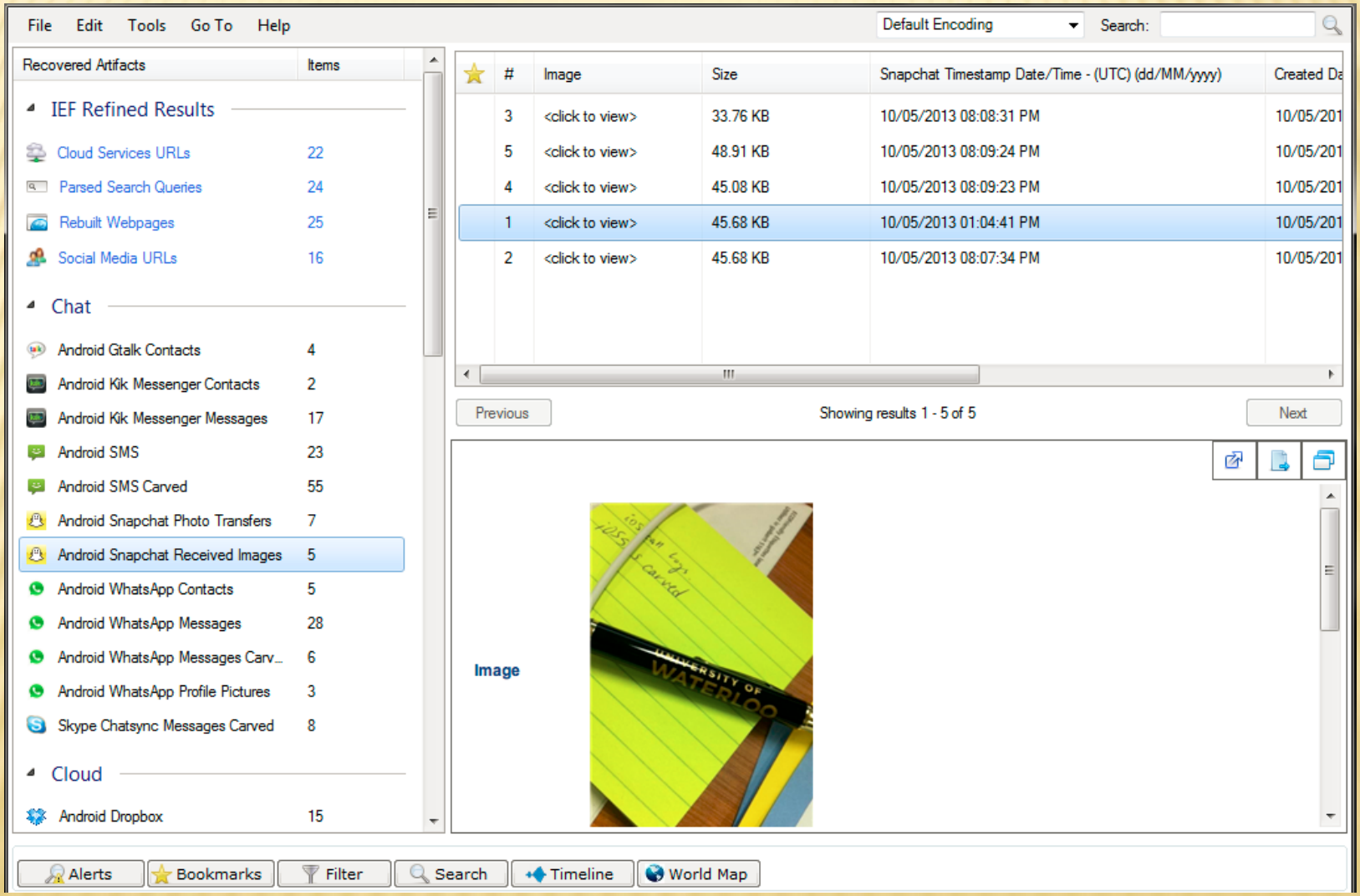
LES MISES À JOURS SONT PRIMORDIALES

IEF S'ATTAQUE AUX SMARTPHONES (1/2)





IEF S'ATTAQUE AUX SMARTPHONES (2/2)



LES BACKUPS / LE CLOUD

Les Backups

Expertise d'un PC → Expertise de plusieurs téléphones

- Souvent les postes informatiques contiennent des backups de téléphone
- De nombreux logiciels permettent d'accéder à ces fichiers
- Les mots de passe peuvent être cassés

Le Cloud : les données accessibles par le Smarphone

- Que faut-il faire ?
- Faut-il le faire ?
- Faut-il le proposer ?

S'ISOLER DU MONDE (1/2)

Un Smartphone en fonctionnement = aspirateur de données

- Réception des Appels, SMS, MMS en attente
- Réception des Emails, iMessage, Alertes, Notifications ….
- Ordre de blocage ou d'effacement
- Mise à jour automatique de la date et de l'heure
- Enregistrement de l'environnement :
  - Borne téléphonique
  - Borne Wifi / Bluetooth
  - Position GPS

Un Smartphone en fonctionnement = fuite de données

- vers l'opérateur
- vers le constructeur (Apple notamment)
- vers le cloud et les applis

Dropbox

iCloud

S'ISOLER DU MONDE (2/2)

Bandes en réception :

- GSM et Edge (921-960 Mhz et 1805-1880 Mhz),
- 3G (2110-2170 MHz), 4G (791-821 MHz et 2620-2690 MHz)
- Bluetooth / Wifi (2400-2500 MHz et 5 GHz)
- GPS (L1 : 1575 MHz, L2 : 1227 Mhz)

- La cage de faraday (800 $)
- Le brouilleur (20 à 200 € et des voisins compréhensifs)
- Le clonage de la SIM (UFED, XRY, MobilEdit)
- Le parking souterrain (6 € et une femme compréhensive)

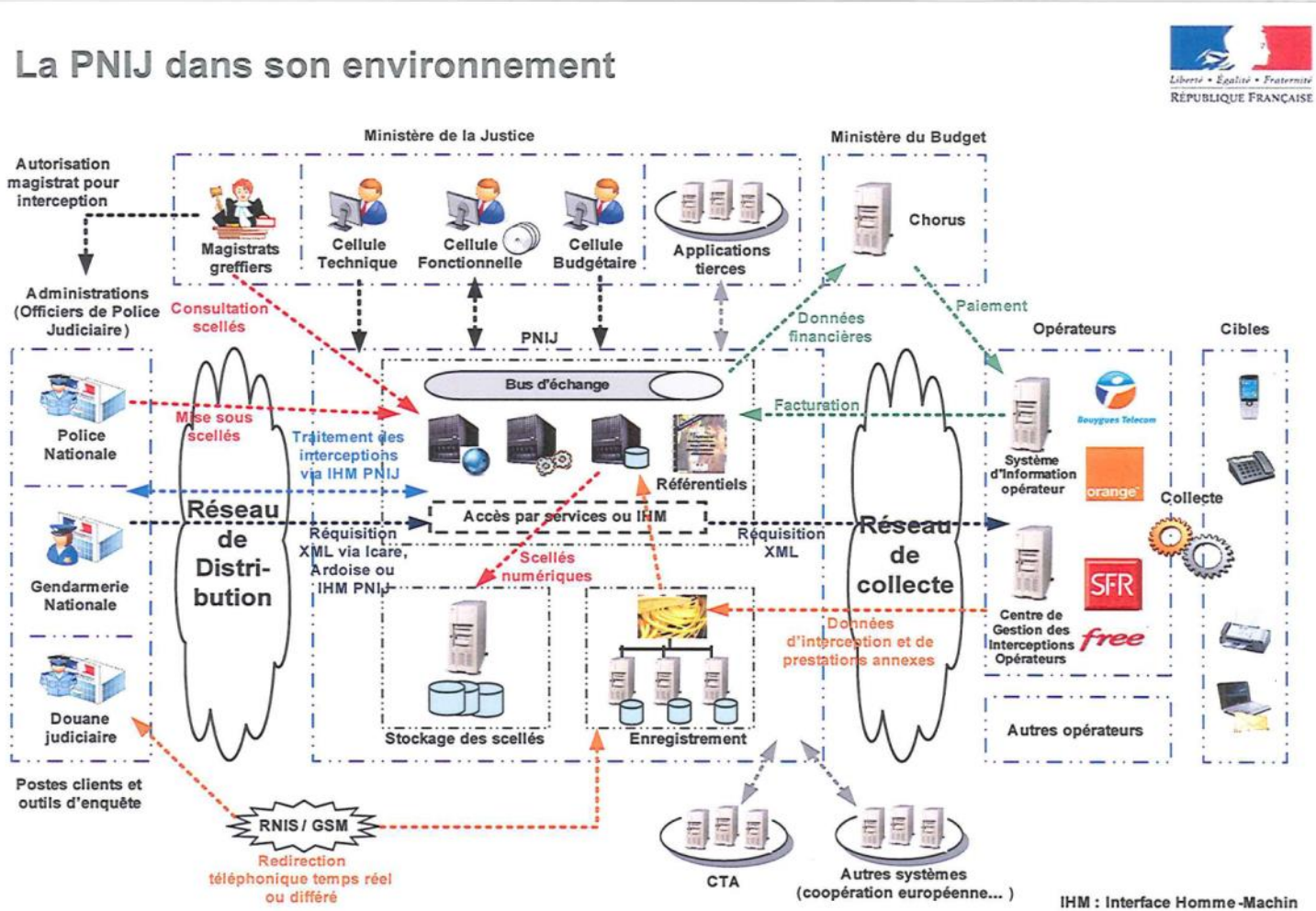
Article L33-3-1 du Code des postes et des communications électroniques
Modifié par Ordonnance n°2011-1012 du 24 août 2011 - art. 40

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Legifrance.gouv.fr
LE SERVICE PUBLIC DE LA DIFFUSION DU DROIT

I. - Sont prohibées l'une quelconque des activités suivantes : l'importation, la publicité, la cession à titre gratuit ou onéreux, la mise en circulation, l'installation, la détention et l'utilisation de tout dispositif destiné à rendre inopérants des appareils de communications électroniques de tous types, tant pour l'émission que pour la réception.

II. - Par dérogation au premier alinéa, ces activités sont autorisées pour les besoins de l'ordre public, de la défense et de la sécurité nationale, **ou du service public de la justice**.

INTERCEPTIONS JUDICIAIRES



CNEJITA
Compagnie Nationale des Experts de Justice en Informatique et Techniques Associées

Journée technique du 11/06/2013

Jean-Arnaud Causse, Toulouse

FIN

SMARTPHONE
QUELLES INVESTIGATIONS