LABOLinx

JEAN-ARNAUD CAUSSE
EXPERT DE JUSTICE

J-T
21 JUIN 2016

CNEJITA EXPERTS

OUTILS D'ANALYSE TÉLÉPHONIE
POINT SUR L'OFFRE

LES MISSIONS AU PÉNAL

5° - de manière générale rechercher tout ce qui pourraient être utile à l'enquête et faire toutes observations utiles à la manifestation de la vérité.

Au civil → *obligation morale de résultats*

« La mission, rien que la mission, toute la mission »

Au pénal → *obligation morale de moyens*

« La mission, toute la mission, plus que la mission »

→ **« M. l'Expert sortez moi tout, car on a rien »**

Au-delà des moyens de premier niveau des enquêteurs
nécessite des outils efficaces d'extraction
Pb mise en forme et transmission des informations
format (vidéo / son) / export / viewer / rapport généré

→ **« M. l'Expert ne sortez que ce qui m'intéresse »**

Au-delà de la seule extraction des données
nécessite des outils efficaces d'analyse
et beaucoup de temps …

LES APPAREILS À ANALYSER (1/2)

du bas de gamme
au Smartphone dernier cri

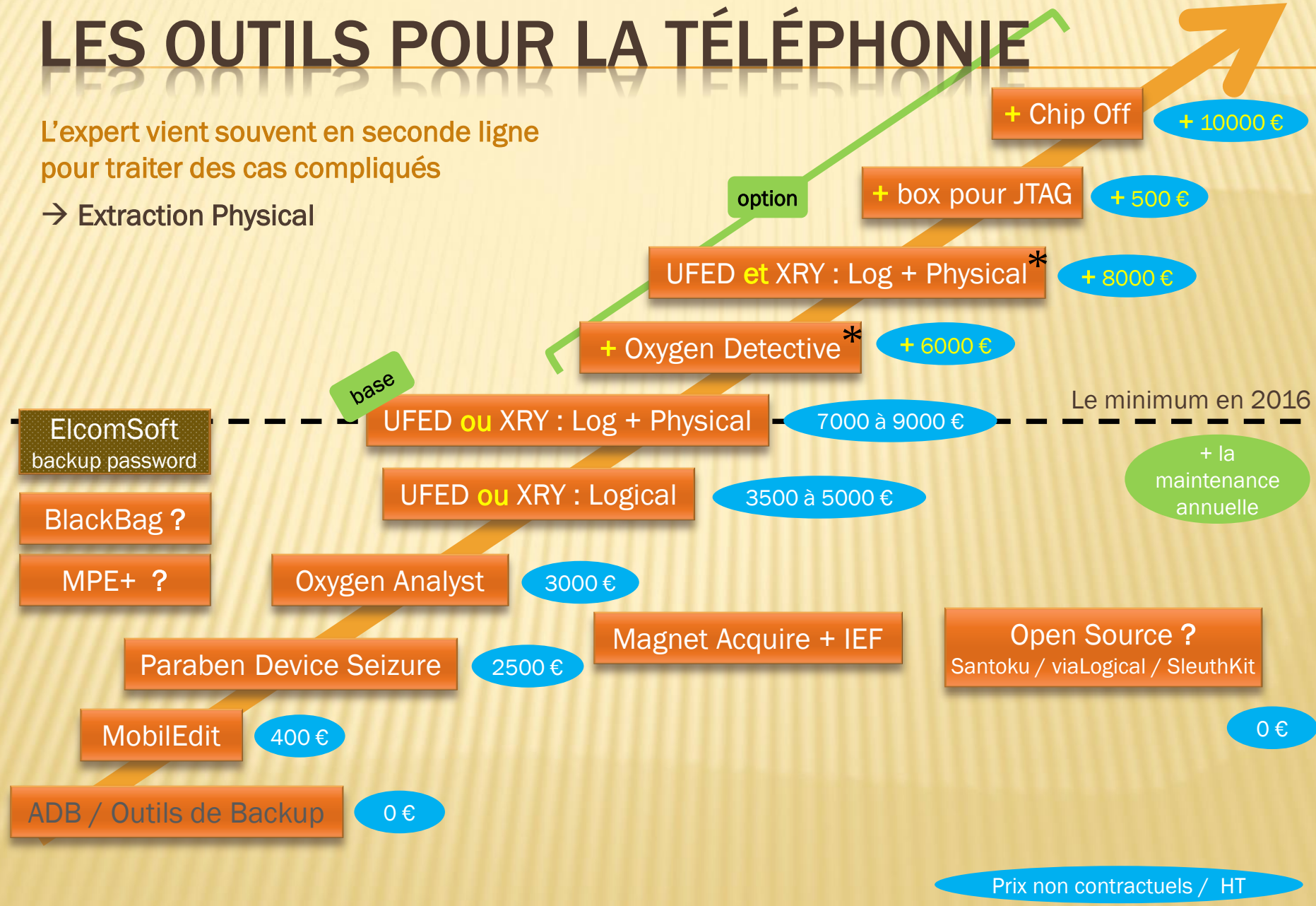
LES APPAREILS À ANALYSER (2/2)

MAIS AUSSI !

LES OUTILS POUR LA TÉLÉPHONIE

L'expert vient souvent en seconde ligne pour traiter des cas compliqués

→ Extraction Physical



LES LEADERS : UFED / XRY

Les plus

- La liste des appareils supportés :
  - Téléphone bas de gamme
  - Smartphone
  - Tablette
  - GPS
- Les extractions *Physical* et le déverrouillage
- La liste des APP supportées
- Les mises à jour presque mensuelles (primordial)
- Le support est très appréciable
- Peut se louer (XRY)

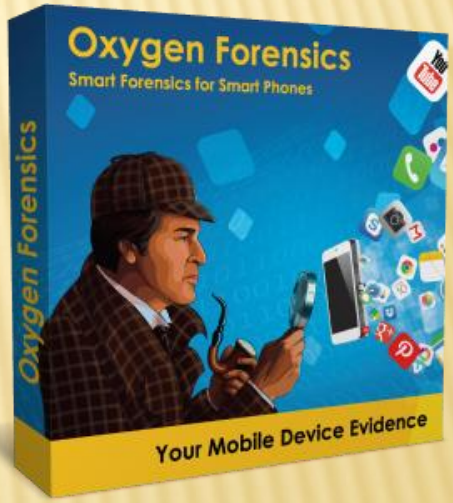
Les moins

- Le prix
- L'achat d'une version *Logical* est à mon avis une erreur pour un expert
- Les IHM sont très en retrait par rapport à Oxygen

UN CHALLENGER : OXYGEN FORENSICS

Les plus

- L'IHM pour analyser les données
- La liste des APP supportées
- La récupération de mot de passe et token
- L'outil d'extraction Cloud
- Les mises à jour presque mensuelles



Les moins

- Presque uniquement pour les Smartphones
- La lenteur des extractions
- L'écriture sur la carte micro-SD
- L'extraction *Physical* sur trop peu de modèles
- Les prix d'achat et de la maintenance s'envolent

UN RETOUR D'EXPÉRIENCE

Les outils sont *malheureusement* complémentaires

- Les deux leaders ont chacun leur famille de téléphones de prédilection
- Les données extraites ne sont pas identiques entre les outils et entre les différents modes d'extraction

  → presque 8 extractions par smartphone

  → fusion des données sans outils du commerce disponibles

La téléphonie représente presque les ¾ de mes missions

- Les outils coûtent très chers à l'achat et en maintenance
- Les téléphones contiennent de plus en plus de données
- Les téléphones sont de plus en plus verrouillés

LABOLinx

JEAN-ARNAUD CAUSSE
EXPERT DE JUSTICE

J-T
21 JUIN 2016

CNEJITA EXPERTS

OUTILS D'ANALYSE TÉLÉPHONIE
POINT SUR L'OFFRE

FIN