LABOLinx

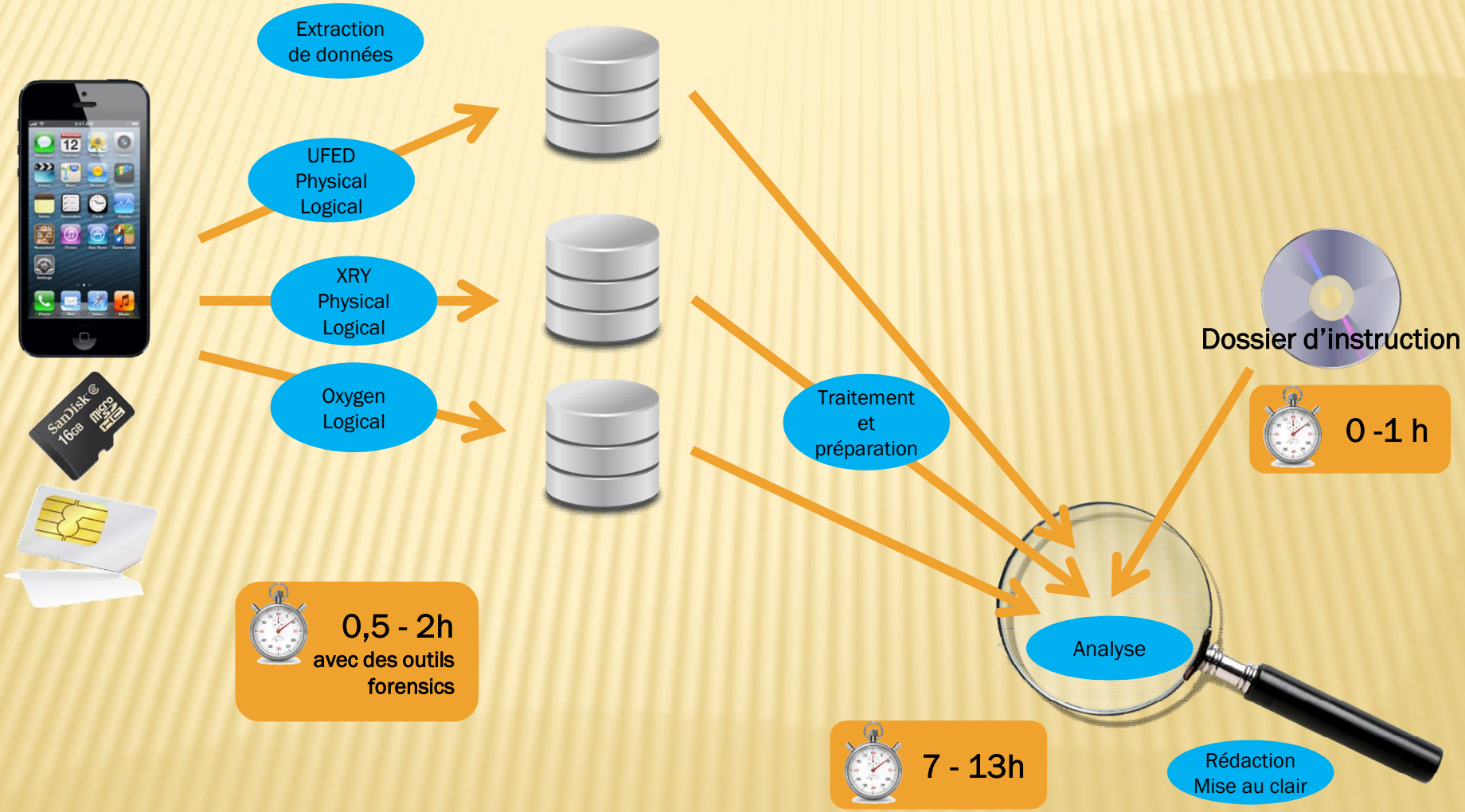
JEAN-ARNAUD CAUSSE
EXPERT DE JUSTICE

J-T
31 JANVIER 2017

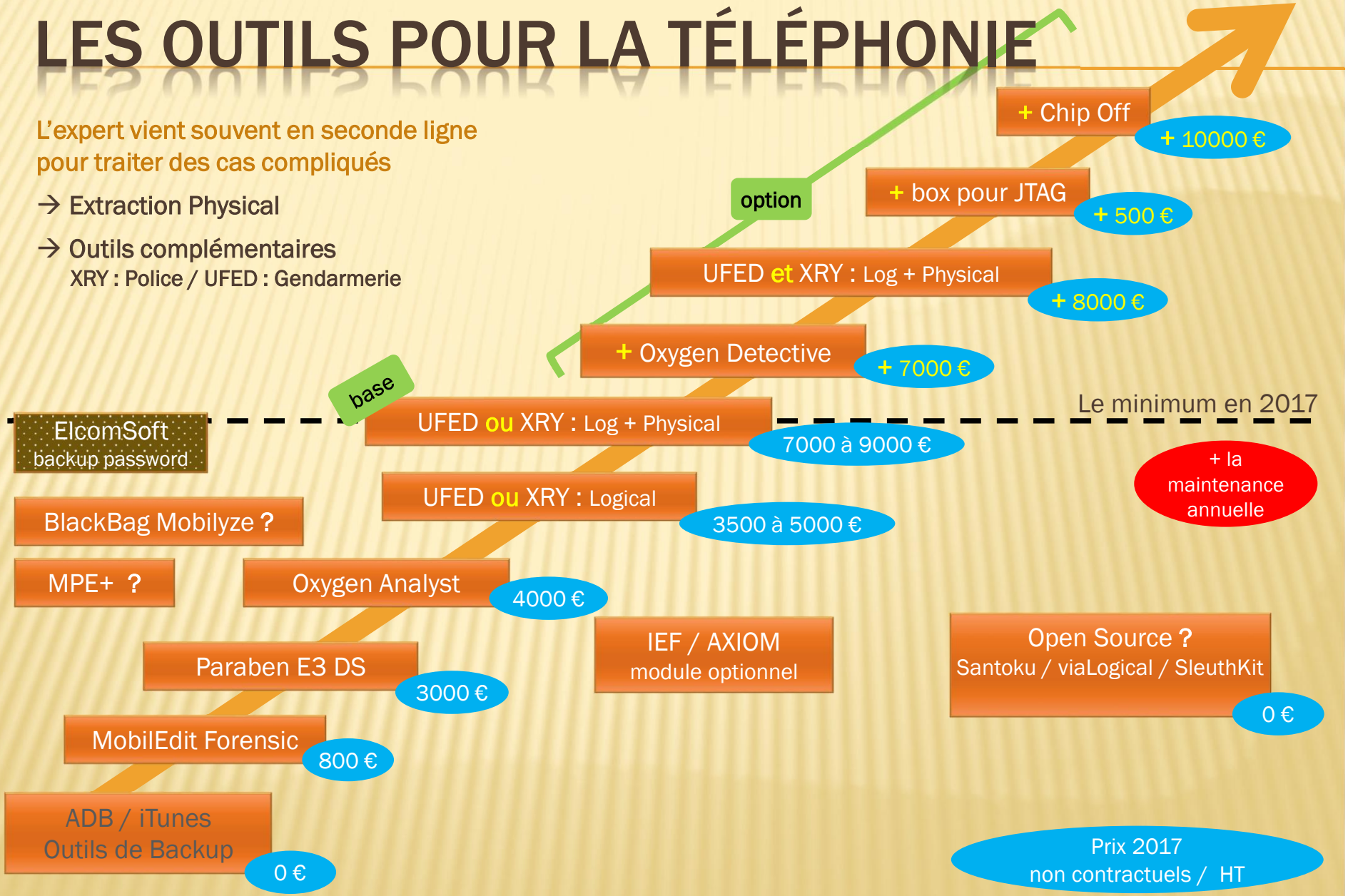
CNEJITA EXPERTS

OUTILS D'ANALYSE TÉLÉPHONE, SMARTPHONE, TABLETTE

UNE ANALYSE STANDARD



LES OUTILS POUR LA TÉLÉPHONIE



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)

Achat
7000 à 9000 €

Maint.
3500 € / an

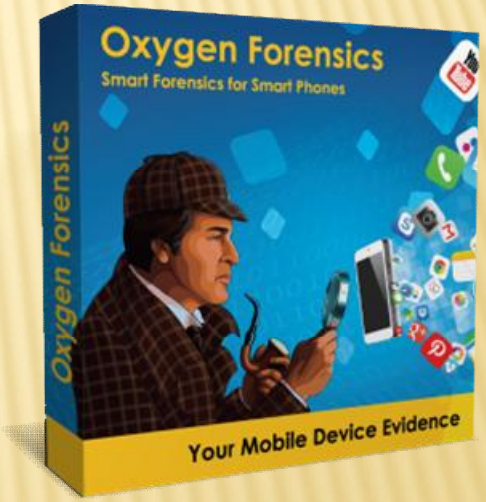
Les moins

- Le prix d'achat et la maintenance
- 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
- Le root intégré mieux que UFED et XRY (→ ré-analyse à chaud)
- L'outil d'extraction Cloud Extractor
- Les mises à jour presque mensuelles
- L'analyse des extractions UFED Physical / Filesys



Les moins

- Presque uniquement pour les Smartphones mais traite maintenant les SIM
- La lenteur des extractions (parfois 12h)
- L'écriture sur la carte micro-SD d'un dossier temporaire
- L'extraction *Physical* sur peu de modèles mais cela s'améliore
- Les prix d'achat et de la maintenance s'envolent !

Achat Analyst
4000 €

Achat Detective
8000 €

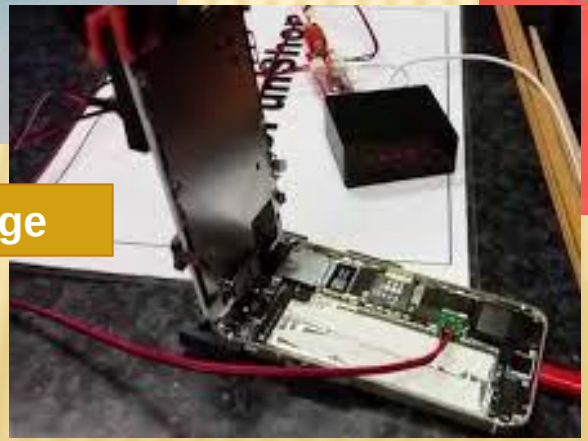
Maint. Detective
2400 € / an

LES BOX

Extraction JTAG

- **Téléphone non supporté**
- **Téléphone détérioré**
- **Téléphone verrouillé**

Méthode non universelle
Risque de destruction du téléphone



Code de verrouillage

Mais aussi:
Analyse en consultant manuellement le téléphone

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
31 JANVIER 2017

CNEJITA EXPERTS

OUTILS D'ANALYSE TÉLÉPHONE, SMARTPHONE, TABLETTE

FIN