LABOLinx

CNEJITA EXPERTS

JEAN-ARNAUD CAUSSE
EXPERT DE JUSTICE

J-T
26 SEPTEMBRE 2017

LE CLOUD AU PÉNAL

LE CLOUD

outils

accès

données disponibles

LES ACCÈS — COMPTE ET MOT DE PASSE

Où les trouver

- **Dans l'OCE ou le dossier d'instruction** → de gros progrès de ce coté
- **Par réquisition**
- **Dans les fichiers de l'utilisateur**
- **Dans les emails**
- **Dans les navigateurs Web** → se connecter au compte local
- **Dans le trousseau d'accès et les Apps** → Apple et Smartphone

Bon à savoir

- **Un mot de passe sert souvent pour plusieurs sites**
- **Booter le poste avec une copie de son HD** → contrôle d'environnement
- **Attention aux notifications de connexion** → avoir la main sur l'email
- **L'ancien smartphone est moins protégé** → ne pas négliger le tél plus utilisé
- **Techniques de hack (social engineering, mot de passe oublié, cookies, …)**

URL FACEBOOK

https://www.facebook.com/ajax/typeahead/search.php?value=florian&viewer=100001946897752&rsp=search&context=search&sid=0.7874068108238346&existing_ids=124653767592695&__user=100001946897752

Profil utilisé pour effectuer la recherche

https://www.facebook.com/profile.php?id=100001946897752

Nom du Profil utilisé sur FACEBOOK

URL FACEBOOK

https://www.facebook.com/confirmemail.php?e=fabiencleuet%40gmail.com&c=69419&ndid=bbb130cG5af546a14e56G0G14dG6b9f94d1&code=69419

Adresse mail utilisé pour ce connecter à FACEBOOK

Dans les historiques des smartphones on peut trouver aussi le n° d'appel du téléphone utilisé pour ce connecter à FACEBOOK Messenger

COOKIES

```
\Users\...\AppData\Roaming\Microsoft\Windows\Cookies\Low\K7LXSXFU.txt
host            = www.wineandco.com/
wac[passwd]     = e4f6532e50d9553ce2c443f722000334
```

Pour un site Web très mal protégé
Mais ce mot de passe m'a permis d'accéder aux autres comptes

LES ACCÈS — JETON D'ACCÈS / TOKEN

Où les trouver

- **Dans le trousseau d'accès et les Apps** → Smartphone / Tablette

oauth2rt_1/vbLe9JnVUifoSqtCQJ3ca0QEPLMDoE6vkUAy1u8VSzY

CAAIcXgMRrWsBAGPtqwskMDXkzyCZCIjE1F3oQS9ZCWZBs4T5e0ZBBMVhQVbZB9hrAQf6cNioP4gSskGXBly7NeLSRaY0GsZBuRP7pTaPZBaaE

Bon à savoir

- **Durée de validité du token :** variable
  certains tant que le mot de passe n'est pas changé
- **Permet de contourner la double authentification** Google Authenticator
- **Un token peut être mono ou multi service**
- **Facebook et Google délivre des tokens pour des sites tiers**
- **IOS : nécessité d'effectuer un backup chiffré pour les récupérer**

LES DONNÉES DISPONIBLES

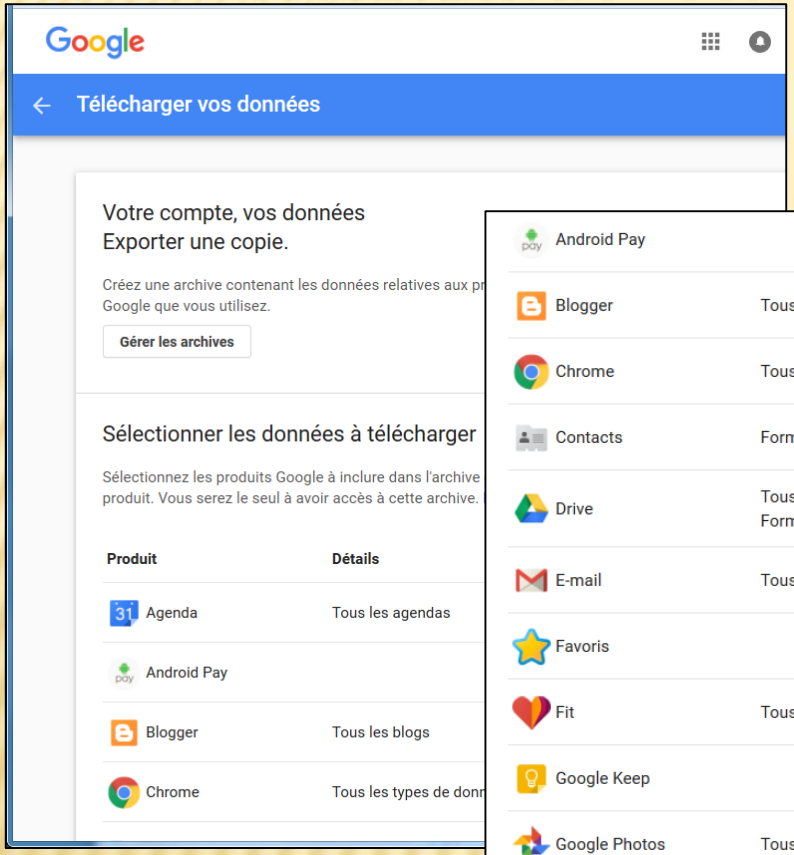
Merci Google, Facebook, Apple !

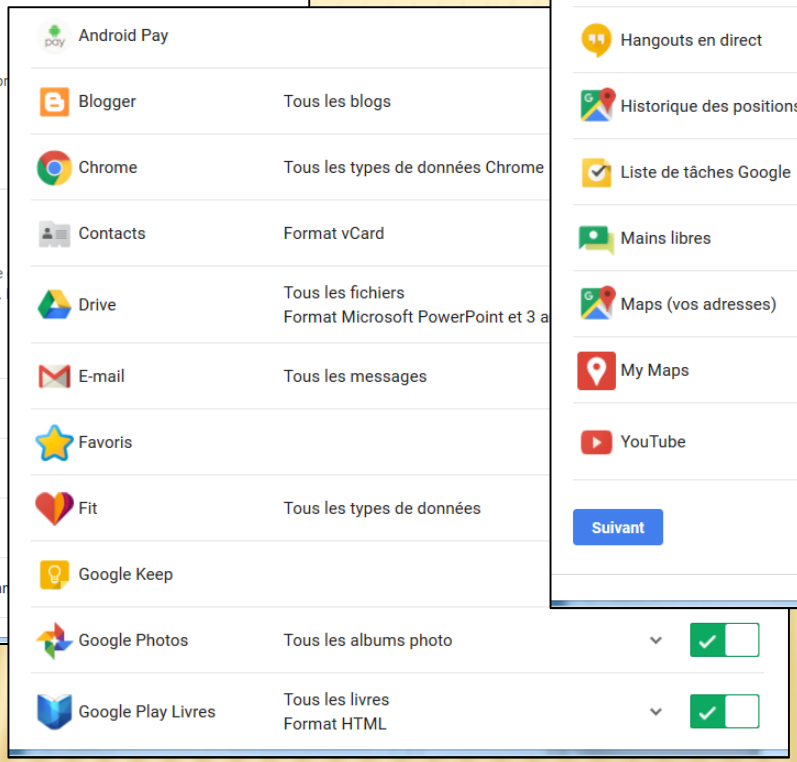
Une mine pour les enquêteurs et l'instruction

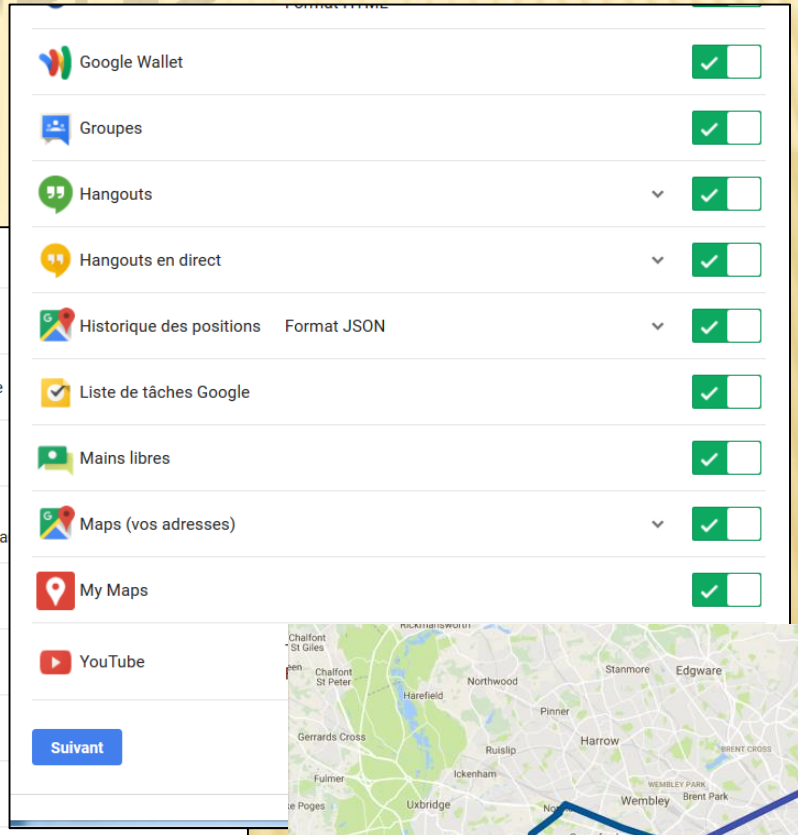
- Contact téléphonique et des réseaux sociaux, Amis
- Appel, SMS, email, conversation des messageries instantanées
- Photo, vidéo, document avec leurs métadonnées
- Agenda, notes
- Activité Internet: historique, signet, recherche effectuée
- Journal de connexions et déconnexions, Adresse IP
- Réseau Wifi
- Mots de passe (pour en télécharger plus …)
- Portefeuille et achat
- Historique des géolocalisations, Adresse cherchée, Itinéraire
- Données de santé
- …

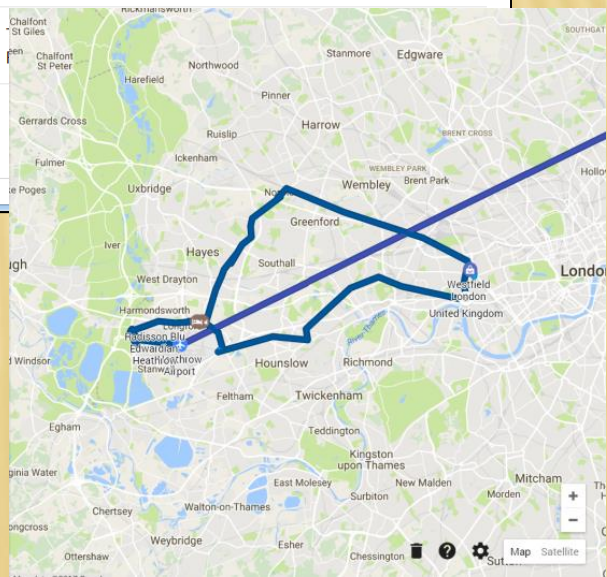
Source multi appareils
Info supprimée sur le téléphone

LES DONNÉES DISPONIBLES









LES DONNÉES DISPONIBLES

Remarques	Articles que vous avez rédigés et publiés sur votre compte.	Historique personnel
Paramètres des notifications	Liste de toutes vos préférences de notification (l'envoi d'un courrier électronique ou SMS était-il activé ou désactivé pour chacune des notifications ?).	Informations téléchargées
Pages que vous administrez	Liste des pages que vous administrez.	Informations téléchargées
Invitations en attente	Demandes d'ajout à la liste d'amis envoyées ou reçues en attente.	Informations téléchargées
Numéros de téléphone	Numéros de téléphone mobile que vous avez ajoutés à votre compte, y compris les numéros vérifiés que vous avez ajoutés pour des raisons de sécurité.	Informations téléchargées
Photos	Photos que vous avez téléchargées sur votre compte.	Informations téléchargées
Métadonnées de photos	Métadonnées transmises avec vos photos téléchargées.	Informations téléchargées
Tokens physiques	Badges que vous avez ajoutés à votre compte.	Informations téléchargées
Pokes	Liste des personnes qui vous ont poké(e) et que vous avez pokées. Les pokes issus de notre application mobile Poke ne sont pas inclus, car ils ne restent disponibles que pendant une période limitée. Une fois que le destinataire les a visualisés, ils sont définitivement supprimés de nos systèmes.	Informations téléchargées
Opinions politiques	Informations ajoutées sous Opinions politiques dans la section À propos de votre journal.	Informations téléchargées
Vos publications	Publications de votre journal (photos, vidéos, mises à jour du statut, etc.).	Historique personnel
	Tout contenu publié sur votre journal par d'autres	Historique personnel

Cartes de crédit	Si vous faites des achats sur Facebook (dans des applications, par exemple) et si vous avez donné votre numéro de carte de crédit.

Comptes liés	Liste des comptes que vous avez associés à votre compte Facebook.
Paramètres régionaux	Langue que vous avez sélectionnée pour Facebook.
Connexions	Adresse IP, date et heure associées aux connexions à votre compte Facebook.
Déconnexions	Adresse IP, date et heure associées aux déconnexions de votre compte Facebook.
Messages	Messages échangés sur Facebook. Veuillez noter que si vous avez supprimé un message, ce dernier ne sera pas inclus dans votre téléchargement puisqu'il a été supprimé de votre compte.

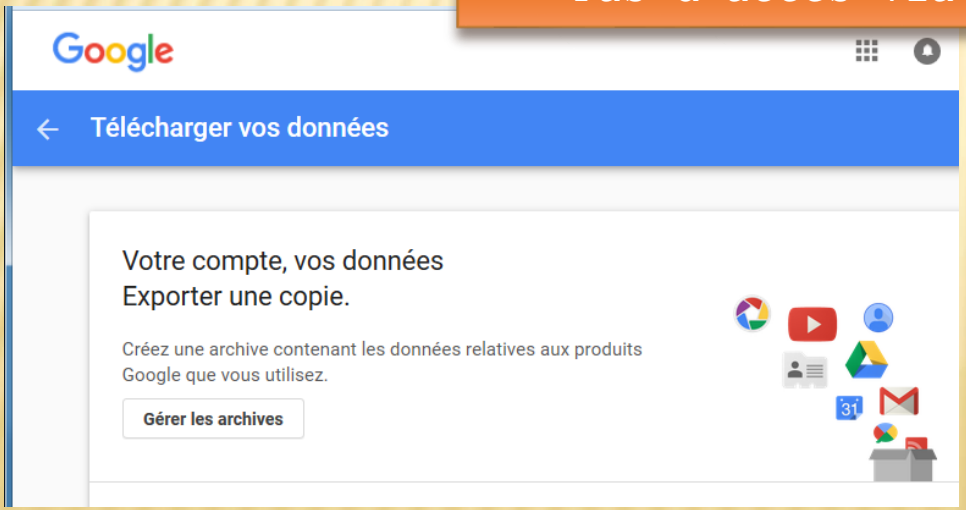
LES OUTILS NON SPÉCIALISÉS

Les outils vus pour les constats

Les fonctions d'archivage

- **FACEBOOK**
- **GOOGLE**
- **ICLOUD**

Données sous des formats divers non intégrées dans les outils d'analyse
Pas d'accès via les tokens



LES OUTILS SPÉCIALISÉS

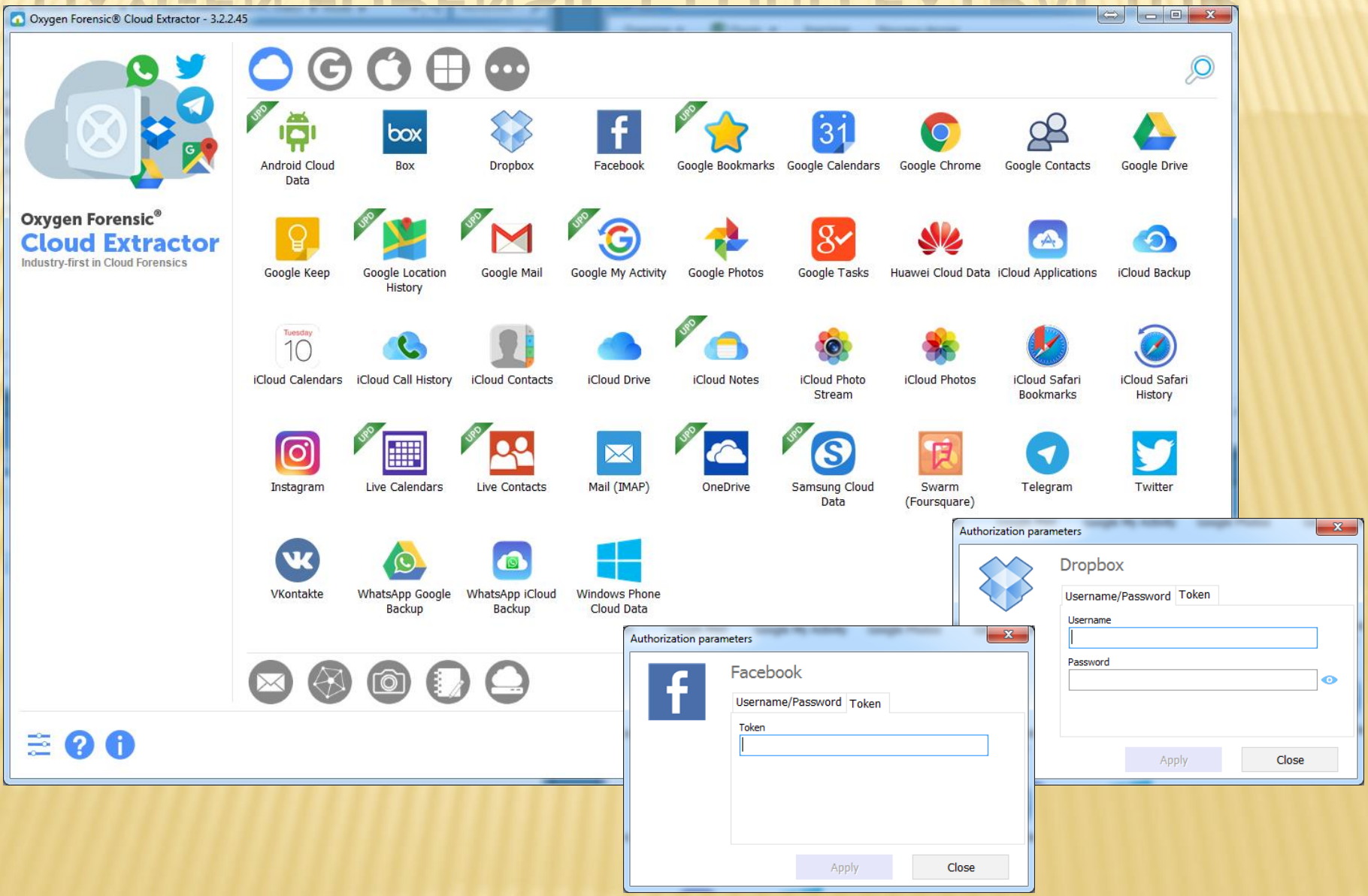
Essentiellement autour des outils dédiés à la téléphonie

- **CELLEBRITE** → UFED Cloud Analyzer — 9000 €
- **OXYGEN** → Cloud Extractor intégré à Oxygen Detective — Suite 7000 €
- **MSAB** → XRY Cloud
- **MAGNET** → Axiom Cloud — bientôt
- **ELCOMSOFT** → Elcomsoft Cloud eXplorer — 2000 €

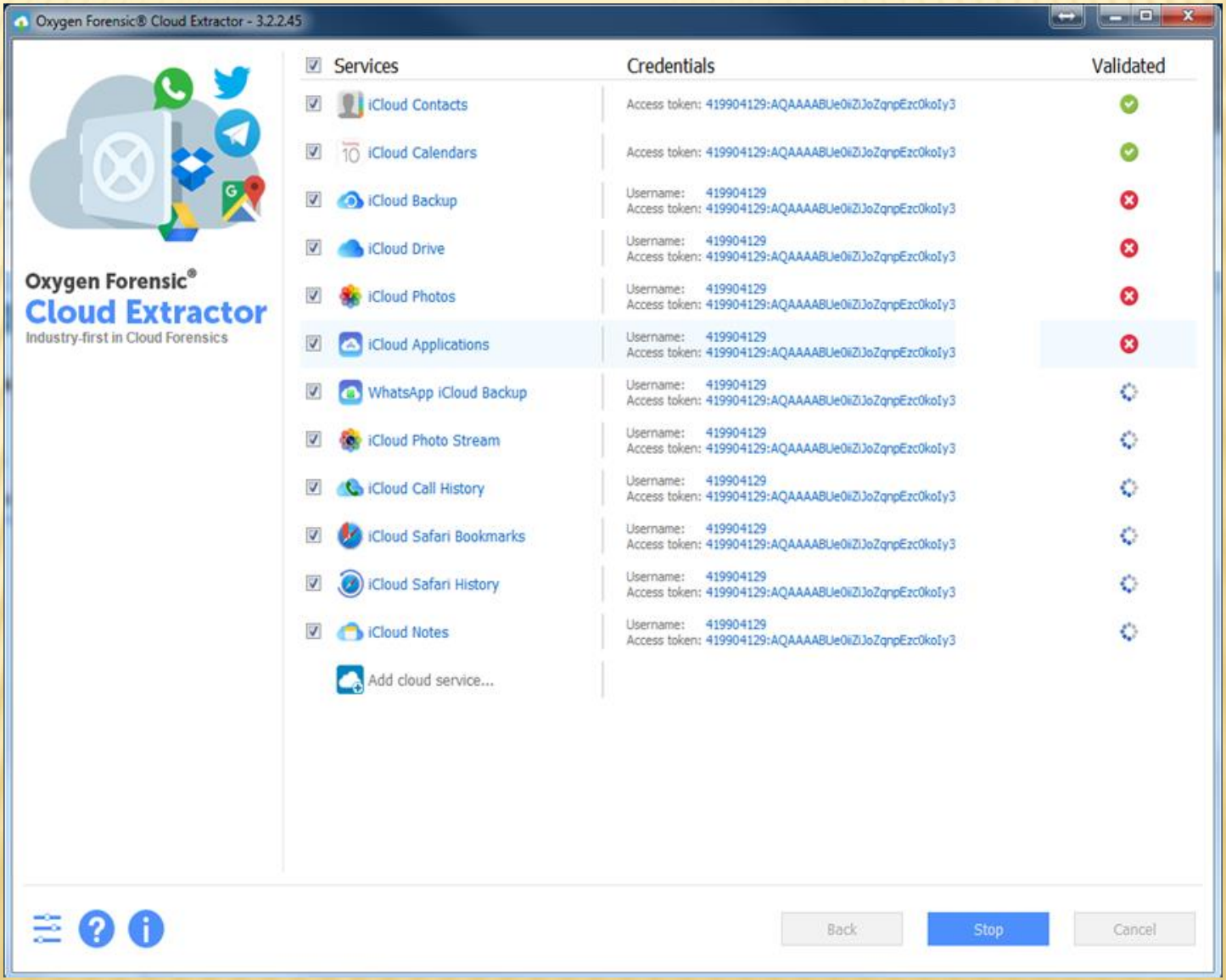
Passerelle entre les extractions de téléphone et l'extraction Cloud

Résultats intégrés dans les outils d'analyse

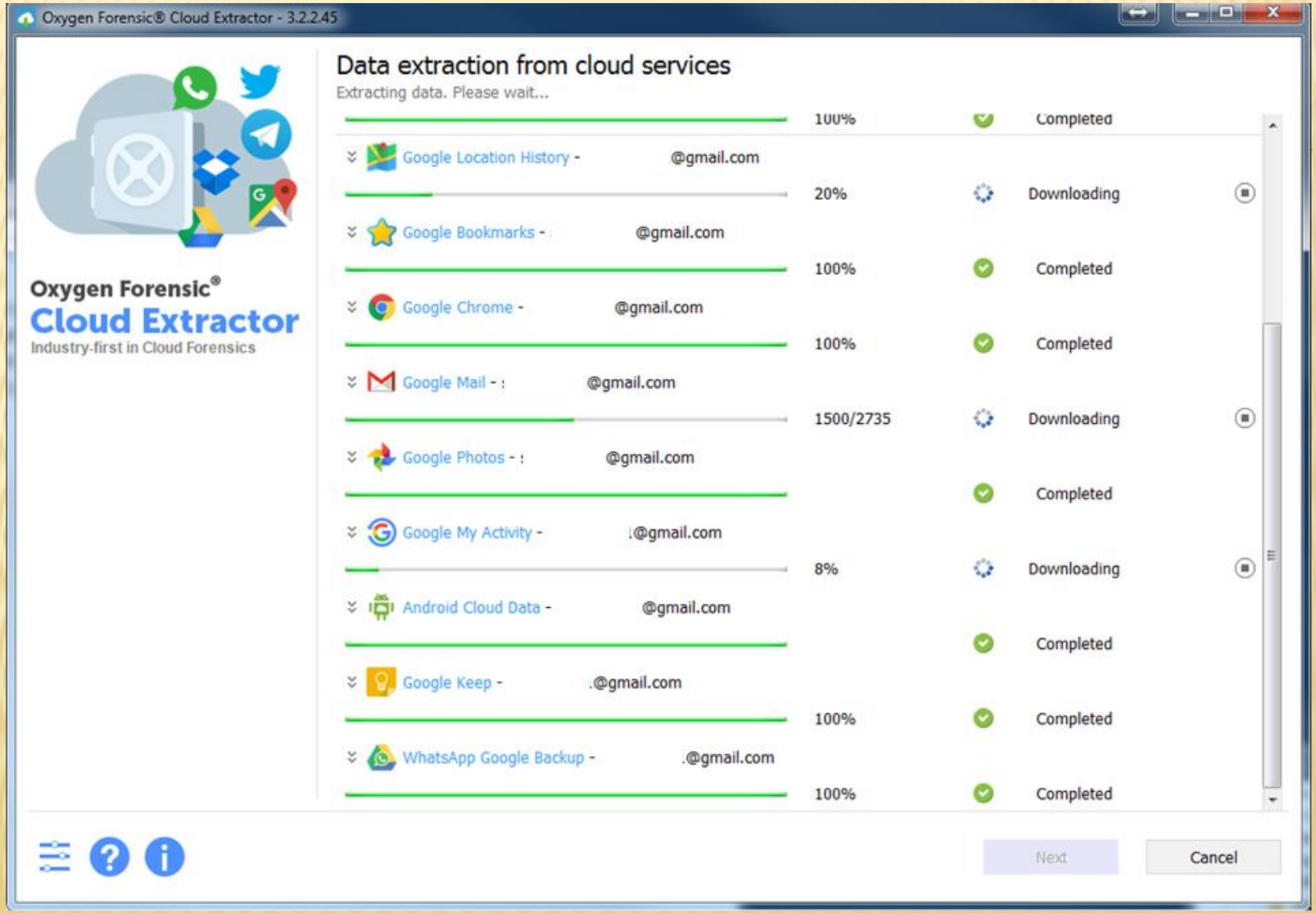
OXYGEN FORENSIC CLOUD EXTRACTOR



OXYGEN FORENSIC CLOUD EXTRACTOR



OXYGEN FORENSIC CLOUD EXTRACTOR



LABOLinx

CNEJITA EXPERTS

JEAN-ARNAUD CAUSSE
EXPERT DE JUSTICE

J-T
26 SEPTEMBRE 2017

LE CLOUD AU PÉNAL

FIN