

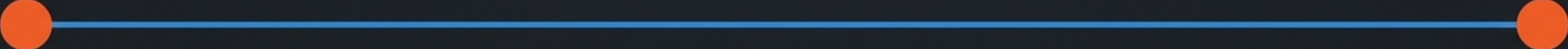
L'empreinte numérique

Masterclass : Traçabilité, OSINT et investigation de scènes de crime numériques.

```
192.168.1.165 -  
102.168.1.165 - [1624-16-27  
00:22:15] - 657 /opt/user/taoto -  
HTTP/1.1 - HTTP/1.1 - 200 OK - 4388;  
202.0.112.45 - [2024-10-27 00:23:22] - SSH  
connection oiva6)12088 - root@oscto-server;  
8a:1b:2a:3d:4e:57 - [2624-18-37 88:24:81] - WL-Pi  
Association - 1320: 'Secoraflet') /var/log/auth.log -  
[2524-18-17 88:25-45] - sudo execution: apt-get instal  
203.0.113.45 - [2024-10-27 08:33:22] - SSH connection  
established - root@ubuntu-server;  
[...]  
[CASE ID: WFS-2024-18-27-A] [CO-51: IP: 203.0.113.45]  
[STATUS: ACTIVE INVESTIGATION] [STATUS: ACTIVE INVESTIGATION]
```

Le message dans une bouteille

Antérieur à l'ARPANET, le courriel gère aujourd'hui 205 milliards de messages par jour. Sa sécurité par défaut est quasi inexistante : non chiffré et trivial à falsifier.

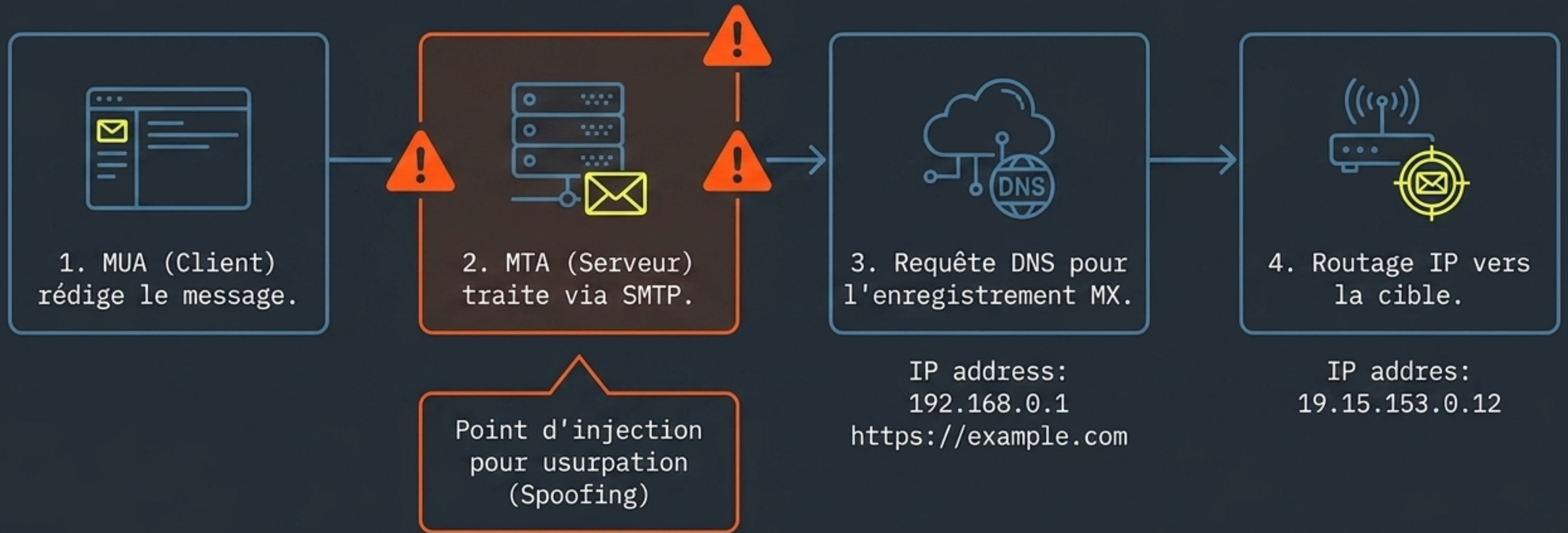


ARPANET
(1969)

Aujourd'hui
(205 milliards/jour)

« Pour analyser un courriel, il est essentiel d'examiner l'intégralité de son en-tête. »

Comment le courriel fonctionne réellement



Dissection d'une falsification (Scène de crime #1)

```
From: myspamhouse@aol.com  
Received: from smtp0422.mail.yahoo.com (80.237.200.67)  
Received: from smtp0422.mail.yahoo.com (80.237.200.67)  
by trademeca.co.kr (211.219.20.86)
```

Anomalie logique : Un utilisateur AOL utiliserait-il une passerelle SMTP Yahoo ? Peu probable.

Règle d'or : Les serveurs ajoutent leur ligne Received en haut.
Les en-têtes falsifiés vont toujours au bas de la chaîne.

Cartographier le mensonge



Trace 1 : smtp0422.mail.yahoo.com
-> Ping : Unknown host (Erreur DNS)

```
tardis1:~ alakhani$ ping smtp0422.mail.yahoo.com  
ping: cannot resolve smtp0422.mail.yahoo.com: Unknown host
```

Trace 2 : IP déclarée 80.237.200.67
-> Localisée en Allemagne
(Faux serveur Yahoo)

IP Address	Country	Region	City	ISP	Organization
80.237.200.67	Germany	Nordrhein-Westfalen	Koeln	Host Europe GmbH	Not Available

Trace 3 : 211.219.20.86
-> IP réelle localisée à Séoul,
Corée du Sud

IP Address	Country	Region	City	ISP	Organization
211.219.20.86	Korea, Republic of	Seoul-teukbyeolsi	Seoul	KT Corporation	Not Available

Interroger la cible (Sans se faire démasquer)

Règle tactique :

Règle tactique :

Ne jamais se connecter directement à l'IP suspecte (risque de honeypot ou d'enregistrement d'IP).

Solution :

Utiliser un proxy externe pour tester le port 25 (SMTP).

Étude de cas : L'employé harcelé

Les en-têtes semblaient internes, mais trahissaient l'usage de webmails et d'un VPN.

Le coupable : un ex-mari jaloux usurpant une identité.

Outils d'attaque fréquents :

- Serveurs d'envoi massif
- Relais SMTP ouverts (TOR/VPN)
- SimpleEmailSpoofers

	Test	Result
✗	SMTP Connect	Failed To Connect

Session Transcript:

```
Connecting to 211.219.20.86<br /> 9/22/2017 3:02:58 PM
Connection attempt #1 - Unable to connect after 15 seconds.
[15.05 sec]<br /> <br />PWS3v2 15049ms<br />
```

Le changement de paradigme : Du courriel à l'OSINT

Vecteur	Structure	Temporalité	Vulnérabilité
Courriel	Données structurées (en-têtes)	Asynchrone	Facile à falsifier techniquement
Réseaux Sociaux	Données comportementales (lieux, photos)	Synchrone	Traces permanentes, difficiles à effacer



Avertissement éthique : L'investigation sociale requiert une autorisation. Ne menez aucune enquête illégale ou contraire à l'éthique.

L'écosystème des registres publics



Niveau 1 : Zabasearch. Gratuit. Dossiers judiciaires, registres fonciers. Sujet aux erreurs.

Niveau 2 : BeenVerified. Premium. Centralise les documents publics pour un profil unifié.

Niveau 3 : Pipl. Moteur de corrélation. Croise réseaux sociaux, blogs et identifiants génériques.

Cas pratique :
Relier le pseudonyme 'OneNicePerson' d'un forum à un compte eBay vendant du matériel d'entreprise volé.

L'entonnoir de la vérité : Pixels et Localisation

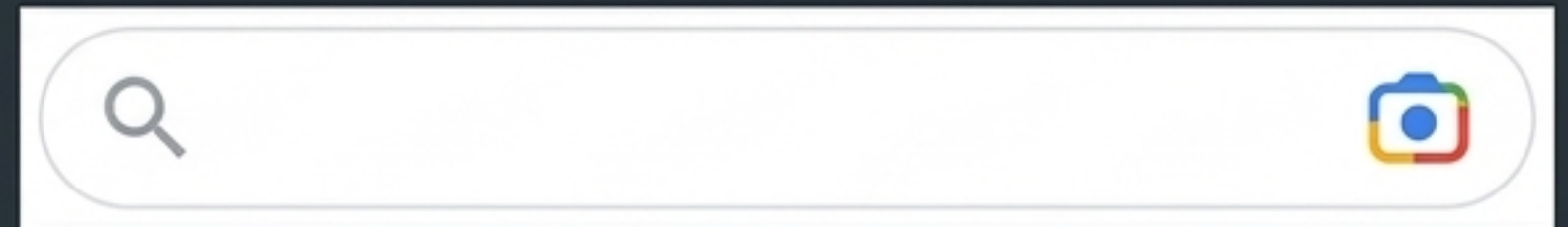
Où ? (Analyse Spatiale)

Outil : Geofeedia. Analyse en temps réel des publications géolocalisées.



Qui ? (Recherche Inversée)

Outil : Google Images. Détecter les faux profils et usurpations.



- L'anecdote : L'avatar de Dr. Chaos utilisé par de multiples profils.
- Preuve de concept : Résolution instantanée de l'énigme mathématique McDonald's.

Le pivot du pseudonyme

Principe comportemental : L'humain est une créature d'habitudes. Un pseudonyme utilisé sur une plateforme est presque toujours réutilisé ailleurs.

KnowEm



Recherche instantanée sur plus de 500 réseaux et 150 domaines.

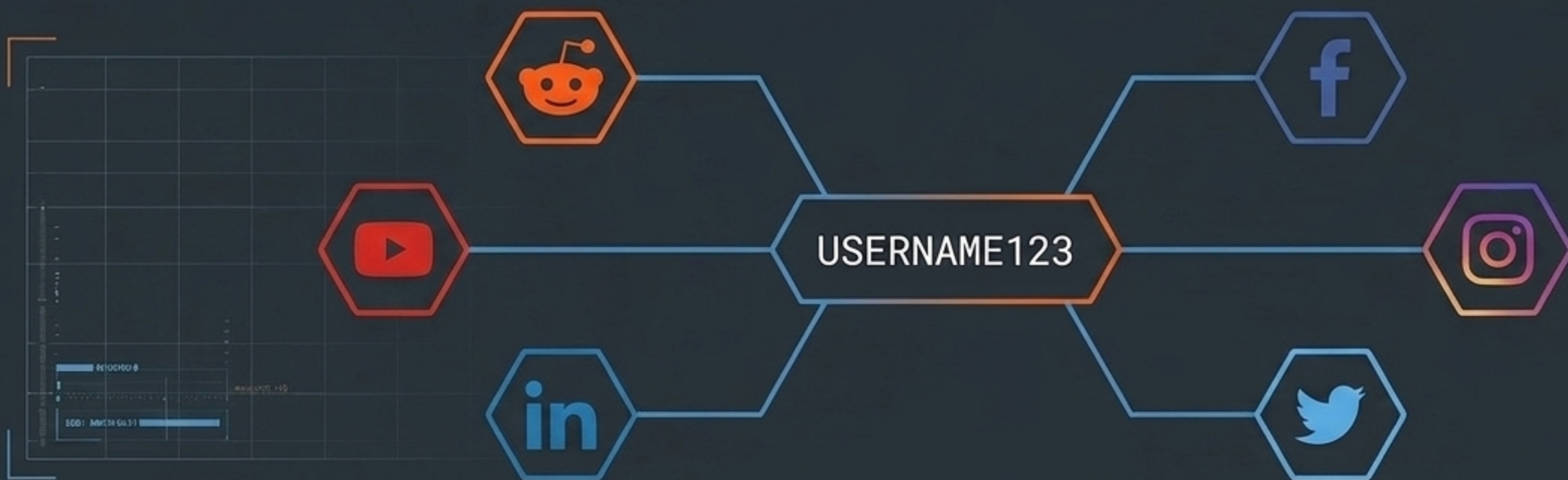


500K 35%

11A 190

16 | 10

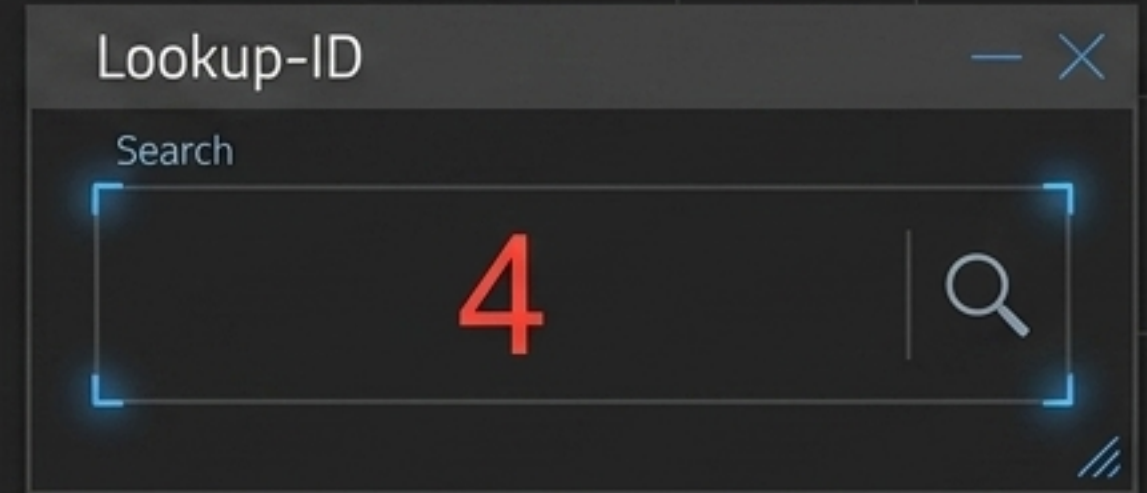
POSTOAI



Déconstruire Facebook (Open GraphSearch)

Tout sur la plateforme possède un identifiant numérique unique (ID).

`https://www.facebook.com/photo.php?fbid=101038...&set=a.[IDENTIFIANT].4`



Requêtes Facebook : Armer les données

```
search/str/[ID]/photos-of
```

Trouver les photos où la cible est identifiée. Contourne le problème d'une photo de profil masquée.

```
search/str/[ID]/employers/stories-at/
```

L'affaire : L'employé se disant paralysé, démasqué en train de jouer au basketball à un événement d'entreprise.

```
search/[ID]/places-visited/
```

L'affaire : Un criminel en cavale arrêté car ses historiques de géolocalisation l'ont ramené au même bar un mardi sur deux.

Pastebin : Le presse-papiers d'Internet

Pastebin ID: 7dE4sLq | Syntax: None | Expires: Never | Visibility: Public

```
1 ---BEGIN PG PRIVATE KEY---
2 [REDACTED]
3 [REDACTED]
4 [REDACTED]
5 [REDACTED]
6 [REDACTED]
7 [REDACTED]
8 [REDACTED]
9
10 User: admin_corp | Pass: [REDACTED]
11 [REDACTED]
12 [REDACTED]
13 [REDACTED]
14 [REDACTED]
15
16 Database dump: client_emails.sql
17 [REDACTED]
18 [REDACTED]
19 [REDACTED]
20 [REDACTED]
21 [REDACTED]
22 [REDACTED]
23 [REDACTED]
24
25 API Key: [REDACTED]
26 [REDACTED]
27 [REDACTED]
28 [REDACTED]
```

Mine d'or pour les fuites :
numéros de cartes bancaires,
mots de passe et bases de
données divulguées.



Mise en garde : Utilisez
toujours la barre de
recherche. Ne saisissez pas
votre requête dans le champ
de création de note publique.

Cas d'usage :

Découverte de dizaines
d'identifiants d'employés
divulgués par un pirate suite
à une brèche.

La boîte à outils OSINT (Matrice de synthèse)



Vecteur / Outil	Point d'entrée (On a...)	Extraction (On obtient...)	Profondeur
MXToolbox	En-tête courriel / IP	Véritable origine réseau	Niveau 1
Zabasearch	Nom	Dossiers publics	Niveau 1
Pipl / KnowEm	Pseudonyme / Email	Alias multiples	Niveau 2
Recherche d'images	Photo	Faux profils / Source	Niveau 2
Facebook Graph	URL Facebook	Géolocalisation / Réseau	Niveau 3