

squad



MIX YOUR
TALENT

Introduction aux techniques *forensics*

1

Introduction de l'Introduction

2

Les types de preuves inforensique

3

Les compétences requises

4

Les jobs dans l'inforensique

5

Historique de l'inforensique

Chiffres clés

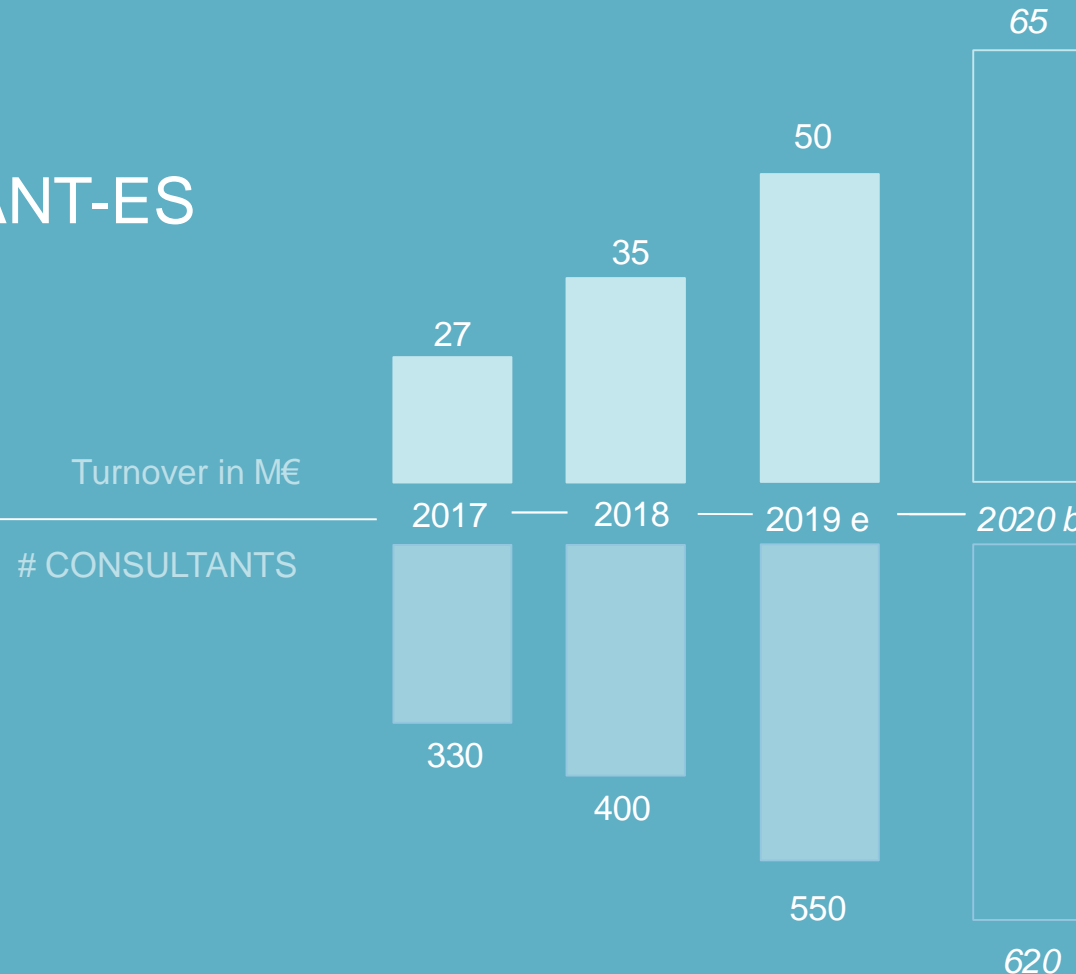
Plus de 85% de croissance organique sur les 3 dernières années



Fin 2019

550 CONSULTANT-ES

50 M€



Paris

Aix-En-Provence

Sophia-Antipolis

Toulouse

Lyon

Rennes

Nantes

Adélaïde (Australie)

NOS METIERS

SMACS : Social Mobility Analytics Cloud Security

Cyber Security



240+ PROFESSIONNEL-LES

Expert-es GRC – auditeur-rices PASSI -
Ethical hackers (pentester) – Expert-es
SIEM / SOC – Analyste SOC – Expert-es
Conformité - Forensics – Formateur-rices.

INVESTISSEMENT EN R&D

SDN & blockchain (brevet)
Data Centric Security
Precognition incidents sécurité

Virtual Infra - Cloud



185+ PROFESSIONNEL-LES

Architectes – DevOps, NetOps, SecOps -
Expert-es Virtualisation, Conteneurisation
- Expert-es Cloud – Expert-es Software
Defined Datacenter – Formateur-rices

INVESTISSEMENT EN R&D

Orchestration, Automatisation et
déploiement de services Software
Defined (Infra As Code)

Digital Factory



125+ PROFESSIONNEL-LES

Expert-es Ergonomie, Design, SCRUM
Agilité, Chef-fe de Projet, Technical
Leader, Développeur-euse Front multi
plates-formes (mobiles, web)

INVESTISSEMENT EN R&D

Ergonomie cognitive UX
Accessibilité numérique
Security by Design

*Services à la carte, Audit & conseil, Assistance Technique, Centre de Services, Projets
en engagement de moyens ou de résultats*

1


Introduction de l'Introduction

Votre intervenant :
Florian
CARFANTAN



PyDens	Lord0rSQL	Sayx1	Nightshade999	invite(x40)
CryptoHack	MysteryTwister	A11len	cuantico	x6d6f6e73
247CTF	CanHackMe	a68523981	surunze	
Énigmes À Thématiques	CTFS.ME	SAIDES	waitfort	

tenflo's Profile

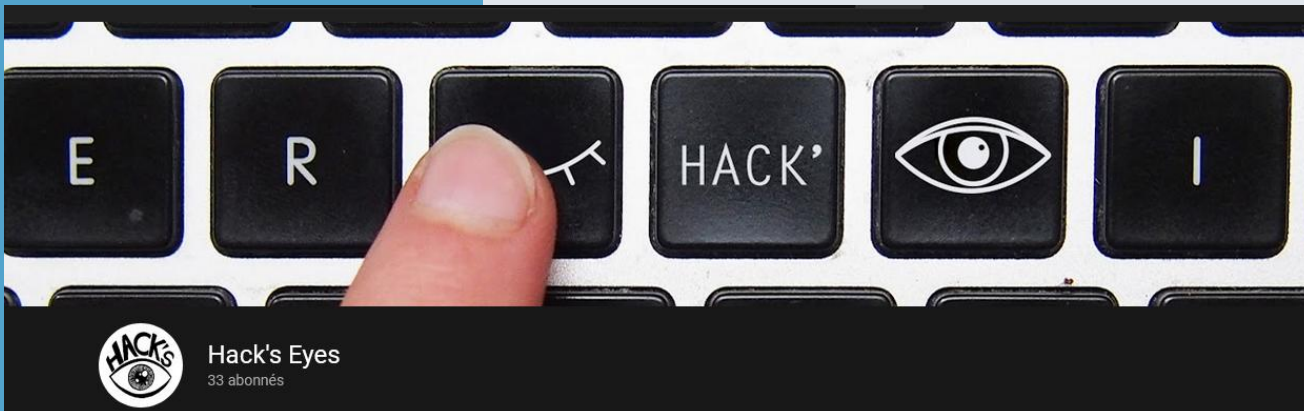
Country	
Username	tenflo
Points	<u>229913</u>
Classement Général	56
Classement par Pays	<u>13</u>
Register Date	Avril 27, 2016 - 17:08:04
Last Activity	Inconnu
Profile Views	27699
Website	https://www.youtube.com/channel/UCJh97sws1B4cMOD_oixiXLQ

Sites préférés

- [Root-Me](#)

Site

- [RedTigers Hackit](#)
- [hax.tor.hu](#)
- [ThisisLegal.com](#)
- [Hack The Box](#)
- [HackThisSite](#)
- [OverTheWire.org](#)
- [Tasteless](#)
- [Net-Force](#)
- [Hacker.org](#)
- [wargame.kr](#)
- [WeChall](#)
- [Defend the Web](#)
- [Hacking-Challenges](#)
- [Root-Me](#)
- [ae27ff](#)
- [wixxerd.com](#)
- [Electrica](#)
- [NewbieContest](#)
- [NOE.systems](#)
- [W3Challs](#)
- [pwnable.kr](#)
- [RingZer0 Team Online CTF](#)
- [247CTF](#)
- [Rankk](#)
- [TheBlackSheep](#)
- [Revolution Elite](#)
- [HackBBS](#)



Mon parcours :

- 10 ans de cybersécurité côté défensif
 - 6 SOC différents
 - SIEM
 - EndPoint protection
 - Investigation
 - Conception de pare-feu embarqué
 - **Forensic**
- 5 ans de cybersécurité côté offensif
 - *Pentest*
 - Red Team
 - Purple Skills
- Beaucoup de CTF
- Créateur de [Hack's Eyes](#)

squad

1

Introduction de l'Introduction



The screenshot shows the Wikipedia page for 'Informatique légale'. The browser address bar displays 'https://fr.wikipedia.org/wiki/Inform'. The page header includes navigation links like 'Non connecté', 'Discussion', 'Contributions', 'Créer un compte', and 'Se connecter'. The article title 'Informatique légale' is prominently displayed. A warning box in orange states: 'Certaines informations figurant dans cet article ou cette section devraient être mieux reliées aux sources mentionnées dans les sections « Bibliographie », « Sources » ou « Liens externes » (novembre 2015). Améliorez sa vérifiabilité en les associant par des références à l'aide d'appels de notes.' The main text begins with: 'On désigne par **informatique légale**, **investigation numérique légale** ou **informatique judiciaire** l'application de techniques et de protocoles d'investigation numériques respectant les procédures légales et destinée à apporter des preuves numériques à la demande d'une institution de type judiciaire par réquisition, ordonnance ou jugement. On peut donc également la définir comme l'ensemble des connaissances et méthodes qui permettent de collecter, conserver et analyser des preuves issues de supports numériques en vue de les produire dans le cadre d'une action en justice.' The text concludes with: 'Ce concept, construit sur le modèle plus ancien de **médecine légale**, correspond à l'anglais **computer forensics**.'

← → ↺ 🏠

🔒 <https://fr.wikipedia.org/wiki/Inform> 📄 ⋮ 🛡️ ⭐ 🔍 Rechercher

👤 Non connecté Discussion Contributions Créer un compte Se connecter

Article Discussion Lire Modifier Modifier le code Voir l'historique Rechercher dans Wikipédia 🔍

WIKIPÉDIA

L'encyclopédie libre

Accueil
Portails thématiques
Article au hasard
Contact

Contribuer
Débuter sur Wikipédia
Aide
Communauté
Modifications récentes
Faire un don

Outils

Pages liées

Informatique légale



Certaines informations figurant dans cet article ou cette section devraient être mieux reliées aux sources mentionnées dans les sections « Bibliographie », « Sources » ou « Liens externes » (novembre 2015).

Améliorez sa **vérifiabilité** en les **associant par des références** à l'aide d'**appels de notes**.

On désigne par **informatique légale**, **investigation numérique légale** ou **informatique judiciaire** l'application de techniques et de protocoles d'investigation numériques respectant les procédures légales et destinée à apporter des preuves numériques à la demande d'une institution de type judiciaire par réquisition, ordonnance ou jugement. On peut donc également la définir comme l'ensemble des connaissances et méthodes qui permettent de collecter, conserver et analyser des preuves issues de supports numériques en vue de les produire dans le cadre d'une action en justice.

Ce concept, construit sur le modèle plus ancien de **médecine légale**, correspond à l'anglais **computer forensics**.



1

Introduction de l'Introduction

L'objectif d'une analyse inforensique est de comprendre ce qu'il s'est passé. Lorsque c'est pour un cybercrime, 3 aspects doivent être établis :

1. le moyen : quels outils ont permis au cybercrime d'avoir lieu
2. l'opportunité : quels faiblesses ont permis au cybercriminel de commettre le cybercrime
3. la motivation : la raison qui a poussé l'auteur-riche du cybercrime à le faire

Dans le monde de l'entreprise, on cherche surtout le qu'est-ce qui s'est passé et pourquoi ça a été possible pour que ce ne soit plus possible dans l'avenir. C'est souvent complexe de pouvoir comprendre la motivation de l'attaquant-e et encore plus complexe de retrouver son identité.

1

Introduction de l'Introduction

2

Les types de preuves inforensique

3

Les compétences requises

4

Les jobs dans l'inforensique

5

Historique de l'inforensique

2

Les types de preuves inforensique

Quelles sont les types de preuves utilisés par l'inforensique ?

- A. Capture réseau
- B. Document imprimé
- C. E-mail
- D. Historique Internet
- E. Photo numérique
- F. SMS
- G. Vidéo numérique

2

Les types de preuves inforensique

Quelles sont les types de preuves utilisés par l'inforensique ?

A. Capture réseau

B. Document imprimé

Voir les points jaunes qui permettent d'horodater avec le numéro de série de l'imprimante ou autre technique de *watermarking*.

C. E-mail

D. Historique Internet

E. Photo numérique

F. SMS ou autre messagerie type WhatsApp ou Signal avec le chiffrement de bout en bout

G. Vidéo numérique (caméra de surveillance)

2

Les types de preuves inforensique

La **capture réseau** est une preuve inforensique peu commune dans le monde judiciaire mais plus courante dans le monde de l'entreprise qui a souvent des sondes réseau en coupure de l'accès à Internet. Ces sondes pouvant avoir un impact sur la vie privée (par exemple avec le cassage de flux SSL), l'utilisateur-riche est prévenu-e en signant la charte informatique.

Petite démonstration pour savoir si votre flux SSL est cassé.

Certains outils génèrent automatiquement des captures réseaux lors d'un comportement suspect sur un poste.

L'inforensique sur du réseau sera détaillé dans le chapitre le concernant.

2

Les types de preuves inforensique

L'**e-mail** est la preuve en inforensique la plus importante car :

1. Le propriétaire de l'adresse mail contrôle l'adresse et il y a preuve d'intention.
2. La date et l'heure d'un mail permettent de l'intégrer à la frise chronologique des événements.
3. C'est très utilisé, surtout dans le monde professionnel.
4. Un e-mail est présent à plusieurs endroits alors c'est compliqué de le compromettre.
5. C'est une preuve qui est communément utilisé en justice.
6. C'est généralement accessible à l'investigateur-rice.

Mais ils sont de plus en plus sur du cloud ce qui apporte des complexifications pour l'inforensique...



2

Les types de preuves inforensique

L'**historique Internet** est une preuve inforensique accessible à quels endroits ?

- A. Dans la mémoire RAM
- B. Dans une capture réseau
- C. Sur une clé USB
- D. Sur le smartphone
- E. Sur le disque dur

2

Les types de preuves inforensique

L'**historique Internet** est une preuve inforensique accessible à quels endroits ?

A. Dans la mémoire RAM

A condition d'avoir un dump mémoire du moment où la personne surfait sur Internet. Les outils de dernière génération sur EndPoint génère automatiquement l'envoi d'un dump mémoire lors d'un évènement suspect.

B. Dans une capture réseau

A condition que le flux n'est pas chiffré ou que du cassage de flux SSL est en place.

C. Sur une clé USB

D. Sur le smartphone

E. Sur le disque dur

A condition que le navigateur soit configuré pour stocker en local l'historique Internet, c'est de moins en moins fréquent en entreprise.

2

Les types de preuves inforensique

Une **image** est une preuve intéressant, pas uniquement pour ce qu'on y distingue, mais aussi pour ses métadonnées :

```
$exif Pictures/1.jpg
EXIF tags in 'Pictures/1.jpg' ('Motorola' byte order):
```

```
-----+-----
Tag                |Value
-----+-----
Manufacturer       |Apple
Model              |iPhone 4S
Orientation         |Top-left
X-Resolution        |72
Y-Resolution        |72
Resolution Unit     |Inch
Software            |6.1.2
Date and Time       |2013:03:11 11:47:07
[...]
Scene Capture Type  |Standard
North or South Latit|N
Latitude            |47, 6, 16.946
East or West Longitu|E
Longitude           | 7, 24, 52.9844
Altitude Reference  |Sea level
Altitude            |16.776
```

2

Les types de preuves inforensique

Le **SMS** est une preuve inforensique commune car il circule en clair sur le réseau téléphonique et qu'il est stocké en local sur le smartphone mais également sur des relais accessible avec un mandat.

La durée de vie des SMS sur les relais est généralement courte.

Les preuves associés au smartphone feront l'objet d'un chapitre complet car elles sont riches et très utiles pour de nombreuses raisons qui seront détaillés.

Comment les investigateur-rices peuvent retrouver une conversation WhatsApp en clair alors que c'est du chiffrement de bout en bout et que c'est chiffré sur le smartphone ?

2

Les types de preuves inforensique

La **vidéo** est très utilisée de nos jours et par tous, que ce soit par les forces de polices ou les manifestants par exemple. C'est évidemment un moyen très efficace pour comprendre ce qu'il s'est passé.

La vidéo-surveillance est une composante importante, notamment dans le monde de l'entreprise.

Même si une vidéo est plus compliqué à modifier qu'un texte ou qu'une image, il est toujours important de vérifier qu'il n'y a pas eu compromission de la preuve, notamment car il est encore fréquent aujourd'hui de voir des flux de vidéo-surveillance non-chiffrés donc modifiable par un attaquant en position d'homme-du-milieu.

Attention aux attaques de type deepfakes qui seront de plus en plus présentes.

2

Les types de preuves inforensique

Pourquoi les données de cartes bancaires enregistrés lors d'un *skimming* sont chiffrés ?

- A. Pour compliquer le travail de la police
- B. Pour que la personne qui récupère le matériel n'utilise pas les informations récoltés
- C. Pour être en accord avec la norme PCI-DSS
- D. Pour éviter la détection de l'exfiltration de données par les équipements de sécurité



2

Les types de preuves inforensique

Pourquoi les données de cartes bancaires enregistrés lors d'un *skimming* sont chiffrés ?

- A. Pour compliquer le travail de la police
- B. Pour que la personne qui récupère le matériel n'utilise pas les informations récoltés
- C. Pour être en accord avec la norme PCI-DSS
- D. Pour éviter la détection de l'exfiltration de données par les équipements de sécurité



1

Introduction de l'Introduction

2

Les types de preuves inforensique

3

Les compétences requises

4

Les jobs dans l'inforensique

5

Historique de l'inforensique

3

Les compétences requises

Quelles sont les compétences requises pour un-e investigateur-rice en inforensique ?

- A. Chimie
- B. Communication
- C. Confidentialité
- D. Curiosité
- E. Jeux vidéo
- F. Langue
- G. Légal
- H. Techniques
- I. Traitement du signal

3

Les compétences requises

Quelles sont les compétences requises pour un-e investigateur-ric(e) en inforensique ?

A. Chimie

B. Communication

Une bonne expression écrite et orale est CAPITALE !

C. Confidentialité

Même avec ses collaborateur-ric(e)s, on ne cite pas les clients. Attention au couple défense/réseaux sociaux !!

D. Curiosité

C'est un monde qui évolue en permanence, il faut aimer apprendre tout le temps.

E. Jeux vidéo

F. Langue

G. Légal

H. Techniques

Dans de nombreux domaines mais surtout les 3 briques réseau, sécurité et système.

I. Traitement du signal

1

Introduction de l'Introduction

2

Les types de preuves inforensique

3

Les compétences requises

4

Les jobs dans l'inforensique

5

Historique de l'inforensique

4

Les jobs dans l'inforensique

L'inforensique nécessite un niveau d'expertise, ne comptez pas en faire avant d'avoir plusieurs années d'expérience professionnel en cybersécurité.

La cybersécurité recrute à tout va, notamment dans les SOC qui sont un bon endroit pour se faire une première expérience technique varié avec des petites investigations sur des comportements anormaux sur le système d'information du client. Il y a en général 3 niveaux au SOC (L1/L2/L3).

Peu de poste à plein temps en France, sauf à l'ANSSI où il y a une même une équipe RE (Reverse-Engineering) séparé de l'équipe inforensique. Il y a surtout des personnes qui font d'autres types d'audit en parallèle des audits en inforensique.

4

Les jobs dans l'infoforensique

Les domaines qui embauchent des experts en infoforensique :

- Les forces de l'ordre (police, gendarmerie, militaire, renseignement...)
- Les cabinets d'audit (Deloitte, Ernst & Young, KPMG, PwC...)
- Les grosses boites ont parfois une personne à temps plein en interne (EDF, SNCF, Banques, Assurance...)
- Les expert-e-s judiciaires en informatique (Moyenne d'âge élevé !)

1

Introduction de l'Introduction

2

Les types de preuves inforensique

3

Les compétences requises

4

Les jobs dans l'inforensique

5

Historique de l'inforensique

5

Historique de l'inforensique

La France a suivi les Américains et non l'inverse sur ce sujet.

Extrait de "A Practical Guide to Computer Forensics Investigations" by DR. DARREN R. HAYES:

1980s: The Advent of the Personal Computer

Interestingly, around this time, the first electronic bulletin boards emerged and facilitated communication between hackers. Subsequently, hacking groups, like the Legion of Doom in the United States, emerged. The 1983 film *War Games* introduced the public to the concept of hacking with a personal computer in order to gain access to government computers. In 1984, Eric Corley (with the handle Emmanuel Goldstein) published *2600: The Hacker Quarterly*, which facilitated the exchange of hacking ideas. Kevin Mitnick, one of the earliest hackers, was convicted in 1989 of stealing firmware (software) from DEC and access codes from MCI. In the wake of numerous high-profile system

Éléments sous droits d

A History of Computer Forensics

15

break-ins, Congress passed the Computer Fraud and Abuse Act in 1986. The act has subsequently been amended several times.

Federal Bureau of Investigation (FBI)

In 1984, the FBI established the Magnetic Media Program, which subsequently became known as the **Computer Analysis and Response Team (CART)**. The group was responsible for computer forensics examinations. Special Agent Michael Anderson, in the criminal investigation division of the IRS, has sometimes been referred to as the Father of Computer Forensics.

National Center for Missing and Exploited Children (NCMEC)

In local and county law enforcement, computer forensics investigators generally spend a large proportion of their time on child endangerment cases, especially those involving the possession and distribution of child pornography. In 1984, the U.S. Congress established the National Center for Missing and Exploited Children (NCMEC). NCMEC is mandated to help locate missing children and combat the (sexual) exploitation of children. It acts as a central repository for documenting crimes against missing children, including victims of child endangerment.

INTERPOL

In terms of international efforts and collaboration, INTERPOL has taken a central role in applying digital evidence to criminal investigations. **INTERPOL** is the world's largest international police organization, representing 188 member countries. In 1989, the General Secretariat was moved to Lyon, France. In 2004, an INTERPOL liaison office was established at the United Nations, and in 2008, a special representative was appointed to the European Union in Brussels.

INTERPOL's Incident Response Team (IRT) has provided computer forensics expertise on a number of high-profile international investigations. In a 2008 report, computer forensics examiners from law enforcement in Australia and Singapore examined 609GB of data on eight laptops, two external hard drives, and three USB thumb drives at the request of the Colombian authorities. The hardware and software belonged to the *Fuerzas Armadas Revolucionarias de Colombia* (FARC). FARC is an anti-government terrorist organization in Columbia, which is largely funded through its control of illegal drug trafficking, primarily the trafficking of cocaine. Colombian investigators contacted INTERPOL to examine the seized laptops in an effort to have unbiased investigators view the digital evidence to corroborate assertions that the digital evidence had been handled in a forensically sound manner.

At the 2008 ICPO-INTERPOL General Assembly in St. Petersburg, Russian approval was made for the creation of an INTERPOL Computer Forensics Analysis Unit. This unit provides training and assistance on computer forensics investigations and has been charged with the development of international standards for the search, seizure, and investigation of electronic evidence.

INTERPOL has worked for many years on fighting crimes against children. Similar to NCMEC, since 2001, INTERPOL has maintained a database of exploited children, referred to as the INTERPOL Child Abuse Image Database (ICAID). Subsequently, in 2009, ICAID was replaced by the International Child Sexual Exploitation image database (ICSE DB). The database is accessible to law enforcement in real time around the world. This powerful database incorporates image comparison software to link victims with places. INTERPOL also works with other agencies worldwide to fight child abuse, including COSPOL Internet Related Child Abuse Material Project (CIRCAMP) and the Virtual Global Taskforce. CIRCAMP is a European law enforcement network, that monitors the Internet to detect child pornography and child abuse. The Virtual Global Taskforce has the same purpose and mission but is a global network of law enforcement agencies fighting online child abuse.

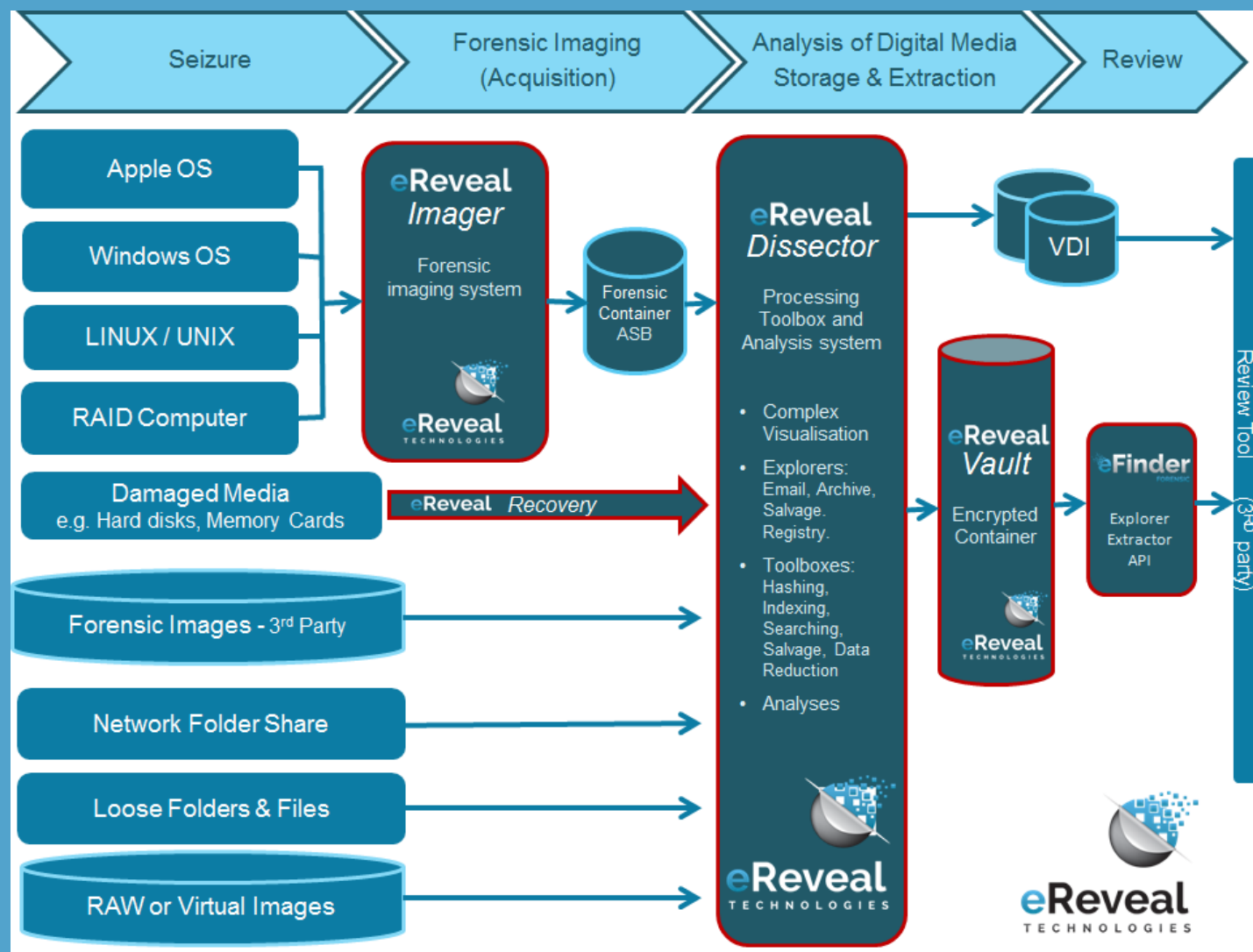
INTERPOL has been successful in coordinating international efforts to apprehend suspected pedophiles. Following a 2006 police raid on Internet predators in Norway, investigators discovered a laptop containing nearly 800 horrifying images of young boys. Nearly 100 of the images depicted a

Éléments sous droits

middle-aged, white male watching these boys being abused. The authorities requested the assistance of INTERPOL to track down the unknown predator. INTERPOL initiated a massive manhunt and solicited help from the public through the media. Within 48 hours of the appeal for help, INTERPOL and Immigration and Customs Enforcement (ICE) arrested 60-year-old Wayne Nelson Corliss of Union, New Jersey.

5

Historique de l'inforensique



Exemple d'usine à gaz pour l'inforensique d'aujourd'hui

5

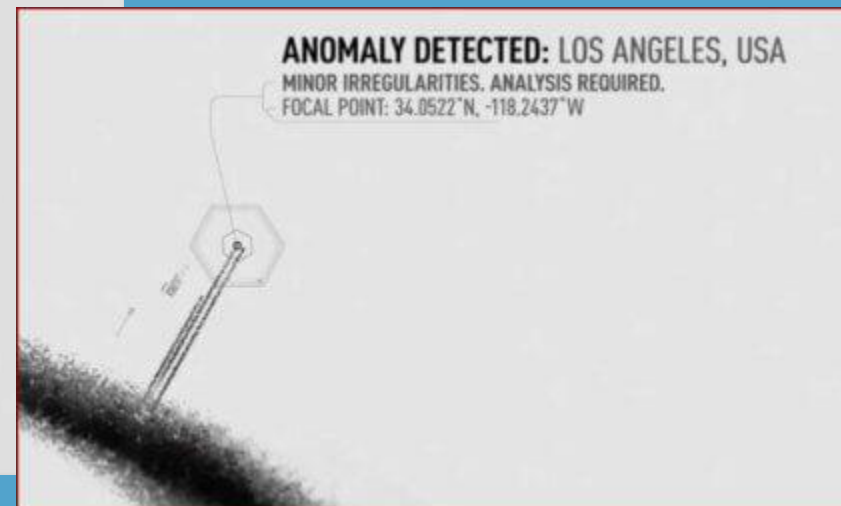
Historique de l'infoforensique

DIVERGENCE: VICTORVILLE, USA
2.3 ARC MINUTES
FOCAL POINT: 34.5362° N, 117.2928° W



Futur de l'infoforensique ?

ANOMALY DETECTED: LOS ANGELES, USA
MINOR IRREGULARITIES. ANALYSIS REQUIRED.
FOCAL POINT: 34.0522° N, -118.2437° W



1

Introduction de l'Introduction

2

Les types de preuves inforensique

3

Les compétences requises

4

Les jobs dans l'inforensique

5

Historique de l'inforensique

Si on résume ensemble

...

Conclusion



I didn't invent forensic science and medicine. I just was one of the first people to recognize how interesting it is.

— Patricia Cornwell —

AZ QUOTES

MERCI

www.squad.fr

PUBLIC

