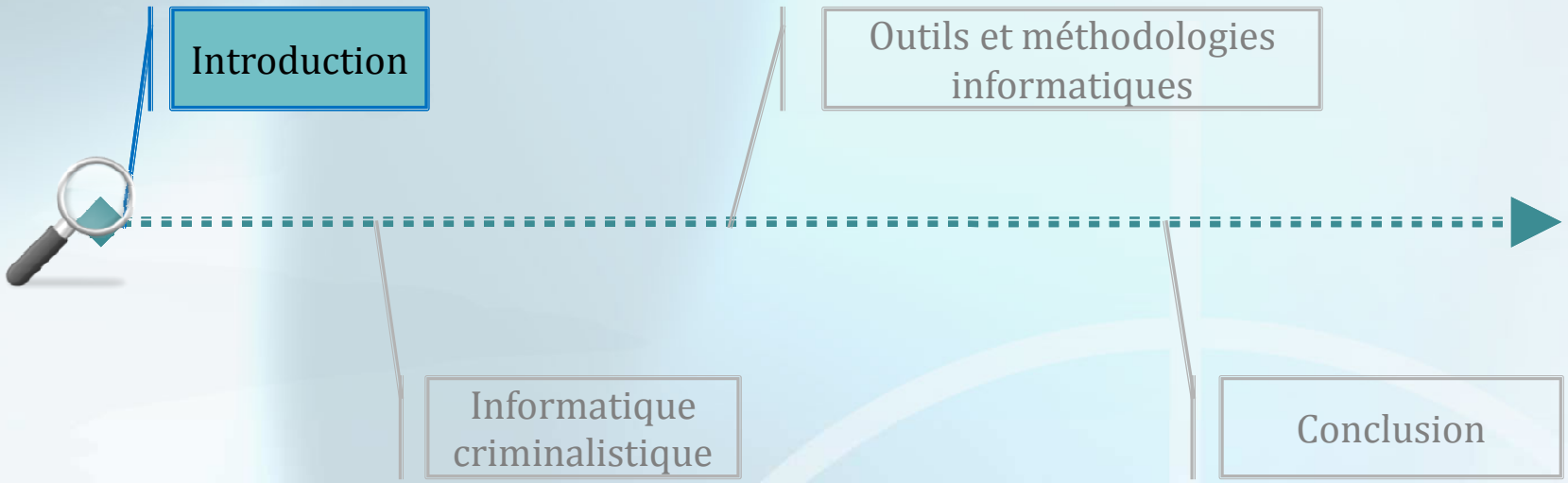
Large panorama des méthodes informatiques criminalistiques

Xposé de 3ème année

Sébastien DESTABEAU – IR3

Plan de présentation

- **Introduction**
  - Objectif de cet Xposé
  - Motivation du choix du sujet
- **Informatique criminalistique**
  - Définitions
  - Expert en informatique légale
  - Périmètre et domaines d'intervention
- **Outils et méthodologies informatiques**
  - Méthodologies
  - Boîte à outils
  - Techniques
  - Contraintes légales
- **Conclusion**



Il était une fois …

INTRODUCTION

Objectif de cet Xposé

Objectif de cet exposé

- Présenter le métier d'expert en informatique légale
- Soulever des notions juridiques importantes
- Démystifier les séries policières

DO

Objectif de cet Xposé

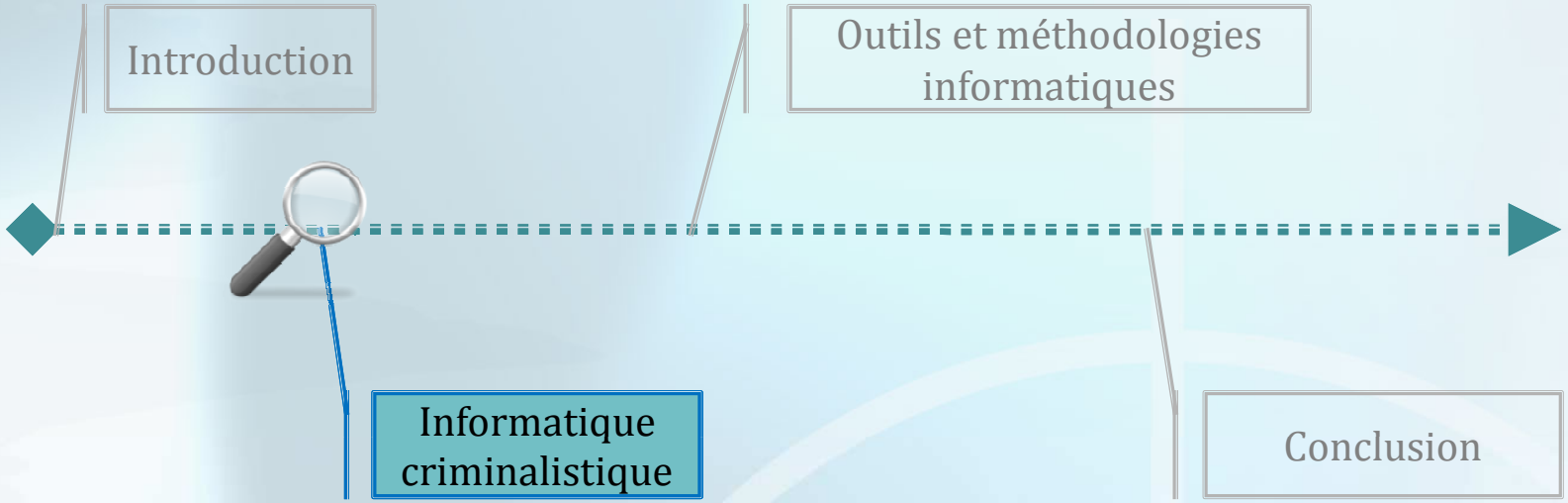
Cet exposé n'a pas vocation à :

- Parler pleinement de sécurité informatique
- Parler pleinement de piratage
- M'étendre sur tous les domaines de la criminologie
- Vendre ou promouvoir un quelconque logiciel
- Faire de la publicité pour des séries TV

Motivation du choix du sujet

Pourquoi ai-je choisi ce sujet ?

- Une passion transmise par un enseignant-RSSI
- Une « addiction » aux séries américaines
- Ma curiosité
- Un domaine d'apprentissage intéressant



Quézaco ?

INFORMATIQUE CRIMINALISTIQUE

Définitions

Idée toute faite…

Définitions

Qu'est-ce que l'investigation criminelle?

- Un important travail de recherche suivi
- Une enquête
- Une étude approfondie des faits
- Fait intervenir des professionnels de tout bords
- Est un ensemble d'outils et de méthodologies
- Est une science qui étudie les faits criminels

Définitions

Qu'est-ce qu'un crime ?

- Acte **ET** intention de porter atteinte au bien-être collectif de la société
- Catégorie d'infractions pénales la plus grave
- Sévèrement puni par la loi

Le saviez-vous ?

Dans les pays anglophones, le mot « **crime** » est un faux-ami qui désigne autant un crime qu'un délit.

Définitions

Qu'est-ce qu'un délit?

- Fait juridique ou infraction causant un dommage à autrui
- Acte jugé au civil ou au pénal selon la situation

Le saviez-vous ?

Les peines correctionnelles possibles pour un délit peuvent être des jours de travaux d'intérêt général, une amende variant entre 3750 € et 7,5 millions d'€ ou même un emprisonnement maximal de 10 ans.

Définitions

Catégories des « Crimes et délits » du Code Pénal :

- Contre les personnes : articles 211-1 à 227-33
- Contre les biens : articles 311-1 à 324-9
- Contre la nation, l'Etat et la paix publique : articles 410-1 à 450-5
- Crimes et délits de guerre : articles 461-1 à 462-11
- Autres : articles 511-1 à 521-2

Définitions

Délits

Abus de confiance
Arnaque
Blanchiment d'argent
Braquage
Car jacking
Chantage
Contrefaçon
Corruption
Deal
Désertion
Détournement de fonds
...

Crimes

Attentat
Empoisonnement
Esclavage
Espionnage
Meurtre
Pédophilie
Pédopornographie
Proxénétisme
Terrorisme
Torture
Viol
...

Définitions

Qu'est-ce que l'informatique légale ?

« Il s'agit d'une science qui a pour but de démontrer comment les preuves digitales peuvent être utilisées pour reconstruire une scène de crime ou un accident, identifier les suspects, appréhender le coupable, défendre l'innocent et comprendre les motivations criminelles. »

Quelques points-clés de l'histoire :

- 1910 : 1er laboratoire de police criminelle en France
- 1984 : 1ère analyse ADN pour résoudre une affaire de meurtre
- 1999 : centralisation des banques de données d'empreintes américaines
- 2001 : création de l'Institut National de Police Scientifique (**INPS**) en France
- 2005+ : optimisation des algorithmes de recherches pour empreintes

Définitions

Une preuve :

- « Ne ment pas, n'oublie pas et ne commet pas d'erreurs »
- Est démontrable
- Est indépendante de la version des faits des témoins
- Est dépendante des conditions environnementales du lieu d'enquête
- Peut être détruite

Une preuve digitale :

- Est une copie numérique d'une information réelle
- Peut représenter une information pertinente pour l'enquête
- Peut être conservée de manière durable

Expert en informatique légale

Qu'est-ce qu'un expert en informatique légale ?

- Monsieur tout-le-monde
- Spécialiste de l'informatique
- Participe aux enquêtes judiciaires

Un expert en informatique légale doit :

- Suivre des formations
- Effectuer de la veille informatique
- Être inscrit sur une liste d'expert judiciaire pour exercer son métier
- Connaître la loi, le secret professionnel et le droit en général
- Rédiger des rapport d'expertise

Expert en informatique légale

En France, il existe différentes entités d'expertises :

- **L'Institut National de la Police Scientifique, qui dispose de :**
  - 1600 employés dont 640 experts
  - 6 laboratoires spécialisés (Marseille, Toulouse, Lille, Lyon, Paris)
- **La gendarmerie**
- **Des entreprises privées et groupes internationaux d'experts**
- **Des experts indépendants**

Pour postuler : s'adresser à la DCPJ à partir de Bac +5.

Expert en informatique légale

Aux Etats-Unis en 2010 :

- 12 000 experts

Dans la branche fédérale exécutive (entreprise privée) :

- Environ 150 employés
- Salaire moyen annuel : 94 800 $
- Fourchette moyenne : 57 – 126 K$

Au FBI :

- 500 experts
- Expertises criminalistiques depuis 1932

Périmètre et domaine d'intervention

Quand fait-on appel à lui ?

- Lors d'une instruction ou d'un procès par un juge
  - Cas du mari espionnant la messagerie de sa femme

- Lors de l'enquête préliminaire par un procureur ou officier de police
  - Cas de l'employeur suspectant un employé d'avoir vendu des données

- Lors de l'enquête de flagrance par un officier de police
  - Cas du pirate pris en flagrant délit contre une TPE

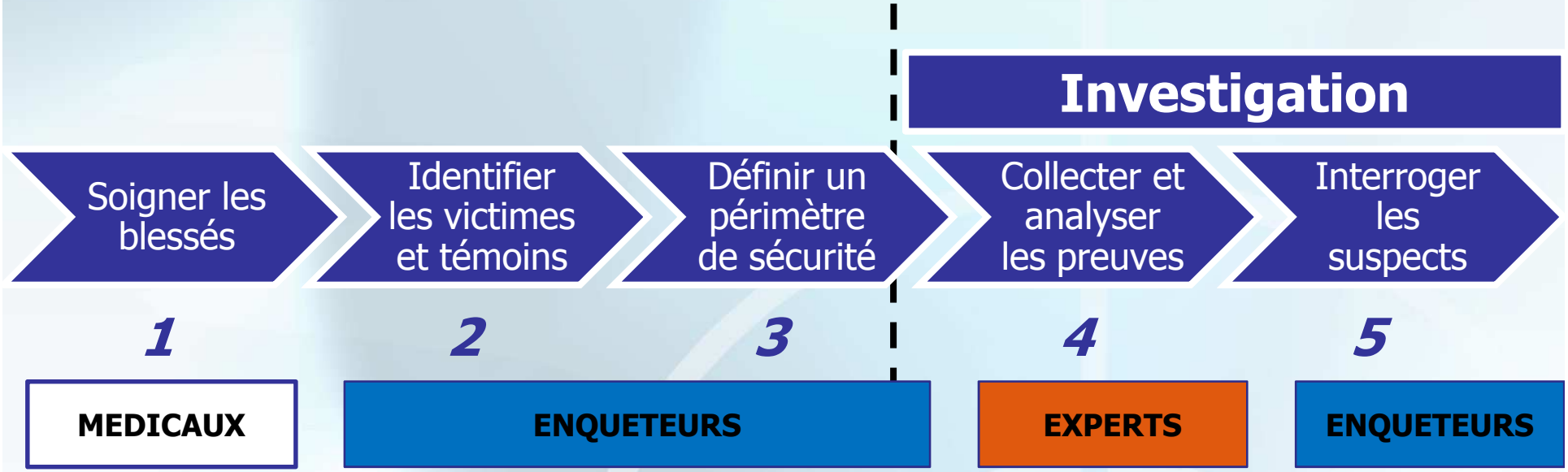
Périmètre et domaine d'intervention

Démarche générale lors d'une enquête préliminaire

D'après vous, à quel niveau intervient l'expert en informatique légale ?

Périmètre et domaine d'intervention

Démarche générale lors d'une enquête préliminaire



REPONSE…

Périmètre et domaine d'intervention

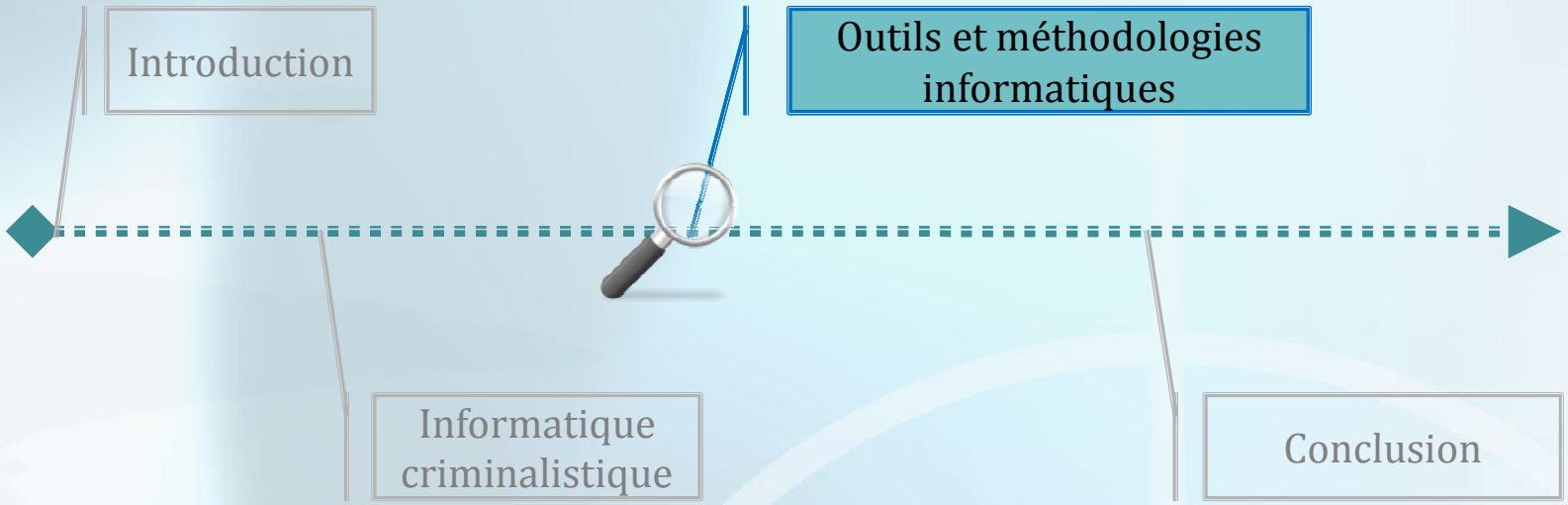
Démarche générale lors d'une enquête de flagrance

D'après vous, à quel niveau intervient l'expert en informatique légale ?

Périmètre et domaine d'intervention

Démarche générale lors d'une enquête de flagrance

REPONSE…

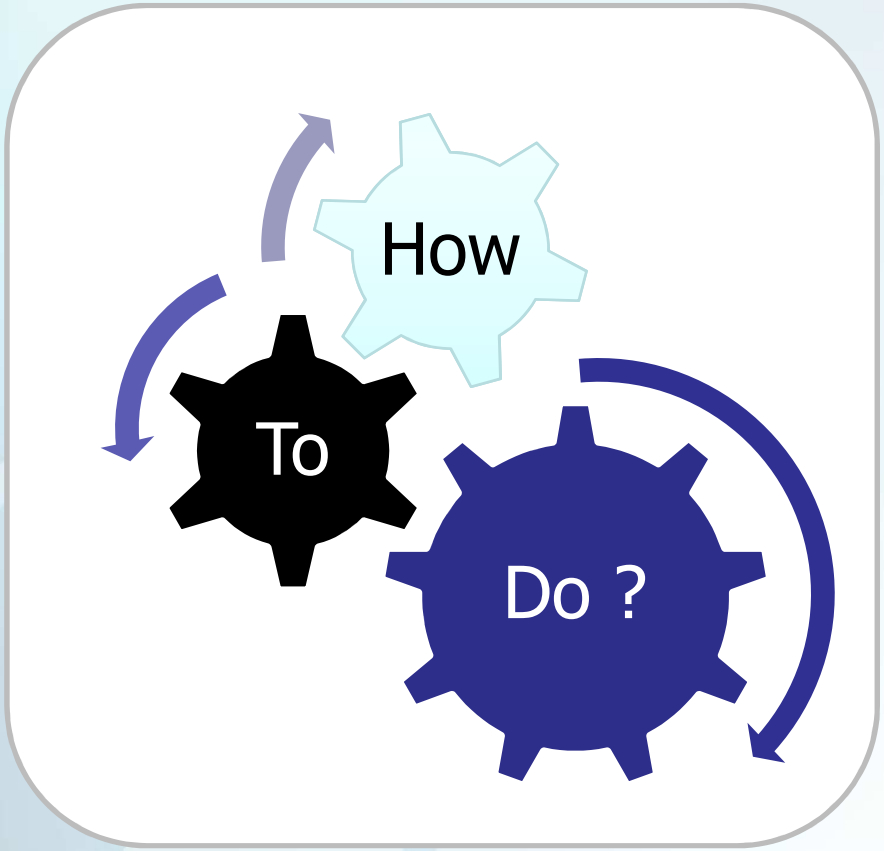


Houston, we have a problem !

OUTILS ET METHODOLOGIES INFORMATIQUES

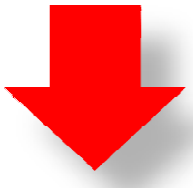
Méthodologies

- Saisir
- Rechercher
- Collecter
- Analyser
- Conserver
- Démontrer



Méthodologies

- Saisir
- Rechercher
- Collecter
- Analyser
- Conserver
- Démontrer



Méthodologies

- Saisir
- Rechercher
- Collecter
- Analyser
- Conserver
- Démontrer

Méthodologies

- Saisir
- Rechercher
- Collecter
- Analyser
- Conserver
- Démontrer

idImage = md5( )

Méthodologies

- Saisir
- Rechercher
- Collecter
- Analyser
- Conserver
- Démontrer

idCopie = md5( )

idCopie == idImage ?

Méthodologies

- Saisir
- Rechercher
- Collecter
- Analyser
- Conserver
- Démontrer

idCopie

Méthodologies

- Saisir
- Rechercher
- Collecter
- Analyser
- Conserver
- Démontrer

Boîte à outils

La boîte à outils de l'expert est composée de logiciels … :

- Système d'exploitation hautement sécurisé (DEFT, SIFT, Helix, Kali Linux)
- Analyse des logs PC, logiciels, Smartphones, Caméras (Autopsy, PhotoRec)
- Analyse des navigateurs (WebLog, Dumpzilla)
- Analyse de la RAM
- Analyse des périphériques connectés (NetSleuth)
- Analyse des fichiers
- Analyse des métadonnées de fichiers (ExifTool)
- Analyse des emails
- Virtualisation (Sandbox, Oracle VM VirtualBox)
- Cassage de mots de passe (OphCrack, Crack, John The Ripper)
- Cassage de clés WiFi (Aircrack)
- Analyse réseau (Wireshark, NetSleuth, Snort)
- Récupération de fichiers supprimés (TestDisk)
- …

Boîte à outils

… Et de matériels :

- Câbles (réseau, croisé, série, USB)
- Adaptateurs
- Connecteurs
- Ordinateur portable
- Disque dur grosse capacité, sécurisé par biométrie
- DVD et CD à graver
- Clé USB bootable pour des systèmes et logiciels en Live CD (Ophcrack)
- Stylos et papier ou dictaphone numérique
- Multiples tournevis toutes tailles, toutes formes
- Lampe électrique
- Ruban adhésif patafix, élastiques et colliers
- Vis, trombones
- Appareil photo
- …

Boîte à outils

Certains outils peuvent être obtenus gratuitement.

Les autres ont un prix conséquent :

- Récupération de données (de 39 à 1000 $)
- Scan de fichiers, image disque (de 495 à 3995 $)
- Scan d'emails (de 394 à 769 $)
- Extraction de données sur smartphones (229 $)
- Système d'exploitation sécurisé (de 139 à 239 $)

Coût des matériels :

- Duplicateur de supports de données (3300 $)

Techniques

Les techniques que nous allons découvrir :

- Stéganographie & stéganalyse
- Analyse de métadonnées
- Cryptographie & cryptanalyse

Les techniques qui ne seront pas abordées dans cet exposé :

- Analyse croisée de disques durs
- Récupération de données
- Analyse de logs
- Audit de réseaux
- Analyse de transactions bancaires
- Défloutage d'images et reconnaissance digitales
- Biométrie
- ...

Stéganographie & stéganalyse

La stéganographie, c'est :

- Dissimuler des informations dans d'autres informations
- Comme « un cheval de Troie »
- Utilisé par les pirates pour cacher des informations illicites
- Le message ou la donnée est souvent chiffré par mot de passe
- Une méthode presque indétectable avec de petits contenus

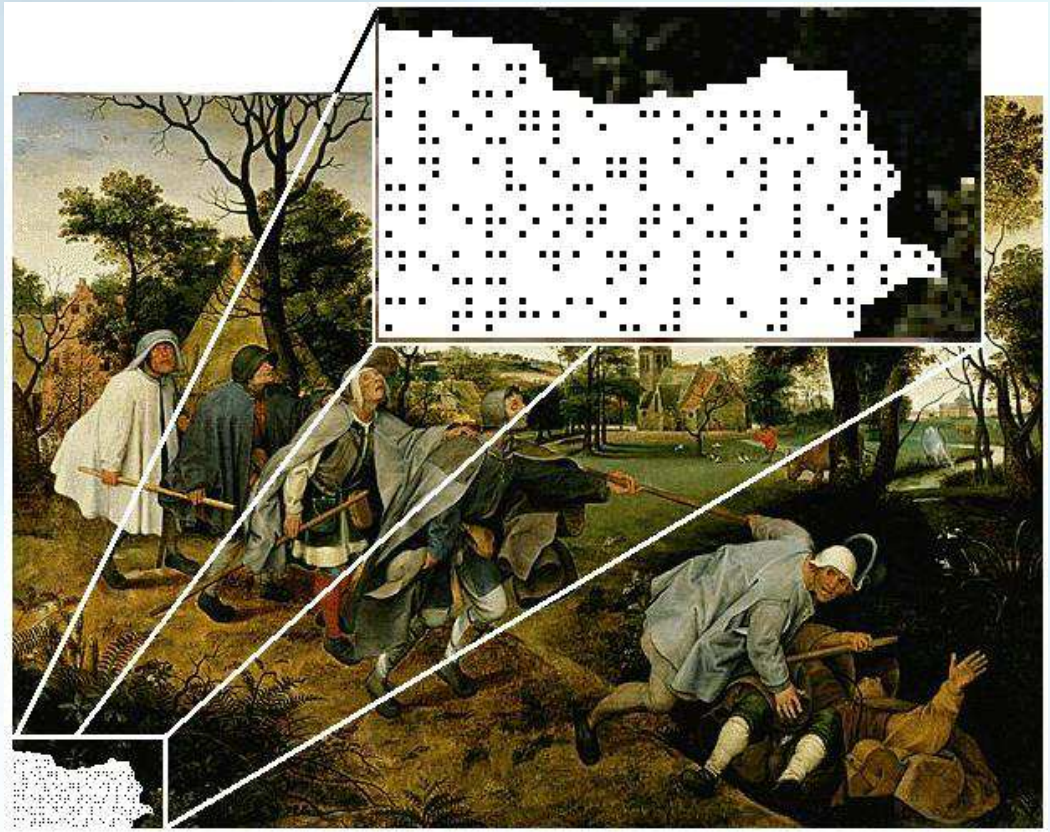
Stéganographie & stéganalyse

Un message est présent dans cette image.

Le voyez-vous ?

Stéganographie & stéganalyse

« Si un aveugle conduit un aveugle, ils tomberont tous les deux dans la fosse » **- Matthieu 15:14**



Stéganographie & stéganalyse

Exemple d'algorithme faible en stéganographie :

- Prendre une image

- Rédiger un message secret

Blablabla

- Pour chaque bit du message secret, prendre le pixel courant de l'image et récupérer le bit de poid faible

B = 01000010

R V B = 11111011 11010000 **10010111**

- Appliquer une opération logique (XOR par exemple) entre les deux bits

01000010 ⊕ 11111011 11010000 **10010111** = 11111011 11010000 11010101

- Tant qu'il existe des bits dans le message secret, passer au bit suivant du message secret et au pixel suivant de l'image

Stéganographie & stéganalyse

Comment détecter l'usage de la stéganographie dans X photos ?

- Réduire manuellement le jeu de photos (copie)
- Ne garder que les photos suspectes
- Vérifier que les photos suspectes contiennent une charge utile
- Détecter les points de modification de chaque fichier
- Déchiffrer et extraire la charge utile

Analyse de métadonnées

Des métadonnées peuvent être présentes dans les fichiers, les emails, les conversations réseaux, …

Une métadonnée, c'est :

- Un entête avec des informations
- Des informations souvent sous forme de données brutes (paquet réseau, musique, texte…)
- Utilisée dans des systèmes et des logiciels
- Une donnée technique utile pour une enquête

Analyse de métadonnées

Prenons l'exemple d'une photographie prise par un Canon …

Cryptographie & cryptanalyse

Qu'est-ce que la cryptographie ?

« Ensemble de techniques permettant de chiffrer des messages. »

Qu'est-ce que la cryptanalyse ?

« Science qui consiste à tenter de déchiffrer un message chiffré sans en posséder la clé de chiffrement. »

Qu'est-ce qu'un hash ?

- Fonction destructrice d'une chaîne de caractères
- Le risque de collisions entre deux hashs identiques est rare
- Pour tout hash, il existe au plus une chaîne de départ

Cryptographie & cryptanalyse

MD5 n'est plus inviolable.

Plusieurs solutions pour casser un hash MD5 :

- Cassage par dictionnaire
- Cassage par tables arc-en-ciel

Démonstration :

- http://www.md5.cz/
- Mot : motdepasse
- Hash : b6edd10559b20cb0a3ddaeb15e5267cc
- Durée avec le logiciel HashCodeCracker : environ 20 secondes

Cryptographie & cryptanalyse

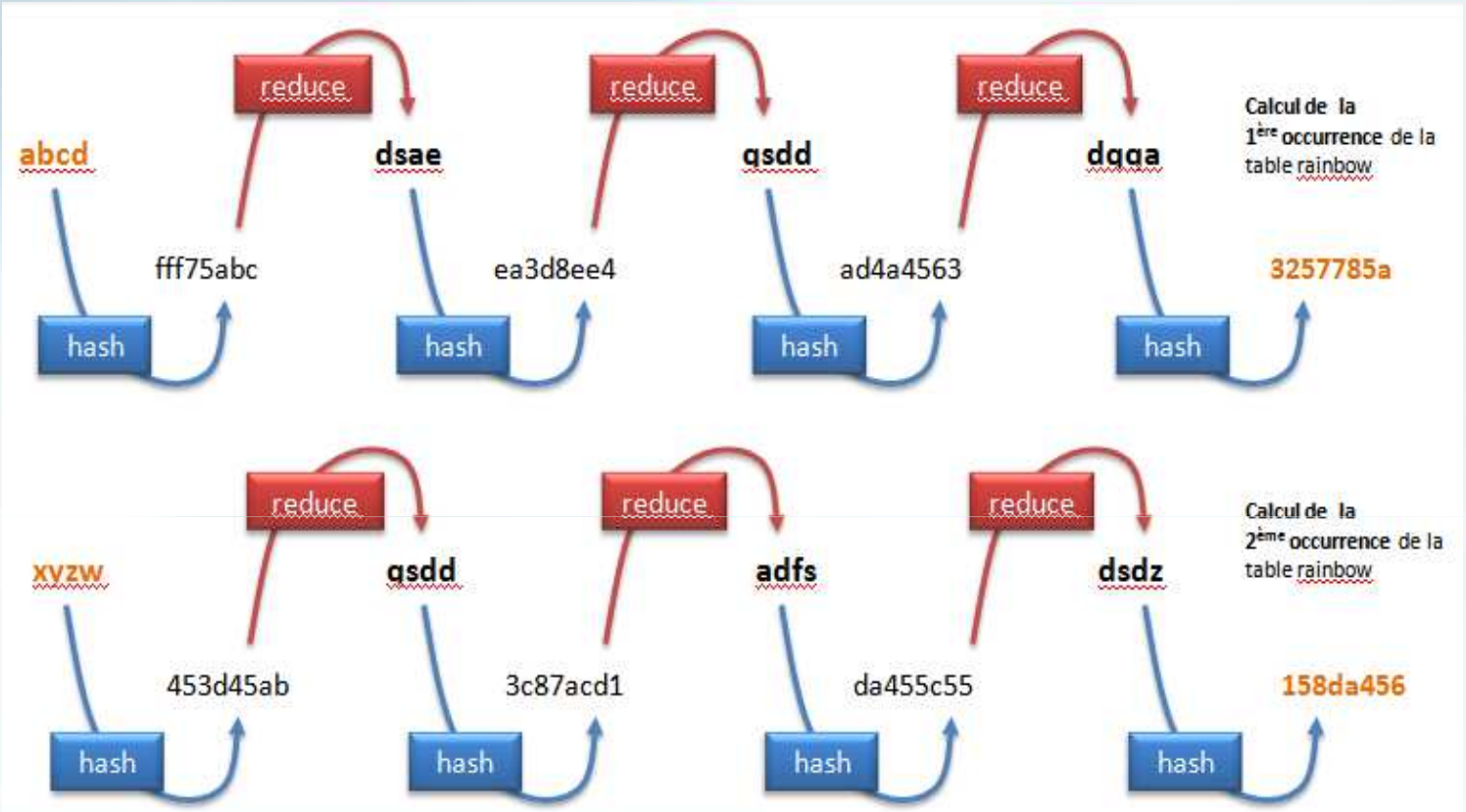
Attaque par dictionnaire :

- Simple à comprendre
- Simple à mettre en place
- Des dictionnaires existent partout sur Internet
- S'armer de patience et des bons dictionnaires

Attaque par table arc-en-ciel (Rainbow Tables) :

- Inventée par Philippe Oechslin en 2003
- Peu abordée dans notre formation
- Compromis entre temps de calcul et mémoire
- Nécessite une grande capacité physique
- Dispose de deux fonctions : hachage et réduction
- Consiste à précalculer des hashs pour obtenir les mots de passe

Cryptographie & cryptanalyse



Mot de passe	hash
abcd	3257785a
xyzw	158da456

Cryptographie & cryptanalyse

Inconvénients majeurs de cette technique :

- Risques de collisions des hashs
- Attaque par botnet

Solutions possibles sur le serveur :

- Saler les hashs de mots de passe
- Utiliser un algorithme de hachage lent
- Appliquer un temps de reconnexion exponentiel à chaque échec d'authentification
- Bloquer les connexions du botnet, faire un audit et remonter à la source
- Parfois, une phrase de poème apprise par cœur est plus efficace et difficile à déchiffrer qu'un mot de passe complexe

Contraintes légales

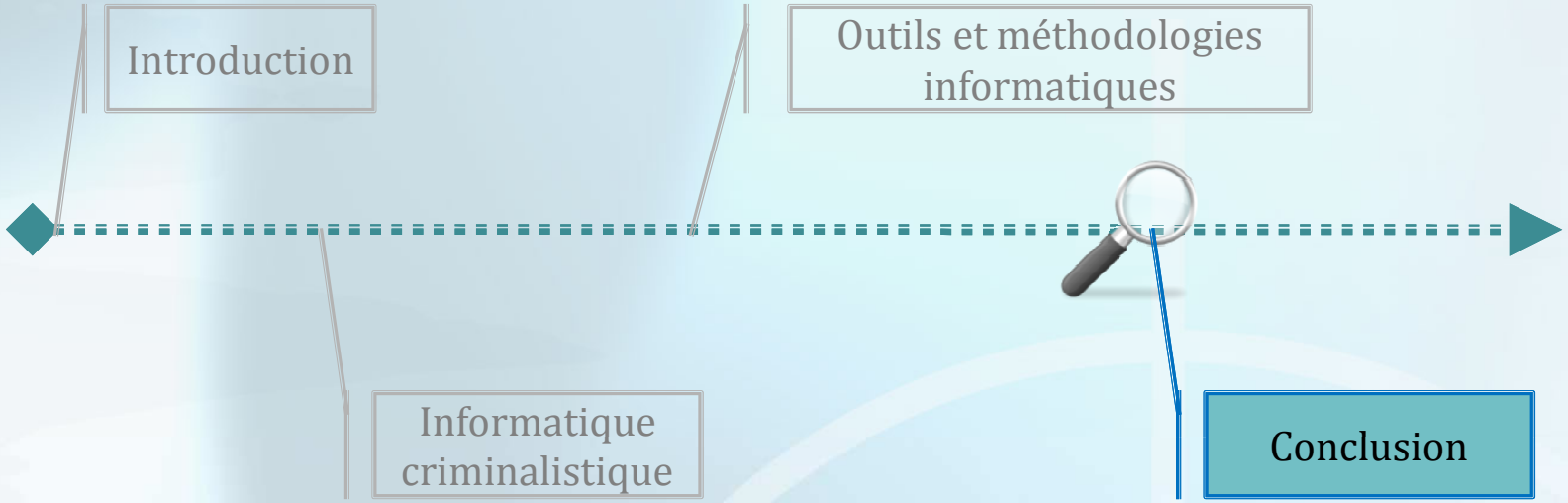
Les contraintes au regard de la loi :

- Puis-je lire un email ?
- Puis-je consulter les appels téléphoniques passés ?
- Puis-je obtenir une copie d'une facture téléphonique ?
- Puis-je consulter le contenu d'une archive chiffrée ?

Les contraintes au regard de la loi :

- Comment formuler le fait qu'on ait trouvé des documents compromettants illicites ou illégaux sur un ordinateur scellé lors d'une enquête ?

- Tout ce qui doit être affirmé doit être prouvé scientifiquement.


Introduction
Outils et méthodologies informatiques
Informatique criminalistique
Conclusion

CONCLUSION

Conclusion

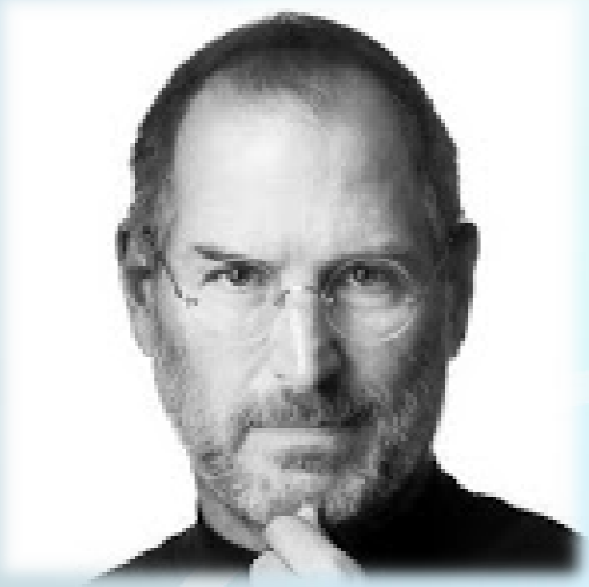
L'expert en informatique légale est un métier mêlant :

- informatique et contraintes légales
- Organisation humaine et matérielle
- Méthodologies et techniques d'expertise

C'est un travail humain éprouvant sur la résolution d'affaires criminelles.

Cette présentation est une infime partie d'un travail décrivant une science.

De nombreux domaines peuvent être abordés dans cet exposé à l'avenir : biométrie, anthropologie, psychologie criminalistique, ...



Merci de votre attention !

AVEZ-VOUS DES QUESTIONS ?

Sources

Culture :

http://fr.wikipedia.org/wiki/Expert_judiciaire
http://www.liste.pro/crimes-delits
http://www.biometrie-online.net/technologies/empreintes-digitales
http://www.prise2tete.fr/forum/viewtopic.php?id=10449
http://www.police-scientifique.com/organisation/inps
http://www.police-nationale.net/liste-des-laboratoires-de-la-police-scientifique/
http://policescientifique-role21.e-monsite.com/pages/content/historique-de-la-police-scientifique/
http://www.tueursenserie.org/spip.php?article60

Informations juridiques :

http://www.legalis.net/
http://www.legifrance.gouv.fr

Professionnels :

http://zythom.blogspot.fr

Sources

Logiciels & Systèmes :

http://www.ivizsecurity.com/blog/penetration-testing/live-cd-penetration-testing-pen/

http://www.deftlinux.net/

http://www.e-fense.com/products.php

http://www.kali.org/

http://ballistic.zdziarski.com/

Ressources gratuites :

http://icones.pro/

Autres ressources et crédits :

NCIS

Les experts

CSI

Dexter