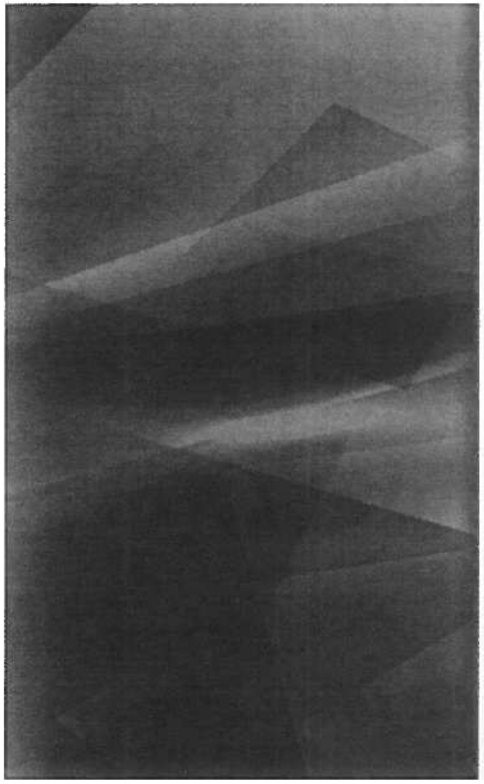


Recueillir les informations par Internet dans le contre terrorisme

De l'information à la preuve

Module 1 : la preuve numérique, principes fondamentaux

CEPOL

[redacted] – Maroc - 2019

« Finalement, ce que preuves matérielle et immatérielle ont en en commun, c'est bien la confiance. Quelle confiance accorder à la preuve immatérielle ? Comment accorder sa confiance à une preuve immatérielle ? A quel acteur du processus de réalisation d'une preuve matérielle accorder ou ne pas accorder sa confiance ? »

Yves Repiquet, bâtonnier de l'ordre des avocats, 21/11/2007 « La Justice à l'épreuve de la preuve immatérielle», débats à la maison du Barreau de Paris.

1) Information, preuve et vérité
2) Le principe de liberté de la preuve
3) Outils, méthodes et normes
4) Les acteurs de la preuve

Information, preuve et vérité

Donnée et information

- « *Ce qui est connu ou admis comme tel, sur lequel on peut fonder un raisonnement, qui sert de point de départ pour une recherche* » (Larousse)
- « *L'information est une indication, un renseignement, une précision que l'on donne ou que l'on obtient sur quelqu'un ou quelque chose* » (Larousse)
- Un fait ? Une vérité ?
  - Fiabilité (source, intégrité, ...)
  - Validité (crédibilité, légalité, ...)
  - Pertinence (intelligibilité, contexte, ...)

Un policier voleur

Un CRS surpris en train de voler un maillot de foot sur les Champs-Élysées ! (Vidéo)

Publié par [redacted] sur 17 Mars 2019, 10:46am

CRS, Paris, Gilets Jaunes

Gilets jaunes : un policier filmé rangeant des maillots du PSG dans un sac, l'IGPN saisie

ACTUALITÉS

L'IGPN saisie après une vidéo où un policier récupère des maillots du PSG sur les Champs-Élysées

franceinfo:

LADEPECHE.fr

Le Parisien

HUFFPOST

Acte XVIII à Paris : un CRS a-t-il profité de la manifestation pour piller la boutique du PSG ?

Un policier voleur, suite

facebook

[redacted] a partagé une publication
10 h
Incroyable !!!!
Afficher la pièce jointe

[redacted] Scandaleux horrifiant putains de force de l'ordre me répugne pourquoi ils agissent ainsi... Mr Macron et castaner ont ils une réponse???
J'aime · Répondre · 2 j

[redacted] a partagé une publication
3 h
Bravo messieurs, et après on met sur le dos des gilets jaunes. Tout les moyens sont bons

largement partagées accusent le premier policier d'avoir volé ces produits du PSG, et le second, auteur du coup de matraque, d'avoir voulu le couvrir.

Contactée par *CheckNews*, une source policière fait état d'images *«embarrassantes»*. La préfecture de police de Paris n'a pas fait de commentaire, indiquant seulement que l'inspection générale de la police

twitter

Un policier voleur, suite

Sollicitée par nos confrères de France Info la préfecture de police de Paris indique que l'Inspection générale de la police nationale (IGPN) a été saisie pour enquêter sur cette affaire. Alors que la CGT Police Ile-de-France ne souhaite pas polémiquer et dément formellement l'hypothèse d'un vol « il s'agit d'une procédure classique de collecte de pièces à conviction ».

"La situation sur place était chaotique. A tout moment ça pouvait dégénérer. Alors dans ces cas-là, on ramasse les objets comme on peut pour matérialiser l'infraction."

— Axel Ronde, secrétaire général VIGI Ile-de-France
à franceinfo

❌ FAKE NEWS / Durant l'#Acte18 des #GiletsJaunes, ce membre des #FDO 👮‍♂️ ne vole pas des maillots d'un magasin du #PSG : 👉 Il met dans un sac des vêtements volés par des casseurs qui ont été interpellés aux alentours & dans la boutique. facebook.com/brutofficiel/v...

Un policier voleur, suite

LCI

Selon nos informations, le policier mis en cause a rédigé un procès-verbal d'interpellation après cette scène. Dans ce PV, le policier indique avoir procédé à l'interpellation d'un individu qui tentait de s'échapper d'une boutique vandalisée sur les Champs-Elysées. Interpellation pour "vol en réunion avec dégradations", précise le policier, indiquant que cet homme, âgé d'une vingtaine d'années, avait les bras chargés de vêtements.

Au verso du procès-verbal, qui a été versé à l'enquête menée au commissariat du 10e arrondissement, l'agent interpellateur prend le soin de faire l'inventaire de toute la liste des objets ramassés et laissés échappés par le pilleur pendant l'interpellation. Le sac que l'on voit dans la vidéo est d'ailleurs un sac du PSG lui aussi volé. Selon nos informations, 18 articles sont décrits très précisément par le policier, avec à chaque fois la valeur de l'objet. Le préjudice est estimé à 2 004 €.

"Le sac et les affaires consignés ont ensuite été remis à l'officier de police judiciaire. C'est l'OPJ qui a pris ensuite le relais", souligne une source proche de l'enquête. Une enquête de l'IGPN a été ouverte. Selon nos informations, le policier n'aurait pas encore été entendu.

De la preuve à l'information ?

- « *La preuve est la démonstration de la réalité d'un fait, d'un état, d'une circonstance ou d'une obligation* » , dictionnaire juridique de Serge Braudo
- « La preuve est un *élément matériel qui démontre, établit, prouve la vérité ou la réalité d'une situation de fait ou de droit* », Larousse
- « La preuve est un *fait ou raisonnement propre à établir solidement la vérité* », Wikipédia
- « *Pour qu'elle soit crédible, la preuve doit résister à la discussion* », Patrick Matet, Magistrat à la Cour d'appel de Paris

Preuve et vérité

- La preuve vise t'elle la vérité ?
- « *utile à la manifestation de la vérité* », « *en vue de la manifestation de la vérité* » (code civil, code de procédure pénal, ...)
- La vérité absolue n'existe pas, c'est la croyance à cette vérité qui importe
- La notion de faisceau d'indice : la vérité judiciaire est une construction, pas une donnée
- Cette recherche de la vérité doit composer avec le respect des valeurs fondamentales (vie privée, dignité humaine, ...)

Le principe de liberté de la preuve

Le principe de liberté de la preuve

- ***Article 1358 du code civil***

« Hors les cas où la loi en dispose autrement, la preuve peut être apportée par tout moyen. »

- ***Article 1366 du code civil***

« L'écrit électronique a la même force probante que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité. »

- **Article 427 du code pénal**

« Hors les cas où la loi en dispose autrement, les infractions peuvent être établies par tout mode de preuve et le juge décide d'après son intime conviction.

Le juge ne peut fonder sa décision que sur des preuves qui lui sont apportées au cours des débats et contradictoirement discutées devant lui. »

Les principes fondamentaux

- « *La procédure pénale doit être équitable et contradictoire et préserver l'équilibre des parties* », article préliminaire al 1, code de procédure pénale
- Le principe de légalité
  - Respect de droits de la défense
  - Interdiction des modes de preuve contraires à la dignité humaine
  - Interdictions des moyens déloyaux
- L'exception majeure : le recours à des preuve déloyales voire illégales par une partie
- Le principe de nécessité
- Le principe de proportionnalité des moyens
- Le principe du contradictoire

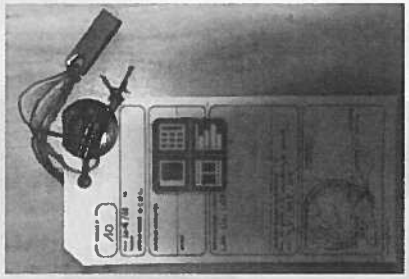
Les principes fondamentaux (suite)

- L'authenticité de la preuve
  - L'origine de la preuve (chain of custody)
  - L'intégrité de la preuve (absence d'altération et répétibilité)
- Existe t'il une hiérarchie des preuves ?
  - De la simple carte postale à l'acte notarié, du témoignage au rapport d'expertise
  - Tout acte de procédure n'a que valeur d'information pour le juge
  - L'intime conviction est humaine
    - Ce qui semble avoir de la valeur
    - Un diplôme, le respect d'une méthodologie connue, une jolie présentation, ...

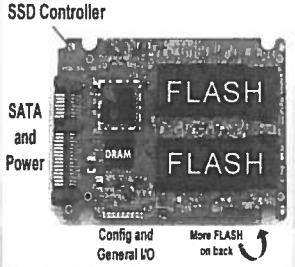
La vulnérabilité de la donnée numérique

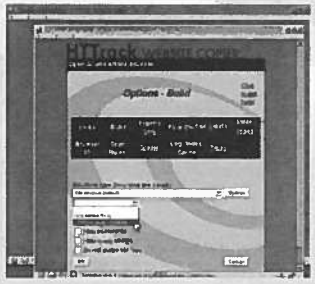
- Toutes les preuves sont falsifiables et fragiles... mais...
- La donnée numérique est très fragile
  - Volatilité de la donnée
  - Évolutivité des technologies
- La donnée numérique est très malléable
  - Facilement copiable (reproduction de preuve)
  - Facilement modifiable (falsification de preuve)
  - Facilement effaçable (destruction de preuve)
- La donnée numérique est incompréhensible au non initié
  - Qui comprend l'hexadécimal ?
  - Existe t'il un expert couvrant tous les domaines de l'investigation numérique ?

La donnée est-elle protégée ?

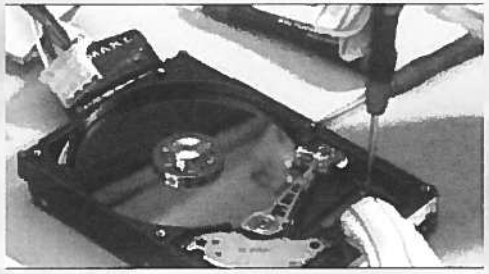


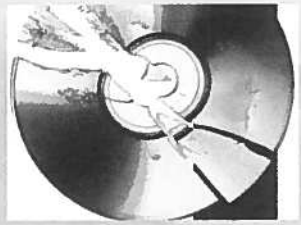
La donnée est-elle protégée ?



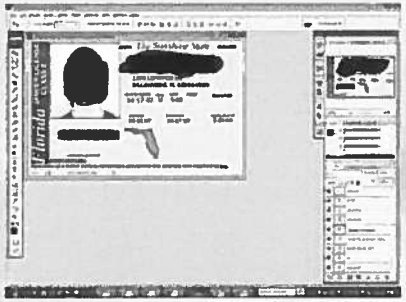


La donnée est-elle toujours accessible ?

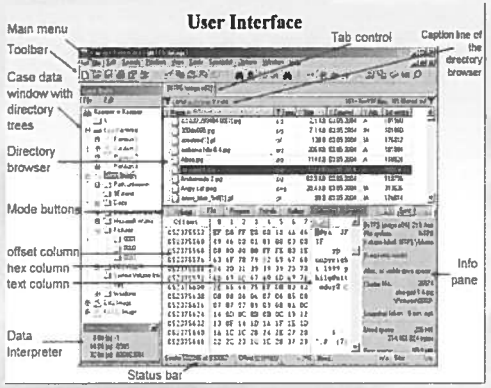


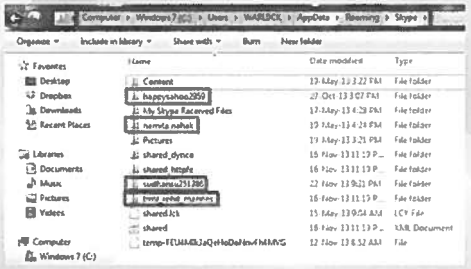


La donnée est-elle fiable ?



La donnée est-elle compréhensible ?





Outils, méthodes, normes

Les outils sont-ils fiables ?

- Outils gratuits et outils payants ?
- Outils à tout faire et outils dédiés ?
- Outils pour experts et outils « facilités »
- Outils « fait maison »
- Comment tester un outil ?

Trouver un outil d'analyse numérique ?

https://toolcatalog.nist.gov/index.php

https://www.dftools catalogue.eu/dftc. home.php

Les outils sont-ils fiables ?

Popular Computer Forensics Top 21 Tools [Updated for 2019]

Tool	Rank
Digital Forensics Framework	1
Open Computer Forensics	2
CAINE	3
XWAYS Forensics	4
Encase	5
Registry Recon	6
The Sleuth Kit	7
Libforensics	8
Volatility	9
WindowsSCOPE	10
etc...	11

https://resources.infosecinstitute.com/computer-forensics-tools/#gref

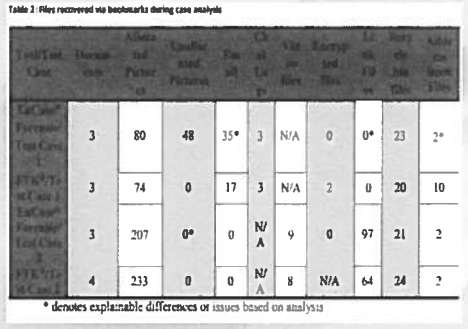
7 Best Computer Forensics Tools [Updated 2019]

Tool	Rank
SANS SIFT	1
Pro Discover Forensic	2
Volatility Framework	3
The Sleuth Kit (+Autopsy)	4
CAINE	5
Xplico	6
Xways Forensics	7
Etc...	8

https://resources.infosecinstitute.com/7-best-computer-forensics-tools/#gref

Les outils sont-ils fiables ?

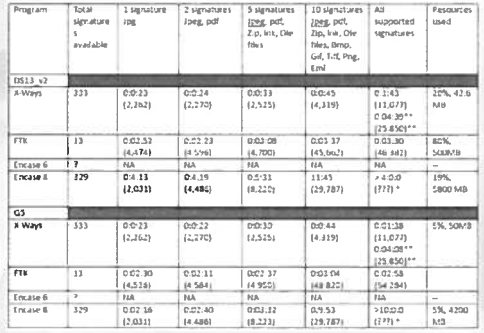
Quelques tests de récupération de données



3	80	48	35*	3	N/A	0	0*	23	2*
3	74	0	17	3	N/A	2	0	20	10
3	207	0*	0	N/A	9	0	97	21	2
4	233	0	0	N/A	8	N/A	64	24	2

* denotes explainable differences or issues based on analysis

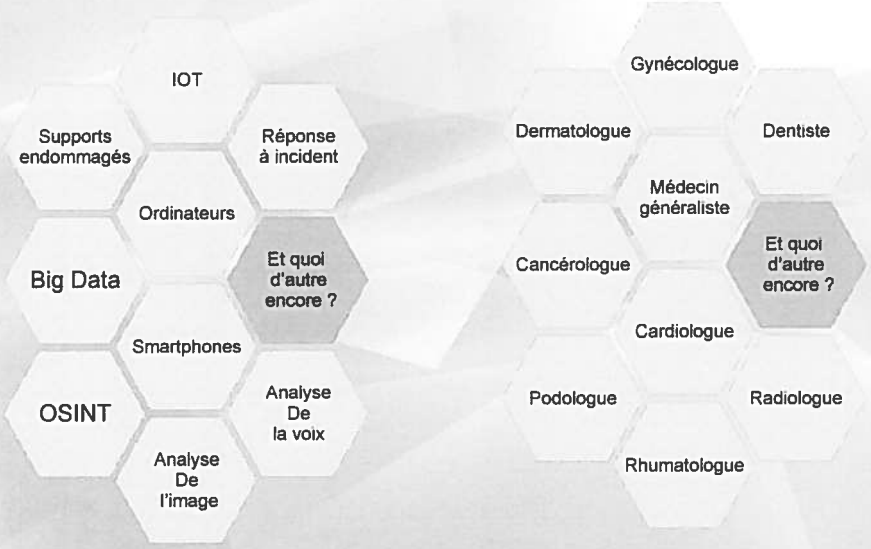
https://www.marshall.edu/forensics/files/CERVELLONEADAM_FinalResearchPaper-8-7-2015_-1.pdf



Program	Total signature s available	1 signature /jpg	2 signatures /jpeg, pdf	5 signatures /jpeg, pdf, Zip, lnk, Ole files	10 signatures /jpeg, pdf, Zip, lnk, Ole files, Bmp, Gif, Tif, Png, Eml	All supported signatures	Resources used
DS13_v2							
X-Ways	223	0:0:23 (2,262)	0:0:24 (2,270)	0:0:33 (2,525)	0:0:45 (4,319)	0:1:43 (11,077) 0:04:39** (25,650)**	10%, 42.6 MB
FTK	13	0:02:52 (4,474)	0:02:23 (4,596)	0:03:08 (4,700)	0:03:37 (45,942)	0:03:30 (46,982)	80%, 568MB
Encase 6	?	NA	NA	NA	NA	NA	--
Encase 8	329	0:4:13 (2,031)	0:4:16 (4,486)	0:5:31 (8,220)	13:43 (29,787)	> 4:0:0 (777) *	19%, 5800 MB
G5							
X-Ways	333	0:0:23 (2,262)	0:0:22 (2,270)	0:0:30 (2,525)	0:0:44 (4,319)	0:01:38 (11,077) 0:04:06** (25,650)**	5%, 50MB
FTK	13	0:02:30 (4,516)	0:02:11 (4,584)	0:02:37 (4,950)	0:03:04 (48,822)	0:02:58 (54,294)	
Encase 6	?	NA	NA	NA	NA	NA	--
Encase 8	329	0:02:16 (2,031)	0:02:40 (4,486)	0:03:32 (8,233)	0:9:53 (29,787)	>10:0:0 (777) *	5%, 4200 MB

https://binaryforay.blogspot.com/2016/09/let-benchmarks-hit-floor-autopsy-vs.html

Les domaines de l'investigation numérique



Diplômes et certifications

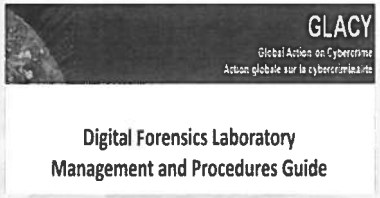
Job board search results (in alphabetical order, by certification)*

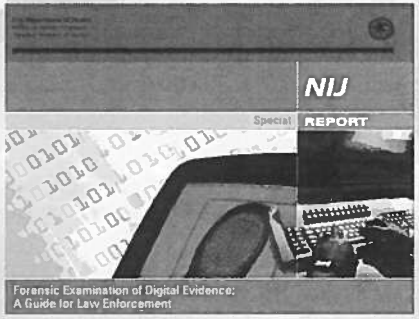
	SimplyHired	Indeed	LinkedIn Jobs	LinkUp	Total
Vendor neutral					
CFCE (IACIS)	65	82	117	46	308
CHFI (EC-Council)	106	140	255	68	567
GCFA (SANS GIAC)	477	489	857	294	2,062
GCFE (SANS GIAC)	203	226	433	143	1,005
Vendor specific					
ACE (AccessData)	25	29	31	12	97
EnCE (EnCase)	110	154	237	114	615

https://www.businessnewsdaily.com/10755-best-digital-forensics-certifications.html

- Quel prix ?
- Quelle notoriété ?
- Quelle durée de validité ?
- Couvrant quel domaine de compétence ?
- Formations métier ou formations outil ?
- La place donnée à l'expérience ?

Les guides méthodologiques





Les normes ISO/IEC

- ISO : norme définie par l'Organisation Internationale de Normalisation
- Standards et certification
- Réévaluation tous les 5 ans
- Quels impacts et à quels coûts ?
- ISO/CEI 17025 : laboratoires d'étalonnage et d'essai
- ISO/CEI 27k : 70 normes relatives à la sécurité des systèmes d'information (https://www.iso27001security.com/html/iso27000.html)
- ISO /CEI 27037 (2015) : Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuves numériques.
- Certification, coût et opposabilité… quels risques ?

Les acteurs de la preuve

Expert ou policier ?

Expert ou policier ?

- **57-1 CPP, extrait :**

  «... Les officiers de police judiciaire ou, sous leur responsabilité, les agents de police judiciaire peuvent, au cours d'une perquisition effectuée dans les conditions prévues par le présent code, accéder par un système informatique implanté sur les lieux où se déroule la perquisition à des données intéressant l'enquête en cours et stockées dans ledit système ou dans un autre système informatique, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial... »

- **60 CPP, extrait :**

  « ...S'il y a lieu de procéder à des constatations ou à des examens techniques ou scientifiques, l'officier de police judiciaire ou, sous le contrôle de ce dernier, l'agent de police judiciaire a recours à toutes personnes qualifiées... »

- ***Article 156 CPP, extrait :***

  « Toute juridiction d'instruction ou de jugement, dans le cas où se pose une question d'ordre technique, peut, soit à la demande du ministère public, soit d'office, ou à la demande des parties, ordonner une expertise... »

Le policier expert

- *L'expert est celui qui a acquis une grande habilité par l'expérience, par la pratique* (Larousse)
- *L'expert est un spécialiste habilité auprès d'un tribunal ou d'une instance quelconque à émettre un avis sur une question exigeant des connaissances spéciales.* (Larousse)
- Il doit s'agir d'une activité accessoire, l'exercice d'une activité principale étant la base du niveau de compétence de l'expert.
- Article 156 et suiv du CPP et la loi n° 71-498 du 29 juin 1971
- *Toute juridiction d'instruction ou de jugement peut désigner un expert. Celui-ci est choisi sur sur la liste nationale dressée par la Cour de cassation ou sur une des listes dressées par les cours d'appel dans les conditions prévues par la loi précitée. A titre exceptionnel et sur décision motivée, un expert non inscrit peut être choisi. Il devra alors prêter serment d'accomplir ses mission, de faire son rapport et de donner son avis en son honneur et conscience.*
- L'expertise ne peut porter que sur l'examen de questions d'ordre technique.

Le policier expert (suite)

- L'expert doit notamment :
  - être indépendant (Civ. 1re, 6 juill. 2000, n°97-21.404), sous peine de nullité (Crim. 8 juin 2006, 06-81.359).
  - justifier de compétences reconnues pour exercer ou avoir exercé pendant un temps suffisant une profession ou une activité en rapport avec sa spécialité, et dans des conditions coférant une qualification suffisante (article 2 du Décret n°2004-1463 du 23 décembre 2004).
  - à l'issue de son travail rédiger un rapport contenant la description des opérations ainsi que ses conclusions.
- L'expert est habilité notamment à :
  - ouvrir et à reconstituer un scellé
  - travailler hors la présence du propriétaire du support numérique visé par l'expertise

Le policier expert (suite)

- L'expert doit notamment :
  - être indépendant (Civ. 1re, 6 juill. 2000, n°97-21.404), sous peine de nullité (Crim. 8 juin 2006, 06-81.359).
  - justifier de compétences reconnues pour exercer ou avoir exercé pendant un temps suffisant une profession ou une activité en rapport avec sa spécialité, et dans des conditions coférant une qualification suffisante (article 2 du Décret n°2004-1463 du 23 décembre 2004).
  - à l'issue de son travail rédiger un rapport contenant la description des opérations ainsi que ses conclusions.
- L'expert est habilité notamment à :
  - ouvrir et à reconstituer un scellé
  - travailler hors la présence du propriétaire du support numérique visé par l'expertise

Le policier expert (suite)

- Note DCPJ 9685 du 30 avril 2008 : les ESCI/ICC n'ont en général pas vocation à réaliser des expertises, missions réservées aux services centraux mais que celles-ci demeurent pourtant possible à titre exceptionnel si elles respectent les règles suivantes :

  (extrait)

  - l'expertise est un acte de service
  - la demande d'expertise doit être présentée au chef de service qui en apprécie le bien fondé.
  - le chef de service indique au magistrat le nom du fonctionnaire à même de remplir la mission **après s'être assuré que celui-ci n'a participé en amont, en aucune façon, à l'enquête dans laquelle l'expertise trouve son origine**
  - le rapport est signé du seul expert, et ne doit pas être établi sur papier à en-ête du service
  - le transmission du rapport est assurée par le chef de service et ne saurait intervenir sous couvert de la voie hiérarchique

Le policier personne qualifiée

- Base légale : la personne qualifiée est visée aux articles 60, 60-3, 77-1, 77-1-3 et 99-5 du code de procédure pénale. Elle peut, sur réquisition d'un officier de police judiciaire, procéder :
  - à des examens techniques ou scientifiques (60, 77-1 CPP)
  - et/ou à une copie de données dont le support a été placé sous scellé (60-3, 77-1-3 et 99-5 CPP)
- La personne qualifiée doit :
  - Si elle n'est pas inscrite sur les listes d'expert (157 CPP), prêter serment par écrit, d'apporter son concours à la justice en son honneur et sa conscience.
  - dresser l'invetaire du contenu du scellé
  - dresser un rapport de ces opérations
- La personne qualifiée peut :
  - agir hors présence du propriétaire du support numérique.
  - briser un scellé et le reconstituer le scellé à l'issue
  - Communiquer oralement ses conclusions aux enquêteurs en cas d'urgence

Le policier personne qualifiée

- Jurisprudence :
  - Crim 14/09/2005 : *les missions techniques confiées à une personne qualifiées sont de même nature que celles qui peuvent être confiées à un expert.*
  - Crim 04/11/1987 : *les mesures techniques qui ont pour objet la recherche et la constatation ne présente pas le caractère d'une expertise, d'où le cantonnement à des questions d'intérprétations technique.*
- *Le policier ICC personne qualifiée :*
  - *Est titulaire de la qualification ESCI ou ICC*
  - *Est compétence uniquement pour ce qui relève de sa formation*
  - *Est indépendant au regard de la procédure et donc n'avoir participé en amont, en aucune façon, à l'enquête dans laquelle la réquisition trouve son origine.*
  - *doit prêter serment par écrit, d'apporter son concours à la justice en son honneur et sa conscience.*

Des questions ?

Recueillir les informations par Internet dans le contre terrorisme

De l'information à la preuve

Module 2 : preuve numérique et support numérique

[redacted] – Maroc - 2019

FBI Computer Analysis and Response Team (CART)

1) Quels supports ?

2) Les phases de l'exploitation

3) Focus sur la collecte (hash, copie, original)

4) L'analyse ?

Quels supports ?

Quels supports numériques ?

- Systèmes de stockage numériques utilisés dans les ordinateurs tels que les disques durs, clés USB, disquettes, disques optiques, etc.
- Supports mobiles tels que les téléphones, smartphones, tablettes tactiles, cartes mémoire, etc.
- Systèmes de navigation de type GPS
- Systèmes numériques de photographies et de vidéo
- Ordinateurs classiques avec connexion réseau
- Systèmes de réseau et appareils associés
- Objets connectés tels que véhicules connectés, appareils de domotique connectés, etc.

Support et donnée

- Tout système de stockage contenant de la donnée numérique et accessible physiquement au spécialiste
- 57-1 CPP extrait : *« ...accéder par un système informatique implanté sur les lieux où se déroule la perquisition à des données intéressant l'enquête en cours et stockées dans ledit système... »*
- Par opposition aux données contenues dans des systèmes de stockage non accessibles physiquement au spécialiste autrement que par un réseau
- 57-1 CPP extrait : *«...données intéressant l'enquête en cours et stockées ...dans un autre système informatique, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial… »*

Les phases de l'exploitation

Les phases de l'exploitation

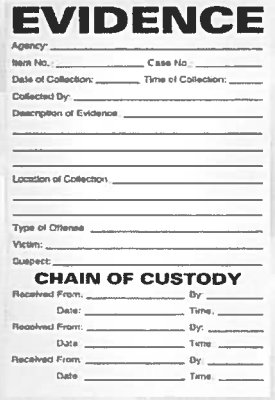
Prise en comte de la mission

- Quelques pistes pour prendre en compte une mission :
  - Le bon interlocuteur
  - Le contexte du dossier
  - Le cadre juridique
  - L'objet de la mission
  - La préparation (matériel, briefing, ...)
- La présence du primo intervenant ou du spécialiste dans la phase d'identification est-elle nécessaire ?
  - L'importance du numérique dans la mission ?
  - Du support facilement identifiable aux supports dissimulés ou maquillés
  - Ah bon, ça aussi cela contient de la donnée ?

Identification

Identification et attribution

- A qui appartient le support original ?
- Quel sera le parcours du scellé, depuis sa saisie jusqu'à sa présentation au procès pénal
- La chaîne de la preuve (chain of custody)
- Et si le scellé n'est pas intègre quand il arrive à l'expert ?
- Et si l'objet est endommagé ?
- Et si l'examen des données démontre un accès postérieur à la saisie et non référencé en procédure?



EVIDENCE

Agency: _____

Item No.: _____ Case No.: _____

Date of Collection: _____ Time of Collection: _____

Collected By: _____

Description of Evidence: _____

Location of Collection: _____

Type of Offense: _____

Victim: _____

Suspect: _____

CHAIN OF CUSTODY

Received From: _____ By: _____

Date: _____ Time: _____

Received From: _____ By: _____

Date: _____ Time: _____

Received From: _____ By: _____

Date: _____ Time: _____

Préservation

- De la protection de la scène de crime à la protection de la preuve numérique
- Le scellé : inviolabilité, inaltérabilité
- Le scellé numérique
  - Plus aucun accès possible à la donnée physiquement
  - Plus aucun accès possible à la donnée via un réseau
  - Les supports magnétiques et les risques de destruction
- Maintien en tension et méthodes de déverrouillage
- Documenter, documenter, documenter…

Focus sur la collecte (hash, copie, original)

Collecte

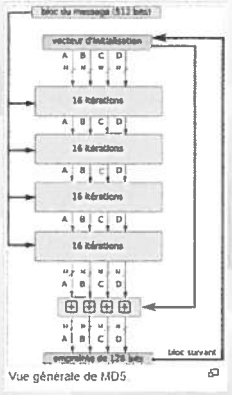
- La répétabilité : Un investigateur doté du savoir-faire requis doit être en mesure d'obtenir le même résultat qu'un autre investigateur doté d'un savoir-faire similaire, travaillant dans des conditions similaires
- La sacro sainte copie
  - Copie physique
    - Format brut ou sans compression (raw, dd, dmg)
      - Taille
      - Altérabilité
    - « expert witness format » (E01, AFF4,...)
      - Compression
      - Log de hash inclu
  - Copie logique
    - Altérabilité

La fonction de hachage

- Fonction de hachage, calcul de hash, somme d'intégrité, condensat, ...
- Calculer une empreinte numérique à partir d'une donnée

$$\forall (x, y) \in S^2, r_o(x, y) \Rightarrow r_o(f(x), f(y))$$

- Au moindre changement de la donnée, le hash sera différent
- S'applique à :
  - Une suite de caractère comme un mot
  - Un fichier
  - Une partition
  - Un volume de stockage complet



Vue générale de MD5

Fonction de hachage (suite)

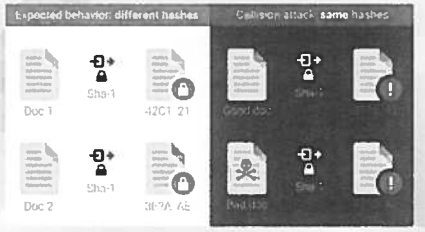
- Formats multiples

Message original	MD4	MD5	SHA-1
Zeste de savoir	7096e36e73cf1a30cd28b603bfb88226	2c598f7a0d3f68686e417ee1ff8aa152	b90f6190fa742e60e93971ee9c4a0764b9de9b8f
Zeste de savoire	52d43d8cf1b544ba65b3fd5d7db2907a	734ad14eea9d911ba6cf2aa4f020b8da	b78d3b92624f0cb684474cb5b8511403dace4b79
Roger le tavernier	4ef1e80cfa57834cc856b9787970ce7e	ff9e99da9c27f04e07d9298a7547885f	26d352c29085348a163728def59253d63ba449ce

- A quoi ça sert ?
  - Vérifier un fichier téléchargé
  - Vérifier si un fichier est présent au milieu de 100 000 autres ?
  - Vérification de mot de passe sans tous les stocker en clair
  - Vérifier si la copie est identique à l'original
  - Etc.
- Combien de temps ?

Fonction de hachage (suite)

- La gestion des erreurs
  - Si le support physique est défectueux à l'origine ?
  - Si la panne ou le crash d'un bloc intervient entre deux phases de vérification ?
  - Le hash par bloc ?
- Les collisions
  - La fonction de résistance à la collision
  - La probabilité de collision
  - MD5 : 1ère collision en 1996
  - SHA1 : collision officielle en 2017, mais suspicions depuis 2011
  - Associer deux calculs de hash en vérification de copie ?



Copie et SSD

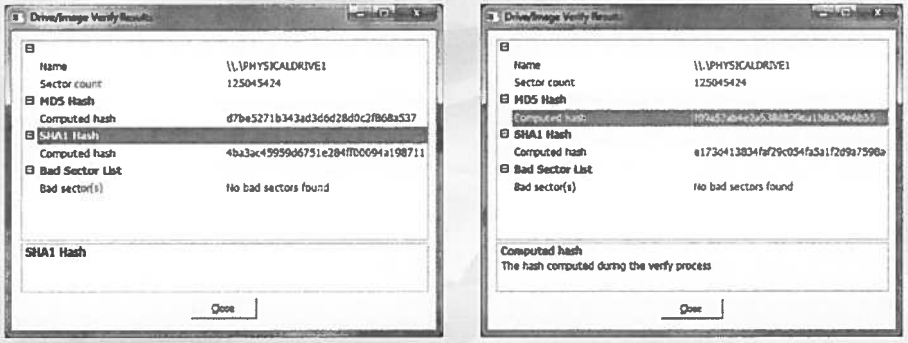
- Plus rapide, plus résistant, moins encombrant
- La mémoire flash
  - Je n'écris pas si ce n'est pas propre, donc je nettoie dès que j'ai un moment de libre (fonction TRIM)
  - J'utilise prioritairement les blocs vides et les moins utilisés car mes cellules ont une fin de vie (le garbage collector)
- La fin de la récupération de données effacées ?
- La fin de la vérification par calcul de hash ?

Copie et SSD

- Plus rapide, plus résistant, moins encombrant
- La mémoire flash
  - Je n'écris pas si ce n'est pas propre, donc je nettoie dès que j'ai un moment de libre (fonction TRIM)
  - J'utilise prioritairement les blocs vides et les moins utilisés car mes cellules ont une fin de vie (le garbage collector)
- La fin de la récupération de données effacées ?
- La fin de la vérification par calcul de hash ?

Copie et SSD

Deux hash générés sur un même support, à une heure d'intervalle



Copie, mémoires soudée et chiffrement

- Les mémoires soudées :
  - Développement des portes ultra transportables
  - Copie logicielle (Paladin, Darwin, …)

- Le chiffrement
  - Bitlocker, Filevault, …
  - Mac : fusion drive, chip t2, … (avant les solutions)

- Quid si le spécialiste forensics n'a pas le bon équipement à l'instant T ?

Copie et support mobile

- Exit les règles sacrées de l'analyse numérique ?
- L'impossibilité d'accéder à la donnée d'une manière forensique
  - Copie logique
  - Back up
  - Méthode agent
  - Downgrade apk
  - Etc.
- Des outils automatisés
- Les logs d'activité
- Cip off et JTAG

MSAB XRY XAMN

OXYGEN FORENSICS

Belkasoft

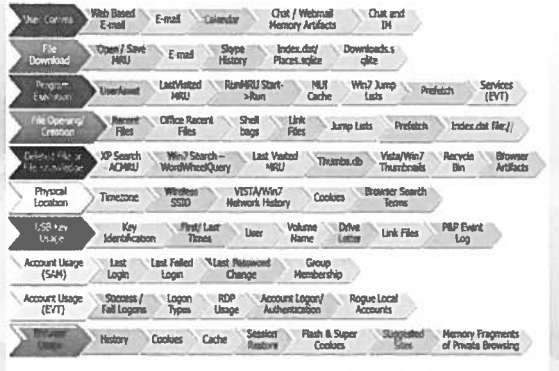
Travailler sur l'original

- C'est mal…
- Les bloqueurs en écriture
  - Logiciels ou matériels ?
  - Différentes connectiques
  - Accès externe ou interne (shadow3)
  - Oui mais les SSD alors ?
  - Oui mais les supports mobiles ?
- C'est mal… mais on le fait… et souvent !

L'analyse ?

L'analyse

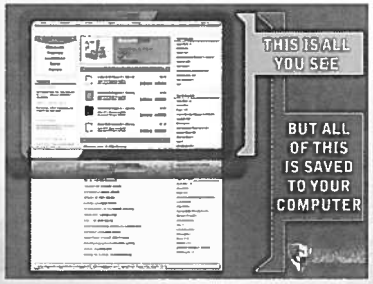
- Données présentes
  - Accessibles ?
  - Humainement intelligibles ?
  - Méta données
  - Données système
- Données effacées
  - Complètes
  - Incomplètes
  - Corrompues



https://digital-forensics.sans.org/blog/2012/01/25/digital-forensic-sifting-colorized-super-timeline-template-for-log2timeline-output-files/

- Données bien documentées et données complexes

L'analyse



- Le problème, c'est :
  - La masse d'information
  - Le temps
  - Savoir ce que l'on cherche
  - Ne pas passer à côté…
- Le meilleur expert du monde peut toujours passer à côté d'une donnée
- Discrimination, analyse rapide et expertise
- *Rendez-vous au module « Compte rendu d'analyse » pour aller plus loin…*

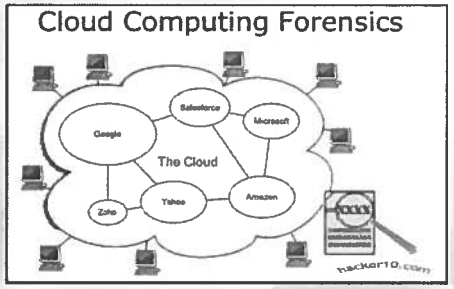
Des questions ?

Recueillir les informations par Internet dans le contre terrorisme

De l'information à la preuve

Module 3 : preuve numérique et données stockées à distance

[redacted] · Maroc - 2019



1) Législation

2) Cloud et forensique

3) Focus sur un outils automatisé

La législation

Opérateurs privés et données de trafic

- L'accès le plus simple à la donnée stockée à distance : requérir l'opérateur qui la détient
- Convention de Budapest, article 18 – Injonction de produire
- France, 60-1, 77-1-1 et 99-3 CPP (accès aux documents) et 60-2 al1, 77-1-2, 99-4 al1 CPP (communication d'information)
- Jurisprudence : arrêt du 6 novembre 2013 dit Ciprelli (Crim., 6 novembre 2013, n° 12-87.130)
  - *communication, sans recours à un moyen coercitif,*
  - *hors le contenu des correspondances échangées,*
  - applicable aux sociétés étrangères : « *ladite société restant, dans ce cas, libre de ne pas y répondre* »

Opérateurs privés et données de contenu

- Réquisitions aux fin de préservation du contenu, articles 60-2 alinéa 2 (enquête de flagrance), 77-1-2 alinéa 2 (enquête préliminaire) et 99-4 alinéa 2 (information judiciaire)
- Production du contenu sur autorisation du juge des libertés et de la détention requis par le Procureur de la République, ou sur autorisation du juge d'instruction
- Ce régime s'explique par le caractère attentatoire à la vie privée de cette réquisition.
- Hors cas de menace imminente grave sur l'intégrité physique d'une personne, les données avancées et les données de contenu ne peuvent être obtenues que sur la base d'une demande d'entraide.

Interception des données

- Données de trafic : Convention de Budapest, article 20 - Collecte en temps réel des données relatives au trafic
- Données de contenu : Convention de Budapest, article 21 – Interception de données relatives au contenu
- Interception de correspondance en France : criminalité organisée et terrorisme, articles 706-95 et 74-2 du code de procédure pénale (flagrance et préliminaire), et articles 100 à 100-7 et 80-4 (commission rogatoire)
- Conversations émises depuis la France vers l'étranger ou depuis l'étranger et entrant en France (Crim., 1er février 2011, n° 10-83.523).
- Interception à l'étranger sur demande d'entraide internationale uniquement (Crim., 27 juin 2001, n° 01-81865).

Les correspondances stockées

- Criminalité organisée et terrorisme, sur autorisation du juge des libertés et de la détention (article 706-95-1 CPP)
- *« ...accès, à distance et à l'insu de la personne visée, aux correspondances stockées par la voie des communications électroniques accessibles au moyen d'un identifiant informatique... »*
- Obtention préalable d'un couple identifiant/mot de passe

USA, le Cloud Act

- Le *Stored Communications Act* de 1986
  - Obligation d'une demande d'entraide judiciaire internationale, fondée sur des traités bilatéraux (MLAT)
  - Issu des suggestions de la Convention de Budapest sur les traités bilatéraux
- Modifié par le *Cloud Act* du 23 mars 2018
  - FBI vs Microsoft, compte Outlook stockée en Irlande
  - Communication des *"contenus de communications électroniques et tout enregistrement ou autre information relatifs à un client ou abonné, ...* [qu'ils] *soient localisés à l'intérieur ou à l'extérieur des Etats-Unis".*
  - Sans que la personne "ciblée" ou que le pays où sont stockées ces données n'en soient informés.

Europe, le règlement « E-evidence »

- Texte proposé par la Commission Européenne le 17 avril 2018
- Une riposte au Cloud act ?
- L'injonction européenne de production :
  - permettre à une autorité judiciaire d'un Etat membre de demander des preuves électroniques directement auprès d'un prestataire offrant des services dans l'Union et établi ou représenté dans un autre État membre, indépendamment de la localisation des données
  - délai de 10 jours, et dans les 6 heures en cas d'urgence (contre 120 jours pour la décision d'enquête européenne existante ou 10 mois pour une procédure d'entraide judiciaire)
- L'injonction européenne de conservation
- Obliger les sociétés proposant un service dans l'Union à avoir un représentant légal dans l'Union

Données publiques

- Donnée publique ou privée ?
  - Accessible à tous, sans condition
  - A l'exclusion de tout espace de discussion nécessitant une inscription ?
    - Forum sur Internet
    - Conversation ou fil de discussion (Telegram par exemple)
- Préserver l'intégrité de la preuve, Cour de cassation, 8 janvier 2019, N° de pourvoi: 18-80748
  - *« le constat d'huissier sur internet doit répondre à des règles techniques garantissant sa fiabilité et sa force probatoire, afin d'éviter que le matériel utilisé ne vienne interférer avec le contenu du site internet sur lequel il est effectué »*

Données publiques

- Vider le cache du navigateur de l'ordinateur afin d'éviter qu'un site qui aurait été préalablement visité ne conserve dans l'ordinateur de constatations des images ou données qui auraient été changées par la suite.
- Supprimer l'ensemble des cookies, les fichiers temporaires et l'historique de navigation avant les constatations.
- Horodater son intervention (pour assurer le suivi ultérieur des actions de l'enquêteur).
- Sauvegarder la page internet où sont réalisées les constatations
  - au format html
  - avec des copies d'écran
  - « outil capture » intégré à Windows depuis 7
  - Utiliser un outil dédié ? (Forensic Acquisition of Websites, Single file sous Firefox, HTTrack,...)

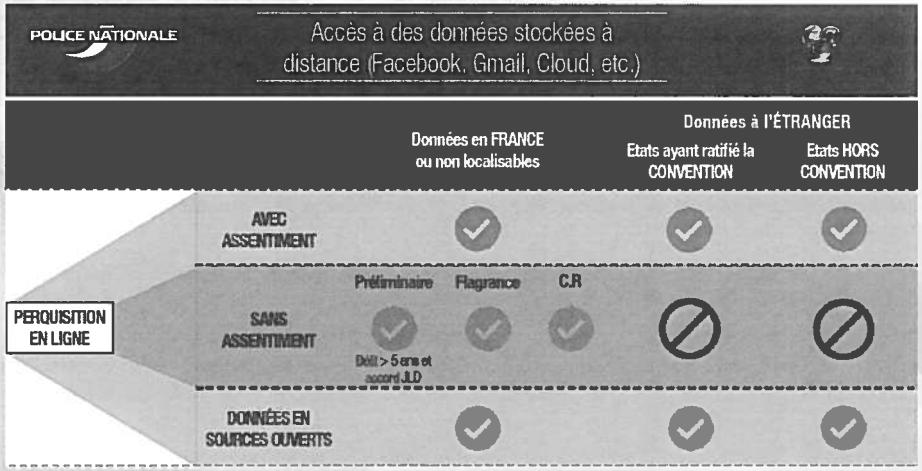
Enquête sous pseudonyme

- France : l'extension du régime avec l'article 230-46 créé par la loi du 23 mars 2019
- Infractions visées : les crimes ou délits punis d'une peine d'emprisonnement et commis par voir de communication électronique
- Enquêteurs habilités et affectés dans des services spécialisés
- Actes autorisés :
  - *Participer à des échanges électroniques, y compris avec les personnes susceptibles d'être les auteurs de ces infractions ;*
  - *Extraire ou conserver par ce moyen les données sur les personnes susceptibles d'être les auteurs de ces infractions et tout élément de preuve*
  - *Après autorisation du procureur de la République ou du juge d'instruction saisi des faits, acquérir tout contenu, produit, substance, prélèvement ou service, y compris illicite, ou transmettre en réponse à une demande expresse des contenus illicites.*

Données stockées à distance et supports numérique

- France : 57-1 CPP
  - Pendant la perquisition, accès aux données accessibles depuis le système initial
  - De retour au service, dans le respect des règles de la perquisition, accès accessibles depuis le système initial
  - S'il est avéré que les données sont stockées à l'étranger, respect des règles internationales.
- Europe : Convention de Budapest, article 32
  - Accès aux données stockées dans un autre Etat partie, avec le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique.

Synthèse



Cloud et forensique

Cloud et règles forensiques

- Le stockage est différent
  - pas d'accès direct à la donnée, pas de container physique exploitable, de localisation classique forensique avec offset ou 1er secteur.
  - Uniquement des containers logiques qui sont téléchargés
  - accès uniquement via les API et le scraping
- La méthodologie est différente
  - pas de comparaison possible entre l'original et la copie quand on fait un backup de type Google takeout
  - les données peuvent varier en fonction du mode de copie/extraction (taille d'une image via une capture écran ou un backup)
  - pas de contrôle total de la procédure de copie extraction quand elle est proposée par le cloud service

Cloud et règles forensiques

- les fichiers n'ont pas toujours de métadonnées complètes (auteur, appareil de prise de vue, etc.)
- certains horodatages disparaissent (mactime) ou sont modifiés (par défaut, l'horodatage d'une donnée est fourni en local time)
- difficultés d'attribution : synchronisation de certains services sur plusieurs appareils. Comment déterminer quel appareil a réalisé l'action ? (ex. Chrome)

- Le consentement ?
  - accord librement consenti par une victime, un témoin
  - accord libre et légal d'un usager suspect d'être l'auteur de l'infraction
  - autorisation du juge (en fonction du cadre légal)

Cloud et règles forensiques

- A qui appartient la donnée ?
  - Le fournisseur de service ? Ou l'usager ?
  - Ex des résiliations unilatérales de compte sur violation des CGU (Google, Facebook, ...)
  - Qu'est ce qu'un ayant droit sur la donnée ?
    - Usager ? Fournisseur de service ? L'Etat de résidence de l'usager, du fournisseur de service ?
- Accès à la donnée ?
  - identifiants et mots de passe données par le suspect
  - identifiants et mots de passe découverts par l'enquêteur mais sans accord de l'intéressé
  - token (jeton) d'activation disponible sur un support numérique (ordinateur, téléphone...)

Cloud et règles forensiques

- Problématique d'accès
  - Authentification avec multi facteurs (vérification par un autre mail, un SMS, etc.)
  - Avertissement au titulaire du compte
  - Variation des techniques d'accès en fonction du service et de sa version

Les outils spécialisés

- Multiplicité d'outils : UFED Cloud Analyzer, XRY Cloud, AXIOM Cloud, ...
- Les services pris en charge varient d'un outil à l'autre mais on retrouve les classiques Facebook, Twitter,Gmail, Google, Dropbox, Instagram, What's App, iCloud, Snapchat, ...
- Quelles possibilités ?
  - acquisition sélective de la donnée (par artefact, par date, etc.)
  - récupération automatisée de token
  - Utilisation d'un mot de passe renseigné manuellement
  - Sécurisation de l'extraction (pas d'effacement des données originales, logs d'audit,...)
  - Traitement facilité pour l'enquêteur (interprétation des données visuelle, corrélation entre les données, ...)
- Une plus value AXIOM : partenariat avec Grayshift et récupération de keychain sur IOS

Focus sur un outil à titre d'exemple

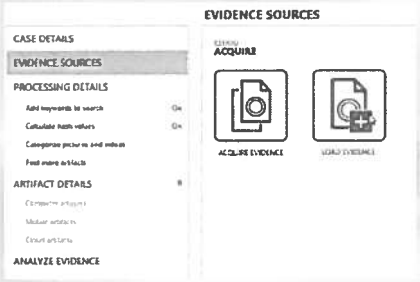
Un exemple, AXIOM

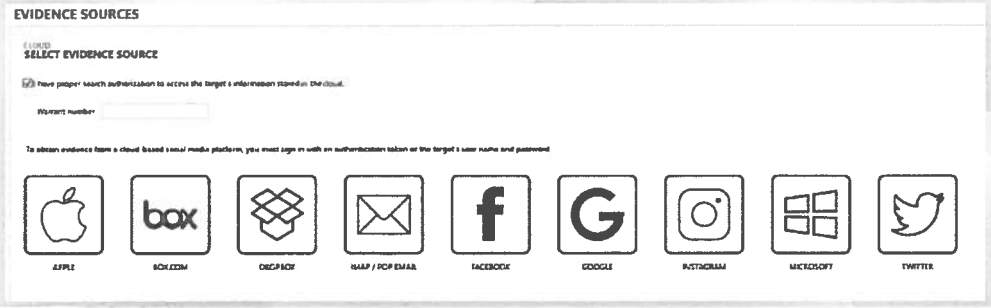
- Organisation : Dashboard / Artefacts / Connexions / File system / Registry / Timeline
- Visualisation : Gallerie / Colonne / Conversation / etc.
- Association de plusieurs sources de données (ordinateur, capture de RAM, Cloud, …)
- AXIOM ressource :

  https://www.magnetforensics.com/resources/

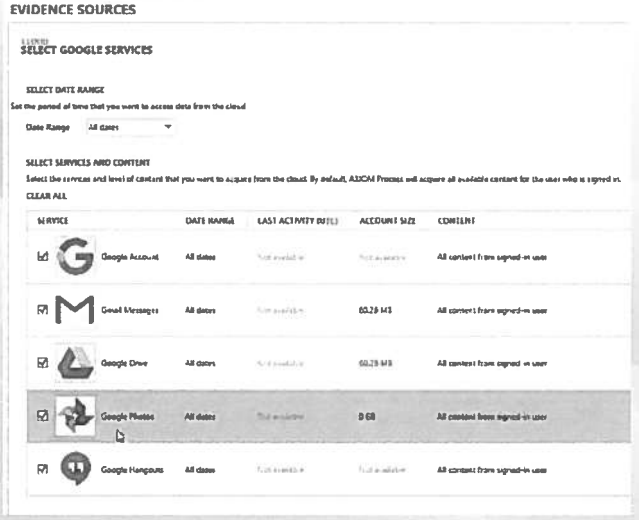
  https://www.magnetforensics.com/resources/getting-started-magnet-axiom/

Un exemple, AXIOM

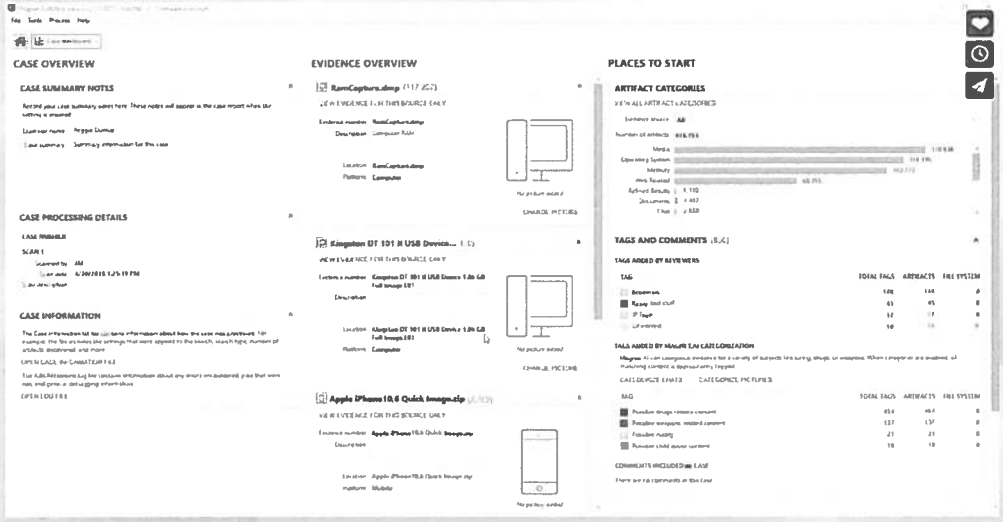




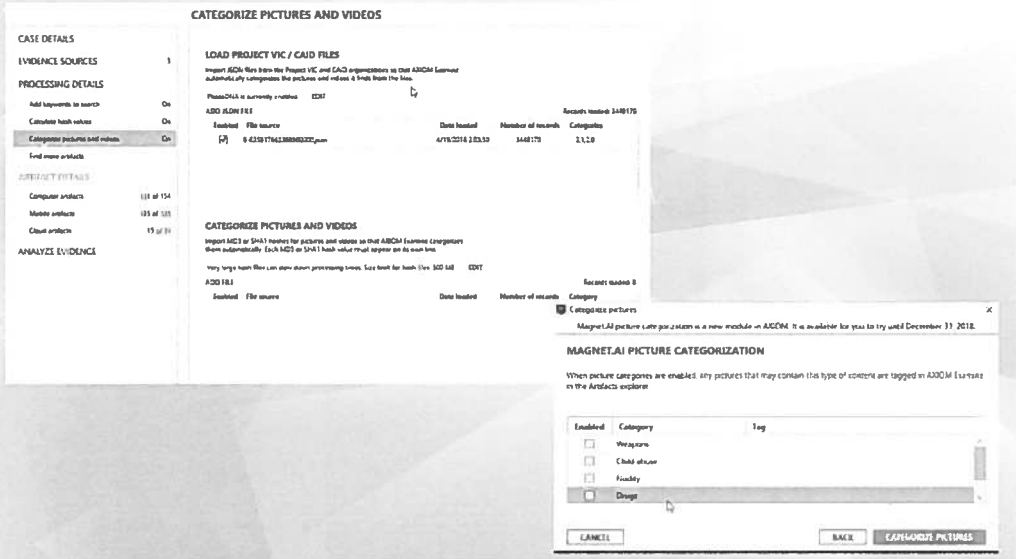
Un exemple, AXIOM



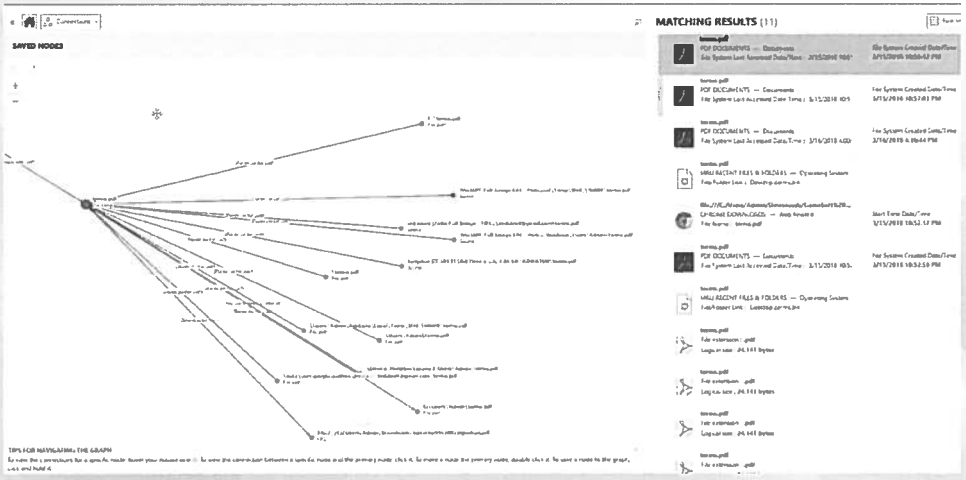
Un exemple, AXIOM



Un exemple, AXIOM



Un exemple, AXIOM



Des questions ?

Recueillir les informations par Internet dans le contre terrorisme

De l'information à la preuve

Module 4 : Anti forensic, live forensic et méthodes de discrimination

· Maroc - 2019

1) Ce qui gêne l'accès à l'information

2) Le live forensics

3) Vers des méthodes de discrimination ?

Ce qui gêne l'accès à l'information

Anti forensic, l'anonymisation

- Nous laissons trop de trace sur Internet
  - http://www.anonymat.org/vostraces/index.php
  - https://myshadow.org/fr/trace-my-shadow
  - https://addons.mozilla.org/fr/firefox/addon/lightbeam/
  - Back up Facebook ou Google...
- Si c'est gratuit, c'est vous le produit
- Une volonté légitime de préserver sa vie privée

1. Créer des mots de passe solides.
2. Prévenir l'usurpation d'identité
3. Demander le déréférencement d'un contenu vous concernant.
4. Distinguer sphère privée/publique.
5. Faire attention aux publications sensibles.
6. Effacer ses données de navigation.

20 juin 2017

Protéger sa vie privée en 6 étapes | CNIL
https://www.cnil.fr/fr/proteger-sa-vie-privee-en-6-etapes

Anonymisation et cyber café

- Les cyber cafés sont soumis aux règles de conservation de données des fournisseurs d'accès Internet, en France, 1 an
- Des logs de connexion... euh, oui ?
- La vidéo surveillance, ah, en panne...
- La comptabilité, vous savez, on paye beaucoup en liquide ici
- Les ordinateurs, on les ghost toutes les semaines, pour éviter les virus
- Un cas concret, le dossier Sophie LETAN, disparue le 7 septembre 2019

Anonymisation et hot spot

- Wardriving : https://wigle.net/
- https://www.aircrack-ng.org/
- Octobre 2018, publication d'une faille WPA2
  (https://www.lesnumeriques.com/informatique/decouverte-d-methode-simple-pour-craquer-wi-fi-wpa2-n79795.html)
- Dossier Nantes, 2018. Et si les hot spots devenaient une source d'information ?

Anti forensic, anonymisation

- Proxy
  - Logiciel ou service
  - Interface origine/cible
- VPN
  - Logiciel ou service
  - Tunnel sécurisé
- TOR, et les autres
  - Réseau indépendant
  - Anonymisation et sites onion
- Navigation privée

Anti forensic, chiffrement

- Chiffrement et code de verrouillage
- 434-15-2 Code pénal, le refus de remise d'une clé de chiffrement
- Conseil Constitutionnel, décision n° 2018-696 QPC du 30 mars 2018
- Tribunal de Nice, 16 mai 2019
  - Le code de verrouillage du téléphone n'est pas un moyen de cryptologie
  - Aucun élément de l'enquête n'indiquait que le téléphone visé contenait des données utilisées pour préparer ou faciliter un délit
  - La demande du code par un policier n'est pas une demande de l'autorité judiciaire (magistrat, institution de jugement)
- Tribunal de Belfort, 5 juin 2019
  - Il refuse de donner son code de verrouillage et est condamné à 3 mois de prison

Anti forensic, effacer ses traces

- *Logiciels de nettoyage (Ccleaner, Bleachbit, Privazer, …)*
- *Wipe (HDShredder, Dban, HDDerase, …)*
- *Destruction de matériel*
- *Deux dossiers sur le Darnet*
  - *Black Hand*
  - *French Deep Web*

Le live forensics

Le live forensics, pourquoi ?

- La généralisation du chiffrement (bitlocker, truecrypt, filevault 1 ou 2, veracrypt, pgp ….)
  - Filevault et bitlocker peuvent se désactiver si la session est active
  - Il est possible d'exporter la clé de mise au clair
  - Il est toujours possible de faire une copie logique des données
- L'augmentation de la taille de la mémoire vive
  - Quelques précisions
    - Pour accélérer le temps de traitement de l'information, et améliorer l'expérience de l'utilisateur, le système n'écrit pas toutes les données utiles et en stocke une partie dans la mémoire vive (RAM)
    - Celle-ci se vide quand elle n'est plus alimentée en électricité

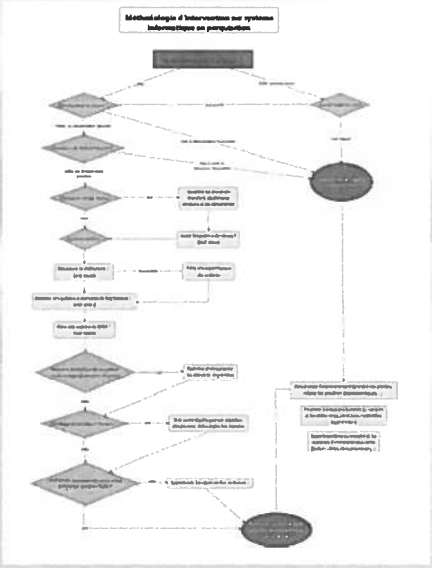
Le live forensics, pourquoi ?

  - La mémoire vive peut contenir :
    - Des mots de passe
    - Des documents en cours d'écriture mais non encore enregistrés
    - Des éléments relatifs aux programmes en cours
    - Etc.
- L'importance croissante du stockage de données à distance
  - Réseaux sociaux
  - Stockage à distance
  - Services externalisés
  - Etc.

Le live forensics, pourquoi ?

- La multiplication des supports numériques et de leur taille
  - De 1956 (5mo) à 2019 (6to), la taille moyenne d'un support a été multipliée par 1200
  - En perquisition, de 1 à 2 supports par foyer à 10 en moyenne
- Certains supports ne s'exploitent qu'en live forensics
  - Box internet (disques souvent chiffrés nativement, données dépendantes de la connexion du domicile)
  - Consoles de jeux (disques nativement chiffrés, systèmes de fichier atypiques)
  - Smart TV (démontage très complexe, navigation facilitée par télécommande utilisateur)

Proposition de méthodologie



Vers des méthodes de discrimination ?

Discrimination, pourquoi ?

- Parce que :
  - Toutes les enquêtes ne nécessitent pas des expertises
  - Tous les mis en cause n'ont pas la même importance dans une enquête
  - Tous les supports numériques ne sont pas susceptibles d'apporter des éléments utiles à l'enquête
  - Le délai disponible pour l'analyse numérique est insuffisant
  - Le nombre de spécialistes n'est pas toujours suffisant
  - Le matériel forensic disponible n'est pas toujours suffisant
- S'adapter, une obligation des services de police
- Et parce que tout dépend des besoins réels de l'enquêteur

Tout prendre ou pas ?

- L'intérêt d'un support dépend d'abord du dossier
  - Il y a t'il des dossiers pour lesquels le numérique est inutile ?
  - Les éléments déjà présents en enquête sont-ils suffisants ?
  - Ces éléments sont-ils incontestables ?
  - Tous les aspects de contexte sont-ils explorés ?
  - Etc.
- Sélectionner les supports
  - En fonction de leur nature ?
  - En fonction de leur dernière date d'utilisation présumée ?
- Il y a t'il des dossiers pour lesquels ont ne peut pas se permettre d'écarter quoi que ce soit ?

Traiter pendant la perquisition

- La perquisition permet :
  - De saisir les supports en vue d'un traitement ultérieur
  - De copier les données en vue d'un traitement ultérieur
  - De traiter les données sur place
- Une obligation, s'adapter au contexte :
  - Les données non exploitées seront-elles accessibles après la perquisition ?
  - Est-il possible de prolonger la perquisition ?
  - Le gain de temps en perquisition est-il utile ?
- Que peut-on dire en quelques minutes ?
  - Vérifier si le support est est exploitable ou HS
  - Dater sa dernière utilisation
  - Déterminer son utilisation générale et corréler cette information au contexte de l'enquête

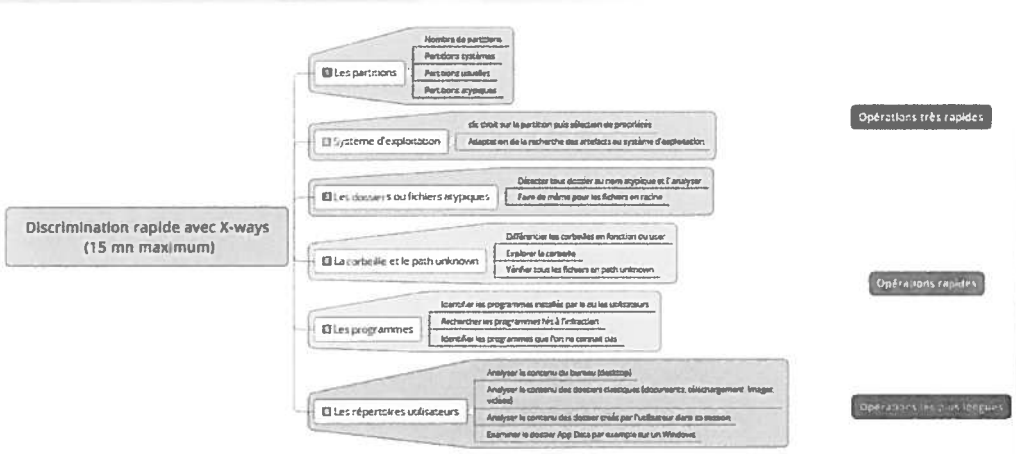
Priorisation

- Le dialogue entre l'expert et l'enquêteur
  - Comprendre les besoins de l'enquêteur
  - Proposer les actes techniques susceptibles de correspondre
  - Evaluer la durée probable de réalisation de ces actes
- Hiérarchiser l'ordre de traitement des supports en fonction des besoins de l'enquêteur
- Limiter les axes de recherche en fonction du type de dossier et du besoin de l'enquêteur
- Ne rien figer et garder une souplesse en fonction :
  - Des éléments découverts
  - De l'arrivée de nouveaux supports au fur et à mesure de la mission
- Les contraintes légales (ex de la copie obligatoire en commission rogatoire)
- Les contraintes techniques (ex de l'extraction sur supports mobiles)

Objectifs

- A l'issue de la discrimination, l'analyse sera en mesure
  - d'exposer tous les axes de recherche qu'il a traité,
  - à quel niveau de profondeur,
  - de préciser ce qu'il n'a pas fait en raison de la demande, du temps imparti, etc.
  - de conclure avec une des options suivantes
    - expliquer si le support analysé contient des éléments pertinents pour l'enquête, lesquels et de les présenter de manière exploitable pour l'enquêteur.
    - expliquer si l'exploitation n'a pas permis la découverte d'éléments pertinents dans le temps imparti
    - informer l'enquêteur que le délai prévu nécessite une nouvelle évaluation de sa part en raison de la découverte d'une complexité technique, de beaucoup d'informations pertinentes, etc.

Méthodologie



Le parcours visuel

- Délai : 15 à 30 mn
- Objectif : "prendre la température" d'un support
- Contraintes : toujours garder une trace de tout élément pertinent découvert
  - Association de table de rapport (Xways)
  - bookmark (Xways, IEF, UFED ou XRY reader)
  - Une simple une prise de note
- **Examen des partitions**
  - Identifier les partitions actives
  - Identifier la partition contenant le système d'exploitation (s'il y en a un)
  - Identifier la ou les partitions de données
  - Différencier les partitions en fonction du nombre de fichiers qu'elles contiennent, de leurs dates de création et d'accès.

Méthodologie de discrimination

- **Système d'exploitation**
  - Orienter l'analyse en fonction des artefacts et localisations propres à chaque système d'exploitation
  - Clic droit > propriété sur la partition sous Xways
- **Les dossiers ou fichiers atypiques**
  - Identifier un fichier atypique en raison de sa taille (les fichiers de machine virtuelle ou de container chiffrés sont en général volumineux ou ont une taille fixée précisément)
  - Identifier les dossiers ou fichiers dont les noms ont un lien potentiel avec l'enquête.
  - Explorer le répertoire racine en premier lieu, puis l'arborescence en recherchant tout nom de dossier ou de fichier inhabituel et/ou en lien avec l'enquête

Méthodologie de discrimination

- **La corbeille et les chemins inconnus**
  - Différencier les corbeilles en fonction de l'utilisateur
  - Rechercher tout élément en lien avec l'enquête
  - Rechercher tout fichier dont le nom est susceptible d'intéresser l'enquête
  - Passer en mode gallerie pour visualiser les images
- **Les programmes**
  - Orienter l'analyse en fonction des artefacts associés ou des fonctions spécifiques de certains programmes
  - Identifier tout programme permettant de découvrir de l'information (messagerie instantanée, mail, etc.)
  - Identifier tout programme susceptible de cacher ou d'effacer de l'information (chiffrement, nettoyeur, etc.)

Méthodologie de discrimination

- **Les répertoires utilisateurs**
  - Concentrer le parcours visuel sur les localisations les plus classiques de stockage d'information
  - Analyser tout le contenu du bureau (Desktop)
  - Analyser le contenu des dossier de stockage dédiés (documents, téléchargement, images, vidéo, etc.)
  - Analyser le contenu des dossiers créés et nommés par l'utilisateur
  - Examiner les dossiers de stockage de données habituels des programmes (App Data sur Windows, Library sur Linux, etc.)

Les tâches automatisées

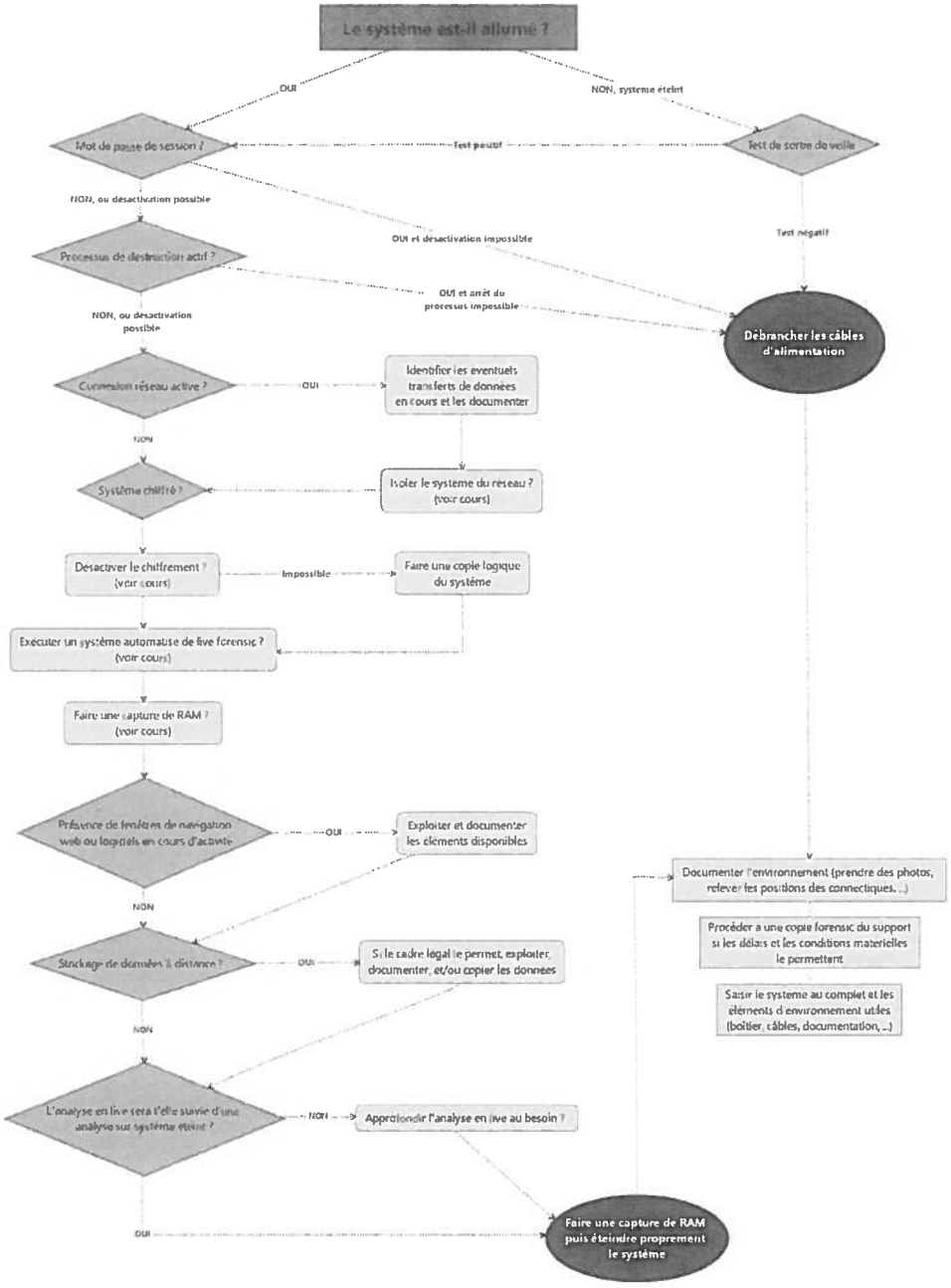
- Adapter les tâches automatisées à la puissance de la machine
  - création du rapport de base de registre pour les systèmes Windows
  - fonction quick search d'Internet Evidence Finder
  - fonction refine volume snapshot de Xways ou Case processor avec Encase
    - sur un volume système, en discrimination, il est préconisé de le lancer sur le répertoire utilisateur pour une analyse rapide

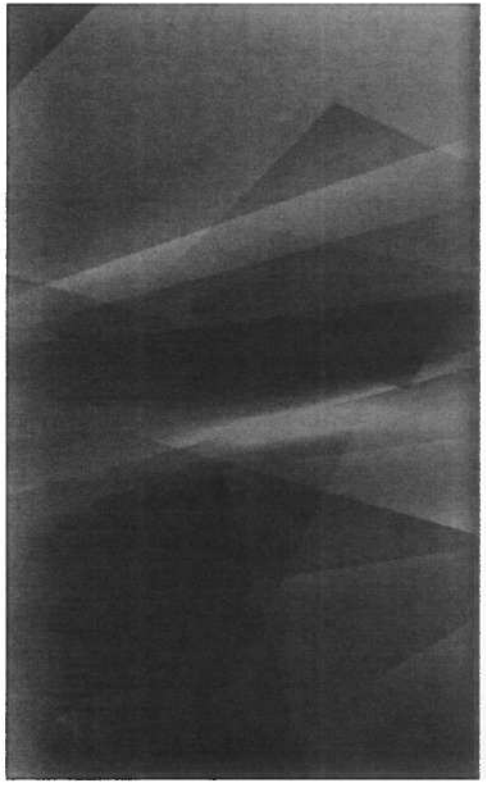
La copie « enquêteur »

- Souvent, la mission de l'expert vise uniquement à faire une copie exploitable par l'enquêteur
  - Par manque de temps
  - Parce que l'enquêteur est celui qui connaît le mieux le dossier
  - Parce que l'enquêteur a les capacités techniques pour l'exploiter
  - Parce qu'il a de toute façon plus de temps que l'expert
- Outils dédiés : UFED, XRY, IEF/AXIOM
- Manuellement ?

Des questions ?

Méthodologie d'intervention sur système informatique en perquisition





Recueillir les informations par Internet dans le contre terrorisme

De l'information à la preuve

Module 5 : le compte rendu d'exploitation

[redacted] – Maroc - 2019

1) Les différents types de compte rendu
2) Les fondamentaux du compte rendu
   - Contexte
   - Horodatage
   - Attribution (utilisateur)
   - Utilisation
3) La forme
4) Conclure

Les différents types de compte rendu

Le rapport d'expertise et rien d'autre ?

- Quelque soit le cadre, un compte rendu oral est toujours possible
  - Missions d'assistance (perquisition par exemple)
  - Expert :
    - *« Les experts doivent remplir leur mission en liaison avec le juge d'instruction ou le magistrat délégué ; ils doivent le tenir au courant du développement de leurs opérations et le mettre à même de prendre à tout moment toutes mesures utiles. »* (164 al 3 CPP)
    - *« Avec l'accord du juge d'instruction, les experts peuvent, directement et par tout moyen, communiquer les conclusions de leur rapport aux officiers de police judiciaire chargés de l'exécution de la commission rogatoire, au procureur de la République ou aux avocats des parties »* (166 al 4 CPP)
  - Personne qualifiée : *« ...Elles peuvent communiquer oralement leurs conclusions aux enquêteurs en cas d'urgence. »* (60 al 3 CPP, extrait)

Le procès verbal

- *Procès verbal de perquisition*
  - *Si l'exploitation a lieu pendant la perquisition (ou de retour au servive dans le respect des règles de la perquisition)*
  - *Les opérations seront obligatoirement mentionnées dans ce PV*
  - *Ou dans un rapport annexé à ce PV*
- *Procès-verbal d'exploitation technique*
  - *Le spécialiste numérique policier qui agit en tant qu'enquêteur hors cadre de perquisition peut choisir son support*
    - *Procès verbal*
    - *Rapport d'exploitation*
- *Quelle différence entre un procès-verbal et un rapport annexé ?*
  - *Les deux sont des pièces de procédure*
  - *Le rapport permet plus de liberté visuelle*

Un rapport, des rapports

- Le rapport est obligatoire
  - Pour l'expert
  - Pour la personne qualifiée requise (policier ou non)
- Mais rédiger un rapport, c'est souvent plus long que rédiger un procès-verbal
  - Faire un rapport uniquement pour les supports dans lesquels on a trouvé quelque chose d'utile ?
  - Un rapport global pour tous les supports ?
  - Un rapport global pour tous les supports négatifs ?
- Proposition : un rapport distinct pour tout support dont l'exploitation a permis la découverte d'éléments utiles à l'enquête.
- La loi n'impose rien de précis et l'efficacité est donc la règle

Les fondamentaux du compte rendu

Contexte

Les fondamentaux d'un compte rendu

- Quelle que soit l'option choisie, un compte rendu est soumis à des règles fondamentales
- **Identifier l'analyste**
  - Identité, service d'affectation
  - Coordonnées (car on est souvent rappelé...)
  - Qualification, certifications, diplômes ?
- **Est-il bon/nécessaire d'indiquer :**
  - Outils utilisés ?
  - Détail des méthodes d'exploitation ?
- **Identification du support**
  - Présenter la manière dont le support a été remis à l'analyste
  - Identifier le support par ses spécifications matérielles (n° de série?)
  - Identifier visuellement le support et son état de réception par une photo ?

Les fondamentaux du compte rendu

Horodatage

Les fondamentaux d'un compte rendu

- **Dater son utilisation**
  - Les considérations de fuseau horaire...
  - Dater la première et la dernière modification d'un support numérique
  - Dater la période pendant laquelle il a été utilisé principalement
  - Système NTFS, date de création de la $MFT et date du dernier fichier accédé
  - Dater la création d'un dossier utilisateur spécifique ?
  - Sur un support non système : du fichier créé le plus ancien au fichier accédé le plus récent ?

Les fondamentaux du compte rendu

Attribution

Les fondamentaux d'un compte rendu

- **Identifier si possible son utilisateur**
  - La difficulté d'identifier réellement l'utilisateur d'un support
  - Différence entre propriétaire et utilisateur
  - Attribution d'une action via le profil utilisateur ?
  - Quid des supports ou sessions non protégés et accessibles par tous ?
  - L'importance de la contextualisation

Les fondamentaux d'un compte rendu

- Pistes de recherches possibles :
  - nom des utilisateurs
  - nom du propriétaire du système d'exploitation (base de registre Windows)
  - tout élément d'identité sur le support (CV, CNI, document signé, etc.)
  - tout élément de navigation attribué (accès à un compte bancaire, à un webmail, à un compte de réseau social, etc.)
  - etc..

Les fondamentaux du compte rendu

Utilisation

Les fondamentaux d'un compte rendu

- **Expliquer à quoi le support a servi dans le cas d'une exploitation ayant permis la découverte d'éléments utiles à l'enquête**
  - Mettre en évidence les éléments pertinents pour l'enquête
  - Cibler les éléments utiles uniquement ?
  - Les contextualiser (en horodatage et en attribution)
  - Les présenter de manière adaptée pour qu'ils soient compréhensibles
  - photo ? (attention aux captures non lisibles)
  - Miniatures d'une vidéo ? (vignetage)
  - Tableau pour de la navigation internet avec date/url (un tableau est plus facile à lire et permet une recherche dans le corps du PV ou du rapport, ce que ne permet pas une capture d'écran).
  - Capture d'écran pour un texte ou une conversation (quand une recherche dans le corps du texte ne sera pas nécessaire)
  - Etc

La forme ?

Les fondamentaux d'un compte rendu

- Localiser la source de chaque info pertinente
  - chemin logique d'accès au fichier
  - offset ou 1er secteur si donnée carvée.
- Exporter les éléments utiles pour une consultation ultérieure ?
  - Simple export avec classement des données ?
  - Conservation des chemins logiques ?
  - La personne qui fera la consultation ultérieure a t'elle les moyens de le faire ?

Les fondamentaux d'un compte rendu

- **Expliquer à quoi le support a servi dans le cas d'une exploitation n'ayant permis la découverte d'aucun éléments utile à l'enquête**
  - Simplement mentionner que les recherches sont négatives ?
  - Synthétiser à quoi le support a servi ?
    - Exemple : disque dur de l'ordinateur familial, principalement utilité pour de la navigation Internet et du stockage de photos familiales
- Les erreurs à ne pas commettre dans un compte rendu
  - Extrapoler à partir d'une donnée
  - Ne pas rappeler le contexte de l'analyse (délai imparti, rappel de la mission, …
  - Lister les axes de recherches exploités ? (et donc à contrario, ceux non exploités?)
- Gérer une mission visant à rechercher « *tout élément susceptible de contribuer à la manifestation de la vérité* »

Conclure

Les fondamentaux d'un compte rendu

- La conclusion d'un rapport
  - Un rapport trop long est rarement lu en entier et de manière détaillée
  - rappeler les points de passages obligatoires :
    - identification du support
    - période d'utilisation
    - son ou ses utilisateurs probables
  - Préciser chaque élément pertinent susceptible d'être utile à l'enquête.
  - Ne pas donner un avis et rester très factuel.
  - Utiliser un vocabulaire facilement compréhensible par un néophyte et au besoin définir les termes complexes dans un lexique.
  - Attention, toute mention dans la conclusion doit faire référence à des éléments qui ont été écrits dans le corps du PV ou du rapport
  - Tout ce qui n'est pas écrit dans le rapport ne peut être utilisé dans la procédure, que ce soit au moment de l'audition d'un suspect ou même lors du procès-pénal.

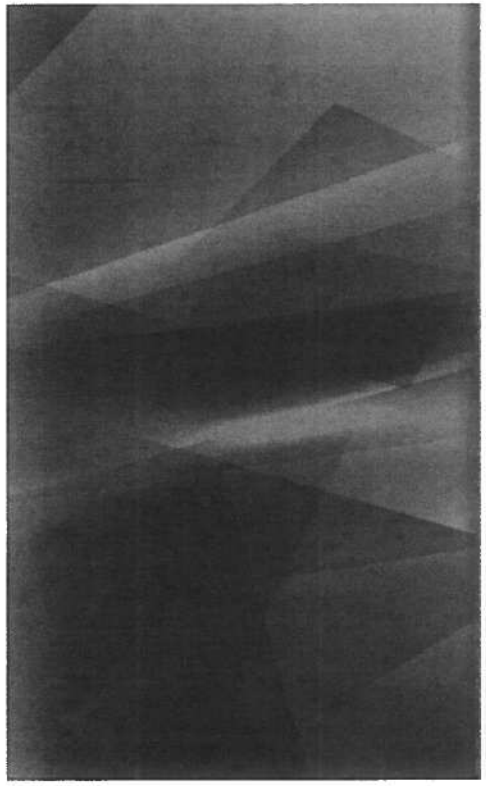
Les fondamentaux d'un compte rendu

- Quelques considérations :
  - Plus la mise en forme d'un rapport ou d'un PV est soignée, plus le contenu est facile à lire et à utiliser.
  - Il est important de contextualiser l'exploitation pour permettre au magistrat ou à l'enquêteur de comprendre que ce qui a été fait est limité par les contraintes imposées (délai, matériel, etc.)
  - Attention aux termes obligatoires de contextualisation
    - Exemple : "l'analyse, réalisée dans le temps contraint de la garde à vue, et sur les orientations fournies par l'enquêteur, a permis de mettre en évidence les éléments suivants : "
    - Ne pas dénigrer une exploitation : "il s'agit d'une première analyse" ou « cette analyse devra être complétée par une expertise »
    - Par contre, si une exploitation différente et nécessaire, le préciser : en cas de chiffrement par exemple.

Et si l'expert avait commis des erreurs ?

- Missions très précises
  - Peu d'erreurs possibles sur des actes purement techniques
  - Des erreurs potentiellement limitées si la méthodologie de travail est bonne
- Les missions larges
  - Aucun expert ne sera jamais à l'abri d'une erreur
    - Même les actes techniques et scientifiques sont susceptibles d'erreurs
    - L'analyse numérique dépendra toujours du facteur humain représenté par l'expert
      - Erreur liée à un manque de connaissance
      - Erreur liée à une extrapolation à partir d'une donnée
      - Information non découverte
- Se préparer à gérer ses erreurs en vue du procès-pénal
  - L'importance de la méthodologie
  - L'importance de documenter ses opérations

Des questions ?



Recueillir les informations par Internet dans le contre terrorisme

De l'information à la preuve

Module 6 : le témoignage de l'expert au procès pénal

[redacted] – Maroc - 2019

- Toute enquête à vocation à finir par un procès
- Aucun enquêteur/expert ne sait ce qu'il va trouver avant de chercher
- Même la plus basique recherche technique peut devenir l'élément de preuve clé dans un procès

« Les experts ne décident jamais eux mêmes le procès, ils ne sont chargés que d'éclairer la religion des juges »

A. Rodière,1878

1) Préparer son témoignage
2) L'expert
3) L'expertise
4) Un procès, des procès, quel tribunal ?
5) Procès et étiquette
6) Gérer un interrogatoire
7) Les attaques et faiblesses habituelles

Préparer son témoignage

Vous êtes convoqués en tant que témoin expert ?
Il est peut-être déjà trop tard pour bien faire certaines choses !

Préparer son témoignage
l'expert

Axes de préparation : l'expert

- Avez-vous votre CV à jour ?
  - Quels sont mes diplômes liés à mon domaine d'expertise ?
  - Ai-je des certifications ? Sont-elles à jour ?
  - Combien d'années d'expérience ais-je dans ce domaine ?
  - Ais-je une notoriété ? Ais-je des publications ?
  - Ais-je une activité extra professionnelle (professeur, chercheur, …) ?

Axe de préparation : l'expert

- Antécédents d'un expert
  - son travail a t-il déjà été reconnu ?
  - son travail a t-il déjà été contesté ?
- Quelle est la notoriété des diplômes ou certifications
- Quelle est la notoriété de son entreprise, de son service, … ?
- Quid si un expert de votre cercle (diplôme, certification, service, entreprise...) a donné une image négative de son travail ?

Préparer son témoignage l'expertise

Axes de préparation : l'expertise

- Qu'est ce qu'une expertise susceptible de susciter une convocation au procès pénal ?
  - Un simple procès verbal
  - Un rapport d'expertise, d'exploitation, de triage, ...
  - L'ensemble d'une enquête
  - Autre ?

Axes de préparation : l'expertise

- La personne qui est convoquée au tribunal est-elle celle qui a rédigé le rapport, réalisé la mission ?
  - Signer une expertise faite par quelqu'un d'autre ?
  - Signer l'expertise réalisée par l'équipe que l'on manage et qui mixte différentes compétences techniques que l'on ne maîtrise pas toutes ?
- De quand date cette expertise ?
  - Plusieurs années ?
  - Avez-vous changé de service, de travail depuis ?

Axes de préparation : l'expertise

- Le support d'expertise est-il suffisamment détaillé ?
  - Saviez-vous au moment où vous l'avez rédigé que votre travail vous conduirait au tribunal ?
  - Avez-vous utilisé un modèle qui vous incite à tout détailler ?
  - Aviez-vous le temps de tout détailler ?
  - Le rapport versé en procédure est-il complété d'un autre rapport plus technique que vous gardez dans vos archives personnelles en cas de besoin ?
- Le rapport est-il trop détaillé ?
  - Perdre son lecteur en donnant trop d'information ?
  - Ouvrir des pistes pour une contestation de votre travail ?

Axes de préparation : l'expertise

- Un rapport clair et intelligible
  - Définir les mots complexes
  - Expliquer les informations techniques compréhensibles des seuls experts
  - Ne pas divulguer des méthodes que les avocats et suspects ne doivent pas connaître
- Les archives
  - Si le tribunal ne vous donne accès qu'à votre rapport papier
  - Si ce support papier n'est pas lisible (les multi photocopies)
  - Avez-vous une archive personnelle ?

Axes de préparation : l'expertise

- Les archives (suite)
  - Avez-vous une copie numérique du support exploité ?
  - La seule copie est-elle un scellé conservé par le tribunal ?
  - Y avez-vous accès ?
  - Votre copie, la copie du tribunal, ou le scellé original sont-ils endommagés ?
  - France : un expert ne peut garder une copie du support que pour la durée de sa mission,Crim, 8 juillet 2015 (15-81.731)

Préparer son témoignage
un procès, des procès, quel tribunal ?

Axes de préparation : le tribunal

- S'informer
  - Localisation du tribunal, trajet pour y aller
  - A quelle heure devez-vous arriver ?
  - Combien de temps devez-vous rester à disposition du tribunal ?
  - Quelles sont les règles applicables du tribunal où vous êtes convoqués ? (contacter le greffe, le secrétariat, le juge, un autre expert qui est déjà passé?)
  - Qui sont les juges, procureurs, avocats prévus pour ce procès ? (OSINT, votre communauté d'expert, …)

Axes de préparation : le tribunal

- Quel type de tribunal ?
  - A quoi ressemble la salle ?
  - Qui sont les intervenants ?
  - Quelle est la procédure de témoignage pour ce tribunal ?
    - Certains tribunaux doivent vous laisser présenter votre témoignage avant de pouvoir vous poser des questions (Cour d'Assise française)
    - Certains tribunaux vous demandent uniquement de répondre à des questions.

Préparer son témoignage
Tribunal et étiquette

Axe de préparation : procès et étiquette

- Arriver en avance
- Avoir une carte professionnelle
- Tenue vestimentaire
- S'adresser aux acteurs du procès (président du Tribunal, autres juges, Procureur, avocats) dans les termes appropriés
- Aucun système électronique n'est autorisé sauf accord préalable du président du tribunal)
- Penser à débrancher son téléphone
- Témoignages assis ou debout... être à l'aise ?
- C'est en général le président du tribunal qui gère la parole et la donne.
- Peut-on refuser de répondre à une question ?

Préparer son témoignage
Subir un interrogatoire

Axes de préparation : le témoignage

- Préparer son matériel
  - Qu'autorise le tribunal
    - Des notes
    - Le rapport d'expertise
    - Des supports de présentation
      - Uniquement votre témoignage oral
      - Paperboard
      - Écran télévisé
  - Votre sujet d'intervention
    - Réviser jusqu'à connaître par cœur votre sujet
    - Vous demandera t-on de faire un cours ?
    - Vous demandera t-on uniquement de présenter vos résultats ?

Axes de préparation : subir un interrogatoire

- Habituellement, vous êtes de l'autre côté du miroir
- Le témoin expert n'est pas un juge
- Ne sortez pas de votre domaine de compétence
- Présentez des faits, éviter toute supposition
- Et pourtant, le tribunal va forcément vous demander votre avis, votre opinion, votre sentiment, sur tel ou tel point
  - Baser un avis sur des faits
  - Énumérer des possibilités plausibles
  - Mettre en avant ce que vous estimez la possibilité la plus plausible ?

Axes de préparation : subir un interrogatoire

- Ne pas se laisser manipuler par une question
  - Prendre du temps pour répondre, même si la question est posée rapidement et que l'on vous presse de répondre
  - Préciser si vous ne comprenez pas la question
  - Préciser si la question contient des élément techniquement erronés
  - Ne répondez pas si la question ne relève pas de votre domaine d'expertise

Axes de préparation : subir un interrogatoire

- Gérer les questions longues et complexes
  - Faire reformuler ou répéter
  - Et si on vous demande une réponse par oui ou non ?
    - Interroger le juge ou la personne qui vous pose la question pour savoir si l'on attend de vous une réponse courte ou une explication
    - Détailler le raisonnement vous permettant de répondre dans un sens ou l'autre
- Questions hypothétiques, situations fictives
- Gérer la pression
  - Le tribunal est une pièce de théâtre...

Axes de préparation : subir un interrogatoire

  - Pour commencer, il est difficile d'être à l'aise (enjeux, lieu inconnu, situation inconnue, etc.
  - On peut chercher à vous déstabiliser
  - Ne reproduisez pas un schéma qu'on cherche à vous imposer
    - Votre interlocuteur parle très vite
    - Il élève la voix
    - Il utilise des mots qu'il veut vous faire répéter
  - Restez vous même et ne modifiez pas votre comportement, le naturel revient toujours
- Les questions pièges

Axes de préparation : subir un interrogatoire

- Avez-vous déjà menti ?
  - Oui
  - Non
  - Oui dans ma vie, mais pas sous serment ?
- Vous avez fait une erreur dans l'une de vos réponses
  - Mentionnez le au président du tribunal dès que vous vous en apercevez
  - Expliquez votre erreur et les raisons de cette erreur (une erreur de vocabulaire ?)
  - Ne tentez jamais de la dissimuler car elle reviendra forcément tôt ou tard.

Préparer son témoignage

Les attaques et faiblesses habituelles

Le témoignage de l'expert, attaques habituelles

- D'où va venir l'attaque ?
  - De l'avocat de la partie adverse en général (pour un policier, il s'agit le plus souvent de l'avocat de la défense)
  - du Procureur ou du Président du Tribunal ou de l'avocat de la défense
    - qui veut discréditer une preuve qui disculpe le mis en cause (car l'expert travaille à charge et à décharge)
    - qui sort de son rôle et veut vous faire dire quelque chose car il a une idée préconçue

Le témoignage de l'expert, attaques habituelles

- la qualification de l'expert
  - expérience en la matière
  - qualification sur les outils
  - durée de la certification
- Les outils utilisés
  - licences payées et à jour ?
  - Failles connues sur l'outil
  - Différence de résultats entre l'outil de l'expert et celui du contre expert
    - Différences génériques (nombre de résultats?)
    - Différence précise (une erreur matérielle?)

Le témoignage de l'expert, attaques habituelles

- L'attribution
  - qui a réellement agi ?
  - Données créées par l'utilisateur et données systèmes
  - Un support peut-il être utilisé par plusieurs personnes
  - un compte de réseau social ? (cf synchronisation d'un navigateur web type chrome)
  - Un espace de stockage en ligne ? (cf boites mails sans envoi des groupes d'escroc)
  - contextualiser une possible attribution avec l'accès, les mots de passe, les utilisations avant et après le fait ciblé, ...

Le témoignage de l'expert, attaques habituelles

- L'horodatage et la chronologie
  - Les fuseaux horaires
  - Création, modification, systèmes de fichier
  - Données effacées et récupérées (data carving)
  - Le contexte policier : existe t'il d'autres actes d'enquête (filature, écoute téléphonique, etc.) qui peuvent aider l'horodatage

Le témoignage de l'expert, attaques habituelles

- L'interprétation de la donnée
  - une donnée mal interprétée
    - erreur matérielle de l'expert
    - manque de connaissance de l'expert
    - le niveau de connaissance sur le sujet a changé
- la bataille d'expertise
  - comment départager deux experts sur un sujet que tout le monde ne comprend pas
  - il y a t'il une vérité « absolue » ?

Des questions ?