

squad



MIX YOUR
TALENT

Problématiques techniques et légales



Hardware



Investigation en ligne



Photo et vidéo



Hardware Introduction

Dans l'inforensique, il est important de savoir reconnaître les différents types de matériel dans un ordinateur. Par exemple un Mac basé sur un processeur Intel peut héberger un système d'exploitation Windows.

De plus, connaître la diversité du matériel informatique est requis pour comprendre quel interconnexion physique il a pu y avoir entre cette machine et le reste du monde. Pour la préparation du planning de l'investigation, il est primordial de comprendre quels sont les équipements à investiguer.

Enfin, afin que les preuves puissent être produites en justice, le processus de collecte de la preuve est aussi important que la preuve elle-même. Aussi, il faut savoir dès le début de l'investigation le type de connectique de tous les équipements numériques.



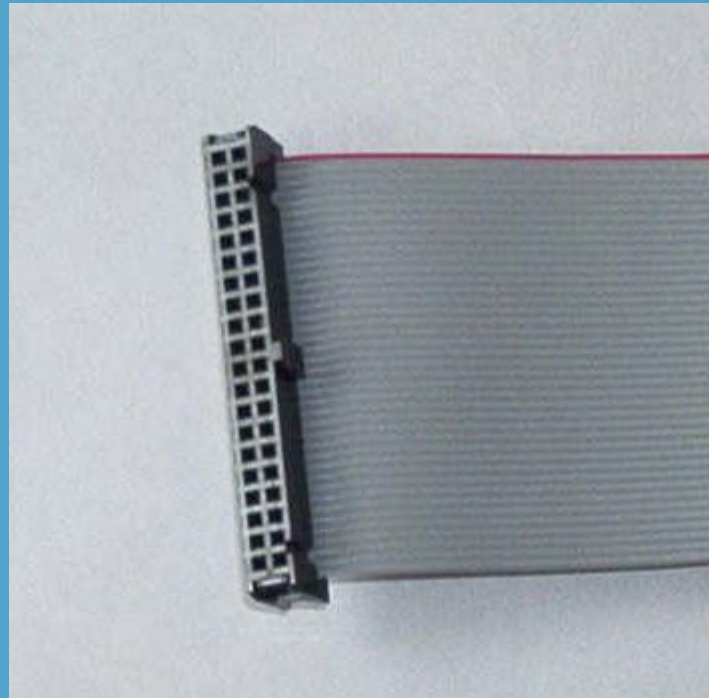
Hardware

Connectiques des disques durs

SCSI



IDE



SATA





Hardware

Connectiques des périphériques amovibles

USB



FireWire



MMC





Hardware

Médias pouvant contenir de l'information

Lesquels de ces éléments sont des médias pouvant contenir de l'information ?

- A. Bande magnétique
- B. Boitier d'alimentation
- C. CD
- D. Disque Blu-ray
- E. Disquette
- F. DVD
- G. RAM
- H. Processeur
- I. Valise



Hardware

Médias pouvant contenir de l'information

Lesquels de ces éléments sont des médias pouvant contenir de l'information :

- A. Bande magnétique
- B. Boitier d'alimentation
- C. CD
- D. Disque Blu-ray
- E. Disquette
- F. DVD
- G. RAM

Sauf si la machine est encore allumée

- H. Processeur
- I. Valise

Ça dépend ce qu'il y a dedans !

1

Hardware

2

Investigation en ligne

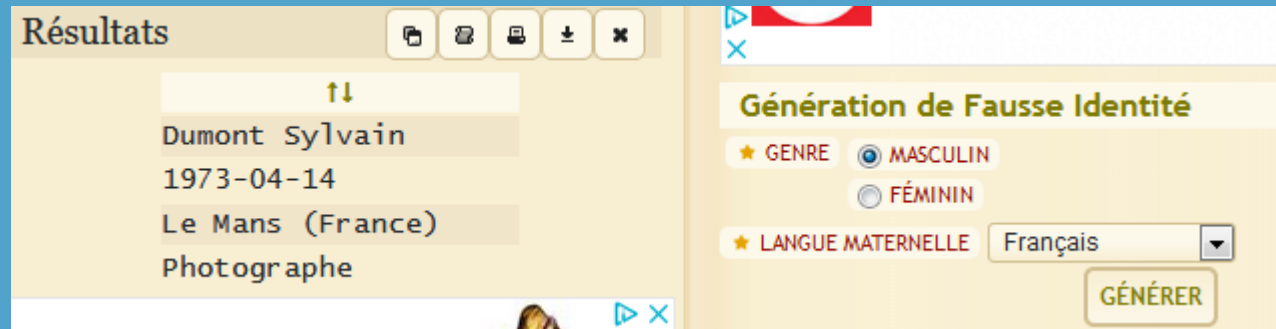
3

Photo et vidéo

2

Investigation en ligne Générateur d'identité

Il y a de nombreux services de génération d'identité (ou d'autres comme des numéros de carte bancaire), par exemple : <https://www.dcode.fr/generateur-fausse-identite>



The screenshot shows a web application interface for generating a fake identity. On the left, under the heading 'Résultats', there is a list of generated details: 'Dumont Sylvain', '1973-04-14', 'Le Mans (France)', and 'Photographe'. Above this list is a small icon with '↑↓'. To the right of the results is a toolbar with icons for copy, paste, print, download, and close. On the right side of the interface, under the heading 'Génération de Fausse Identité', there are input fields for 'GENRE' (with radio buttons for 'MASCULIN' and 'FÉMININ'), 'LANGUE MATERNELLE' (with a dropdown menu set to 'Français'), and a 'GÉNÉRER' button.

Il est également possible pour n'importe qui de se créer une adresse mail, par exemple : <https://temp-mail.org/>

Sans oublier qu'un compte sur n'importe quel réseau social (Facebook, Instagram, LinkedIn, Twitter...) peut être un faux compte. Pour gagner un concours basé sur un nombre de *like* sur Facebook, il suffit donc d'avoir un réseau de faux-compte plus grand que les autres ou de payer quelques euros sur le *dark web*, mais c'est un autre sujet.

2

Investigation en ligne Masquer une identité d'un-e agent-e sous couverture

Quelles moyen sont à disposition d'un-e agent-e sous couverture pour dissimuler sa réelle identité ?

- A. Forum
- B. I2P (Invisible Internet Project)
- C. Ne pas aller sur Internet
- D. Outils/sites web pour *spoof*er le numéro de l'appelant
- E. P2P (peer-to-peer)
- F. Proxy
- G. Pseudo
- H. SecureDrop
- I. Tor
- J. VPN

2

Investigation en ligne Masquer une identité d'un-e agent-e sous couverture

Quelles moyen sont à disposition d'un-e agent-e sous couverture pour dissimuler sa réelle identité ?

A. Forum

Sauf si vous avez confiance dans les administrateurs du forum.

B. I2P (Invisible Internet Project)

C. Ne pas aller sur Internet

On peut retrouver l'identité grâce aux personnes qui parlent de vous ou avec des méthodes de graphes reliant des profils Facebook à des gens n'ayant pas de profil Facebook.

D. Outils/sites web pour *spoof*er le numéro de l'appelant

E. P2P (peer-to-peer)

Utilisé pour échanger du contenu à caractère pédosexuel

F. Proxy, les logs peuvent être demandé par un mandat.

G. Pseudo, attention à ne l'utiliser que dans un seul cadre !

H. SecureDrop

Pour les lanceurs d'alertes, même si dans le cas de Julien Assange, c'était probablement les renseignements russes.

I. Tor, le plus efficace de la liste !

J. VPN

Uniquement si vous avez confiance dans les administrateurs du VPN.

2

Investigation en ligne

Recherche sur les antécédents d'une personne

Il y a tellement de moyen d'obtenir des informations sur une personne aujourd'hui avec les nombreux réseaux sociaux qu'il est impossible d'en faire une liste exhaustive. Mais voici quelques exemples :

1. Facebook, Twitter, Instagram...
2. Blogs
3. Groupe Usenet
4. AIM/Skype/GoogleTalk...
5. IRC
6. Github
7. WhatsApp/Signal...
8. LinkedIn/Viadeo...
9. Les bases de données des différentes agences des forces de l'ordre
10. archive.org qui permet parfois de trouver un post d'un utilisateur qui l'avait effacé



Quelles sont les types de cybercrime ?

- A. Blanchiment d'argent
- B. Contrefaçon ou toute autre violation de propriété intellectuelle
- C. Cyberharcèlement
- D. Cybermeurtre
- E. Fraude à la carte bancaire
- F. Fraude à la carte bibliothécaire
- G. Hébergement de services en ligne illégaux
- H. L'incitation au terrorisme et à la haine raciale sur internet
- I. Rançongiciel
- J. Revenge porn
- K. Revente de données sensibles
- L. Vol d'avatar
- M. Vol d'identité

2

Investigation en ligne Cybercrime

Quelles sont les types de cybercrime ?

- A. Blanchiment d'argent
- B. Contrefaçon ou toute autre violation de propriété intellectuelle
- C. Cyberharcèlement
- D. Cybermeurtre
- E. Fraude à la carte bancaire
- F. Fraude à la carte bibliothécaire
- G. Hébergement de services en ligne illégaux (pédocriminalité, DDoS as a service...)
- H. L'incitation au terrorisme et à la haine raciale sur internet
- I. Rançongiciel
- J. Revenge porn
- K. Revente de données sensibles (des données de santé par exemple)
- L. Vol d'avatar
- M. Vol d'identité

2

Investigation en ligne OSINT

Le **renseignement de sources ouvertes** ou **renseignement d'origine sources ouvertes** (ROSO)¹, (en anglais : **open source intelligence**, *OSINT*) est un **renseignement** obtenu par une **source** d'information publique.

Par extension, le ROSO désigne également les activités et méthodes de collecte et d'analyse de l'**information** de sources ouvertes, c'est-à-dire des informations accessibles au grand public. Ces sources incluent les **journaux**, l'**internet** dont les réseaux sociaux, les **livres**, les **magazines** scientifiques, les diffusions **radio**, **télévision**, etc.

Ce type de renseignement est un élément essentiel de l'**intelligence économique et stratégique** dans le secteur privé.

Comme souvent c'est utile pour l'attaque et pour la défense. Par exemple, profiter du Certificate Transparency pour identifier des certificats et des sous-domaines aide la *red team* pour augmenter la surface d'attaque mais ça aide aussi la *blue team* pour identifier un C&C de malware ou son auteur-rice.



Investigation en ligne OSINT

Quelles sont les outils utiles pour de l'OSINT ?

- A. censys.io
- B. exploit-db.com
- C. factionc2.com
- D. github.com
- E. haveibeenpwned.com
- F. robtex.com
- G. shodan.io
- H. tineye.com
- I. virustotal.com



Investigation en ligne OSINT

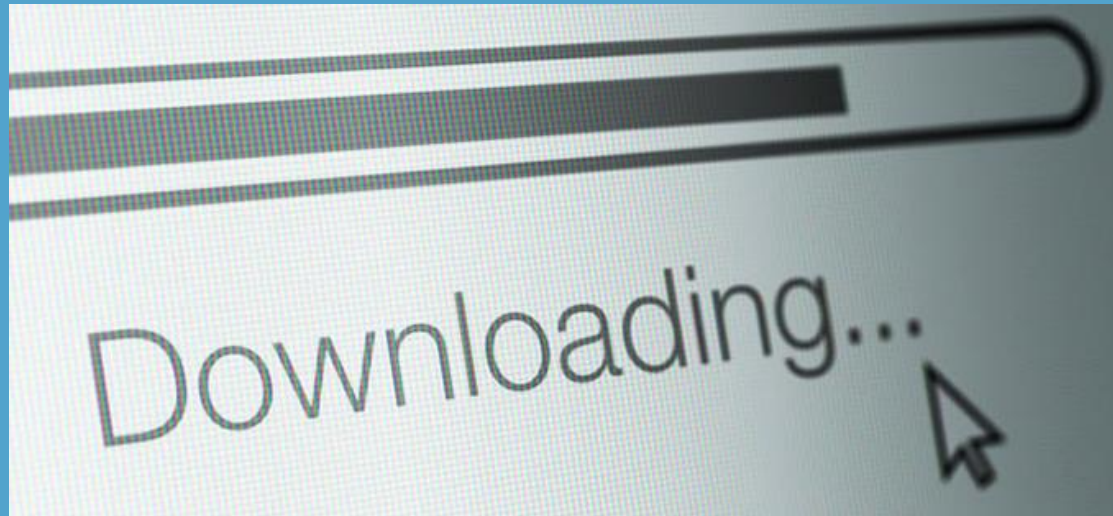
Quelles sont les outils utiles pour de l'OSINT ?

- A. censys.io
- B. exploit-db.com
- C. factionc2.com
- D. github.com
- E. haveibeenpwned.com
- F. robtex.com
- G. shodan.io
- H. tineye.com
- I. virustotal.com

2

Investigation en ligne Cas concret

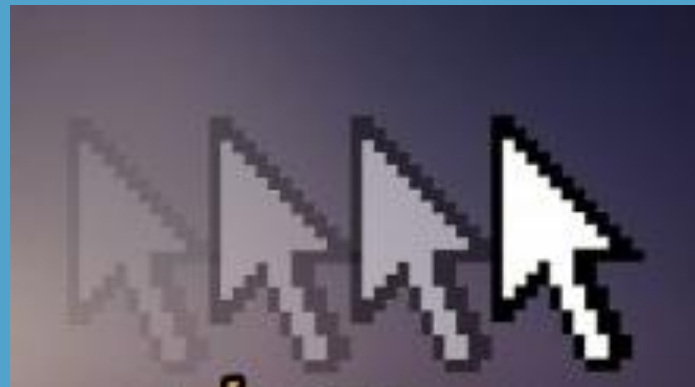
Des outils de hacking ont été détectés par l'antivirus sur un poste utilisateur. L'utilisateur a remonté qu'il n'était pas au courant. Pourtant les outils étant dans son répertoire de téléchargement, c'est très anormal que ça a été fait à son insu. Afin de gagner du temps au lieu de lancer une longue investigation, l'utilisateur a été appelé au téléphone et après lui avoir expliqué qu'il était préférable qu'il nous dise la vérité plutôt que l'investigation nous indique que c'est bien lui qui a téléchargé ces outils. Il a fini par avouer que c'était bien lui. Nous avons pu ainsi gagner du temps et simplement le réprimander afin qu'il ne renouvelle pas l'expérience.



2

Investigation en ligne Cas concret

Une utilisatrice nous a remonté des mouvements de souris étranges, un peu comme si quelqu'un avait pris le contrôle de son PC. Après une première analyse, rien de suspect n'était présent dans les traces de la machine. Après une longue conversation avec l'utilisatrice, en prenant le temps de lui expliquer qu'il est rare qu'un utilisateur se rende compte qu'il s'est fait piraté dans les attaques actuelles, nous avons fini par comprendre que l'utilisatrice avait des craintes côté personnel à cause de son ex-conjoint. Comme elle n'a pas accès à des informations sensibles pour le client, nous avons clos l'investigation en lui indiquant de nous recontacter si ça se reproduit. C'était probablement la touche Alt ou Ctrl qui était bloqué et a affiché des choses inhabituelles.



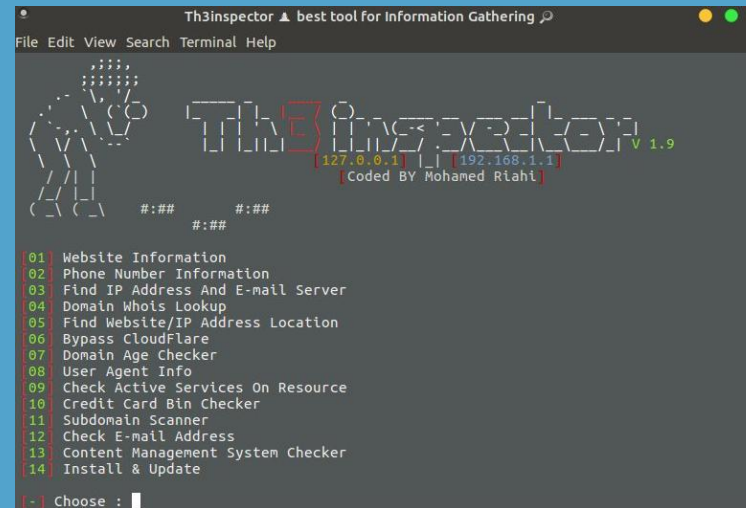
2

Investigation en ligne

Cas concret



Le PC portable professionnel d'un utilisateur a été infecté par un rançongiciel durant le confinement. Il n'avait pas effectué de backup car la sauvegarde automatique n'est pas active pour les personnes en télétravail. Il n'y avait pas d'outils de déchiffrement proposés pour ce malware. Heureusement, une partie du code du malware a été retrouvée sur GitHub, dont sa clé en dur qui était présente dans une ancienne version, ce qui a permis de déchiffrer les fichiers.

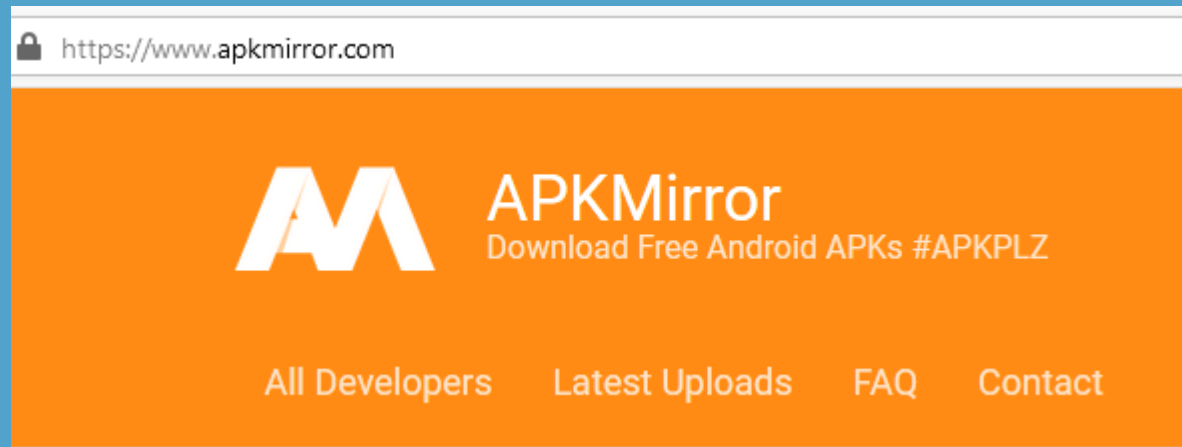


2

Investigation en ligne

Cas concret

Un smartphone est infecté par une application malveillante qui est complexe à analyser car elle a obfusqué son code. Une ancienne version de l'application a été trouvée sur un site stockant des applications Android. Cette ancienne version n'était pas obfusquée, ainsi l'analyse du code malveillant de l'application actuelle a été simplifiée.



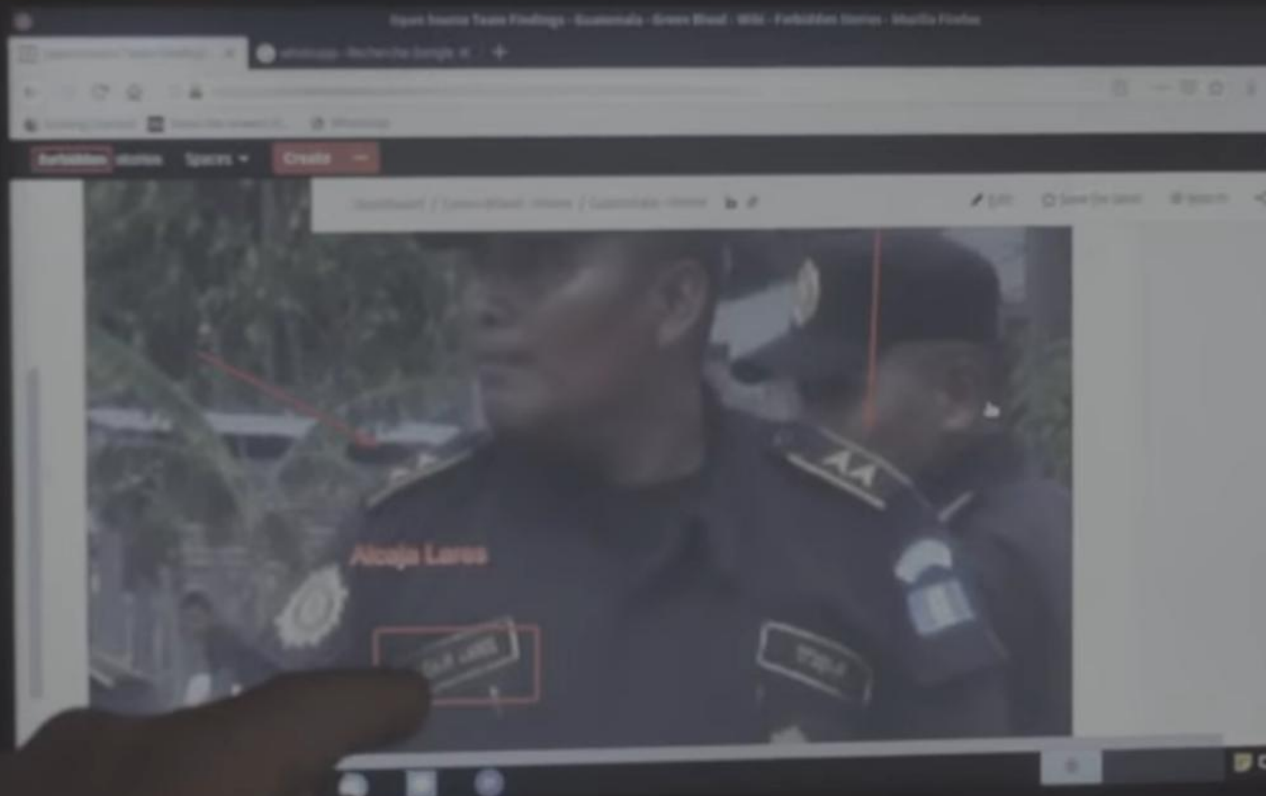
2

Investigation en ligne Cas concret d'OSINT par des journalistes

<https://forbiddenstories.org/fr/case/green-blood/>

forbidden stories

PROTECT YOU



L'équipe Forbidden Stories

Rédacteur en chef : Laurent Richard

Coordinateur du projet : Jules Giraudat

Journalistes : Arthur Bouvart, Marion Guégan, Cécile Schilis-Gallego

Enquêtrices : Paloma Dupont de Dinechin, Audrey Travère

Editrice (articles Forbidden Stories) : Martha M. Hamilton

Video trailer :

Réalisateur : Alexis Marant

Monteur : Matthieu Lère

Graphistes : Ludovic Gaillard, Mathieu Faure

Enquêteurs Open source : Bart Libaut, Youri van der Weide

Production : Aurelien Baslé, Camille Gruson, Daphné Haussely, Constance Juilliard

Création visuelle du projet : Paul-Emile Raymond et Adrien Mancel pour Wunderman Thompson

2

Investigation en ligne

Cas concret d'OSINT

https://www.lemonde.fr/big-browser/article/2014/06/10/intrusion-2-0-avec-shodan-controlez-des-webcams-et-imprimez-chez-les-autres

Rechercher

Le Monde

Se connecter

Consulter le journal

ACTUALITÉS ▼ ÉCONOMIE ▼ VIDÉOS ▼ OPINIONS ▼ CULTURE ▼ M LE MAG ▼ SERVICES ▼

BIGBROWSER

Partage

BILLET DE BLOG

Rédaction du Monde.fr

INTRUSION 2.0 - Avec Shodan, contrôlez des webcams et imprimez chez les autres.

Publié le 10 juin 2014 à 11h51 | Lecture 2 min.

Le blog du *Monde* j'ai du bon data évoquait en mai l'enquête "Null CTRL" publiée en octobre 2013 par le quotidien norvégien *Dagbladet*. Les journalistes Espen Sandli et Linn Kongsli Hillestad y mettaient en évidence d'inquiétantes failles de sécurité informatique en Norvège.

Grâce à Shodan, un moteur de recherche initialement créé pour répertorier les objets connectés à Internet, ils parvenaient à prendre le contrôle de caméras de surveillance, pouvaient régler le chauffage

Édition du jour

Daté du mercredi 17 juin

Le Monde

1

Hardware

2

Investigation en ligne

3

Photo et vidéo



Photo et vidéo

Les types de fichiers photos

Quelles sont les types de fichiers photos qui utilisent des images matricielles (matrice de point) et pas des images vectorielles (image en mode trait) ?

- A. Adobe Illustrator File (.ai)
- B. Bitmap Image File (.bmp)
- C. Drawing File (.drw)
- D. Encapsulated PostScript File (.eps)
- E. Graphics Interchange Format (.gif)
- F. Joint Photographic Experts Group (.jpg ou .jpeg)
- G. Portable Network Graphics (.png)
- H. RAW
- I. Scalable Vector Graphics File (.svg)
- J. Tagged Image File Format (.tif)

2

Photo et vidéo Les types de fichiers photos

Quelles sont les types de fichiers photos qui utilisent des images matricielles (matrice de point) et pas des images vectorielles (image en mode trait) ?

- A. Adobe Illustrator File (.ai)
- B. Bitmap Image File (.bmp)
- C. Drawing File (.drw)
- D. Encapsulated PostScript File (.eps)
- E. Graphics Interchange Format (.gif)
- F. Joint Photographic Experts Group (.jpg ou .jpeg)
- G. Portable Network Graphics (.png)
- H. RAW
- I. Scalable Vector Graphics File (.svg)
- J. Tagged Image File Format (.tif)

2

Photo et vidéo Altération d'image

L'affaire [\[modifier \]](#) [\[modifier le code \]](#)

Plus de deux cents photographies décrites par la police comme montrant un homme au visage brouillé abusant de jeunes enfants ont surgi sur [Internet](#). Le visage de l'homme avait été brouillé numériquement par un tourbillon sur les photographies, mais les experts informatiques de l'[office fédéral de police criminelle](#) allemand ont été capables de reconstruire l'image d'origine, en utilisant des techniques qu'ils n'ont pas révélées, bien qu'apparemment peu complexes techniquement².



2

Photo et vidéo Magic Number

En [programmation informatique](#), le terme ***magic number*** (en français « nombre magique ») peut désigner :

- une constante numérique ou un ensemble de caractères utilisé pour désigner un [format de fichier](#) ou un protocole¹ ;

- Les images [gif](#) utilisent le code ASCII `GIF89a` (47 49 46 38 39 61) ou `GIF87a` (47 49 46 38 37 61).
- Les images [JPEG](#) commencent par `FF D8` et finissent par `FF D9`. Les images [JPEG/JFIF](#) contiennent le code ASCII pour `JFIF` (4A 46 49 46) et se terminent par une [chaîne de caractères](#) vide. Les images [JPEG/Exif](#) contiennent le code ASCII pour `Exif` (45 78 69 66) et se terminent aussi par une chaîne nulle suivie d'autres [métadonnées](#).
- Les images [png](#) commencent par une signature de huit octets : `\211 P N G \r \n \032 \n` (89 50 4E 47 0D 0A 1A 0A). Cette signature permet la détection de problèmes de transmission : vu qu'elle contient des [sauts de ligne](#) (« \n »), cela permet de détecter par exemple les sauts de fin de ligne ajoutés automatiquement lors d'un [transfert en mode ASCII](#) par [ftp](#) (au lieu d'utiliser le mode binaire).

```
tenflo@FRMRSHOLT6809:~/Téléchargements/VM_write_share/ESIEA_VM$ hexdump -C Capture\ d'écran_2019-10-22_17-46-52.png
00000000  89 50 4e 47 0d 0a 1a 0a  00 00 00 0d 49 48 44 52  |.PNG.....IHDR|
00000010  00 00 01 d0 00 00 00 f1  08 06 00 00 00 7b da e6  |.....{..|
00000020  27 00 00 00 04 73 42 49  54 08 08 08 08 7c 08 64  |'....sBIT....|.d|
00000030  88 00 00 03 b6 49 44 41  54 78 9c ed d5 31 0d 84  |....IDATx...1..|
00000040  00 10 00 c1 e3 2d 50 61  00 ff d6 be 21 74 60 81  |....-Pa....!t`.|
00000050  6c 43 48 66 14 6c b7 cb  ba ed d7 00 00 8f 9c c7  |lCHf.l.....|
00000060  7f 66 66 7e 2f 77 00 c0  27 19 28 00 04 06 0a 00  |.ff~/w...'.(....|
00000070  01 01 02 03 04 05 06 07  08 09 0a 0b 0c 0d 0e 0f  |123456789abcde|
```


2

Photo et vidéo Cas concret

Un client recherche une taupe en son sein qui alimente un blog d'un avocat anglais diffusant des scandales à son sujet.

La première vague de l'investigation sur les postes des suspects ne donne rien alors le périmètre est élargi et les tablettes professionnelles sont également analysés.

Une vidéo effacée est retrouvée sur une tablette où l'on voit une personnalité politique filmé en douce durant une réunion.

Il n'a pas été prouvé que cet employé avait un lien avec l'affaire mais il a été licencié pour non-respect du règlement intérieur.



2

Photo et vidéo Cas concret

Une investigation sur une intrusion numérique indique qu'il y a des connexions non-identifiées depuis une des caméras de surveillance vers des serveurs en interne. L'analyse des caméras de surveillance a permis d'identifier qu'une faille est présente sur celles-ci qui permet de prendre la main en tant que *root* sans besoin d'être identifié. Le prix d'une analyse inforensique de la centaine de caméra étant trop élevé, il a été décidé de mettre à jour les caméras sans avoir pu identifier l'attaquant qui a utilisé les caméras comme rebond.

```
msf exploit(linux/http/axis_srv_parhand_rce) > sessions -i 5  
[*] Starting interaction with 5...  
  
id  
uid=0(root) gid=0(root)
```

1

Hardware

2

Investigation en ligne

3

Photo et vidéo

Si on résume ensemble :

- Introduction
- Connectiques des disques durs
- Connectiques des périphériques amovibles
- Médias pouvant contenir de l'information
- Générateur d'identité
- Masquer une identité d'un agent sous couverture
- Recherche sur les antécédents d'une personne
- Cybercrime
- OSINT
- Les types de fichiers photos
- Altération d'image
- Magic Number

Conclusion

NCIS



What my friends think I do.



What my mom thinks I do.



What society thinks I do.



What my boss thinks I do.



What I think I do.



What I actually do.

MERCI

www.squad.fr

PUBLIC

