



Les Fake News



Tous les jours, sur Internet et plus particulièrement sur les réseaux sociaux tels que Facebook ou Twitter, vous êtes confrontés à toutes sortes d'informations. Mais, sur le Web, tout le monde peut publier des contenus et les diffuser librement sans qu'ils soient vérifiés.

Alors, comment s'assurer qu'une information est vraie avant de la partager ?

L'activité suivante va vous plonger au cœur des **Fake News** !

➤ Définition

La définition et la traduction du terme « **fake news** » en français a été l'un des premiers axes du débat autour de cette notion. Le *Collins dictionary*, qui a fait de ce terme son mot de l'année 2017, définit les fake news comme « une information fausse, souvent sensationnelle, diffusée sous le couvert de reportages ». Certains ont traduit dans un premier temps « **fake news** » par « **fausse nouvelle** ». La Commission d'enrichissement de la langue française a inventé le mot « **infox** », forgé à partir des mots « **information** » et « **intoxication** ». Elle définit l'infox comme une information « mensongère ou délibérément biaisée », servant par exemple « à défavoriser un parti politique, à entacher la réputation d'une personnalité ou d'une entreprise, ou à contrer une vérité scientifique établie ».



“Il est temps que chaque acteur compétent engage la bataille d'influence sur le marché cognitif en faveur de la démocratie de la connaissance et de la pensée méthodique pour faire reculer, partout les savants d'illusion.”

G. Bronner, dernière phrase de *La démocratie des crédules*, 2013

“Celui qui contrôle les images contrôle les esprits. ”



Bill Gates





➤ Articles du web

Lisez attentivement ces deux articles trouvés sur le web :

- Jean-Luc Melenchon se justifie après l'achat d'un jet privé : 
<http://www.legorafi.fr/2013/07/01/jean-luc-melenchon-se-justifie-apres-lachat-dun-jet-prive-par-le-parti-de-gauche/>
- « Quand je serre la main d'un pauvre je me sens sale pour toute la journée » Emmanuel Macron : 
<http://www.legorafi.fr/2016/06/01/emmanuel-macron-quand-je-serre-la-main-dun-pauvre-je-me-sens-sale-pour-toute-la-journee/>



1. Ces informations vous semblent-elles fiables ?
2. D'autres médias mentionnent-ils ces infos ? Vérifiez sur Internet. Que pouvez-vous en déduire ?
3. Lisez les titres des articles suggérés à droite de l'image : que pensez-vous de ces sites Web ? Définissez le terme de « pièges à clics ».

1. Le Fact checking

La **vérification des faits** est une technique consistant d'une part à vérifier en temps instantané la véracité des faits et l'exactitude des chiffres présentés dans les médias par des personnalités politiques et des experts, d'autre part à évaluer le niveau d'objectivité des médias eux-mêmes dans leur traitement de l'information. Cette notion est apparue aux États-Unis dans les années 1990 sous l'appellation de « **fact checking** ».

Quelques sites de vérification de l'info

<https://www.lemonde.fr/verification/> 





Un blog recensant 30 méthodes pour dépister les fake news :

<https://blog.digimind.com/fr/tendances/fake-news-ressources-essentielles-pour-apprendre-comprendre-lutter-contre>



2. Quelques exemples



<https://www.lefigaro.fr/actualite-france/2015/01/05/01016-20150105ARTFIG00179-l-araignee-la-plus-dangereuse-du-monde-retrouvee-dans-un-magasin-bio.php>



<https://www.20minutes.fr/insolite/1509267-20150104-haute-savoie-trouve-araignee-mortelle-bananes>

4. Ces deux journaux ont publié la même information. Vérifiez la qualité de ces quotidiens à l'aide du **Decodex**. Sont-ils des sources fiables ?
5. Peut-on en conclure que cette information est véridique ? Effectuez tout de même une recherche sur Google afin de voir si d'autres sites traitent de ce même sujet et décrivez vos résultats.
6. D'après vos résultats, que peut-on en conclure sur la véracité de cette information ?

3. Analyse de vidéo

a. Les effets spéciaux

Regardez ces deux vidéos :

https://youtu.be/_sBBaNYex3E

<https://youtu.be/wQauv7vWSBo>



7. D'où proviennent ces vidéos (de quel compte) ?
8. Laquelle est fausse ? Qui sont les véritables auteurs de la parodie ?
9. D'après vos recherches, et maintenant que vous en savez plus sur cette vidéo, pourriez-vous la relayer sur les réseaux sociaux ? Pourquoi ?

b. Le Deep Fake



Le **deepfake** ou l'**hypertrucage** est une technique de synthèse d'images basée sur l'intelligence artificielle. Elle sert principalement à superposer des images et des vidéos existantes sur d'autres images et/ou vidéos (par exemple : le changement de visage d'une personne sur une vidéo). Le terme **deepfake** est un mot-valise formé à partir de **deep learning** (« apprentissage profond ») et de **fake** (« faux »)



10. Quelles peuvent-être les dérives du deep fake ?



➤ Les enjeux de la vérification de l'image

Voici 3 captures d'écrans issus de Facebook



Pique nique dans le cimetière de Calais !
Aucune image ni info à la TV ! C'est ce que l'on appelle..... La chance pour la France
Réfléchissez, juste un instant, en vous disant que les tombes de ce cimetière pourraient être celles de vos parents. Mais, ce n'est pas important, cela se passe à Calais, et ça ne vous concerne pas parce que vous ne les connaissez pas.
Alors, c'est vous qui voyez.... See More

Share

5

24,784 shares

2 Comments

Patrick Payen scandaleux
September 16 at 10:55am

Lecroq Marie Laure Dans quel monde on vit !
quel pays pour nos enfants ? On veut du respect de la tolérance et là on dit quoi ?

11. Retrouvez le contexte exact de chacune de ces images ?
12. Commentez l'utilisation et le partage de ces images ?



➤ Synthèse

Comme vous l'avez découvert, sur Internet, l'information peut être trompeuse...

Certaines personnes diffusent et partagent de fausses informations, parfois par ignorance, parfois dans un but idéologique, ou bien simplement pour faire le buzz.

- ✓ Même les sources les plus fiables peuvent par moments se laisser berner et publier des informations erronées.
- ✓ Avant de partager un article, une image, ou une vidéo sur les réseaux sociaux, il est donc important de se poser les bonnes questions, et d'utiliser pour cela les bons outils.

L'information me paraît-elle vraisemblable ?

- Le site sur lequel j'ai trouvé cette information est-il fiable et sérieux ? (Decodex)
- Quelles sont ses sources ? Qui a publié ce contenu en premier ? (Google Images Reverse)
- D'autres sites sérieux traitent-ils du même sujet ? (Google)





➤ Comment savoir si une photo a été retouchée ?

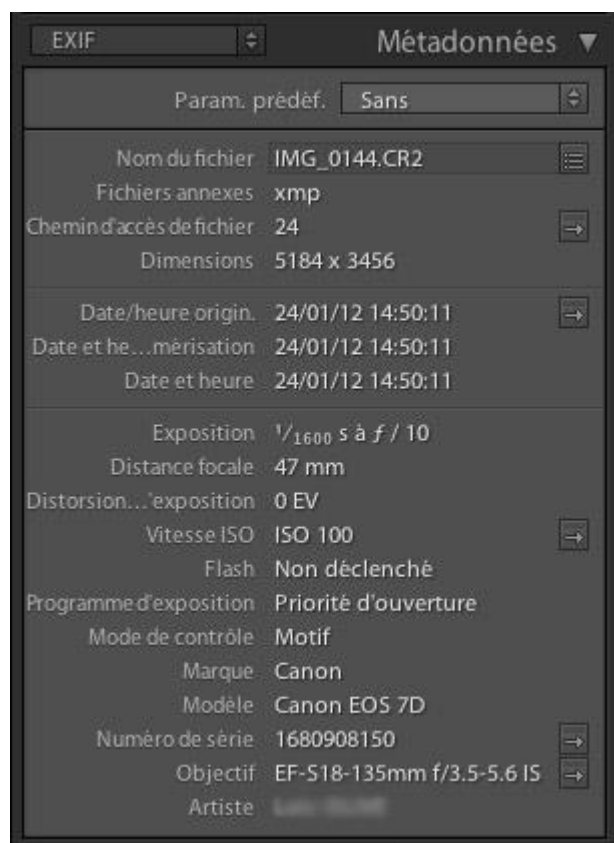
Les photos retouchées sont partout ! Des mannequins à la peau parfaite et aux formes qui le sont tout autant, aux publicités présentant des produits flatteurs ou encore des photos insolites que l'on retrouve sur le net. Difficile du coup de croire ce que l'on voit (St Thomas à des soucis à se faire...). Comment, dès lors, être sûr que la photo qui s'affiche sous nos yeux a été retouchée ou pas ?

1. Les métadonnées

Les photographes méticuleux qui ont connu l'époque de la photographie argentique et qui voulaient progresser avaient presque tous un carnet. Après chaque photo, ils le sortaient et notaient les principaux paramètres de prise de vue (date, vitesse, diaphragme, mémorisation d'exposition etc.). Cela permettait ainsi d'analyser à posteriori les choix qui avaient été faits et de voir, quelques jours plus tard une fois la pellicule terminée et développée, si les paramètres choisis étaient les bons.

Ces carnets ou cahiers ont bien évidemment disparu le jour où les appareils photos numériques sont arrivés. **Aujourd'hui, une bonne partie de ces informations sont enregistrées dans votre photo au moment de la prise de vue. C'est cela que l'on appelle les données Exif.**

Exchangeable image file format ou EXIF



La liste des données Exif (Exchangeable image file format) intégrées par vos appareils photos numériques regroupe foule d'informations parmi lesquelles :

- La date et l'heure à laquelle la photo a été prise.
- Les paramètres de prise de vue (vitesse, diaphragme, sensibilité ISO, mémorisation d'exposition, etc.)
- La géolocalisation de l'image (pour les appareils équipés de la fonction GPS).
- L'identification du type de boîtier et d'objectif (y compris les numéros de séries)
- Les informations relatives aux droits d'auteur et au copyright (si vous avez enregistré votre nom dans votre appareil)





a. Comment lire ces données Exifs ?

Il existe trois possibilités pour afficher les données Exif contenues dans vos photos :

1. Via le système d'exploitation de votre ordinateur. Sachez toutefois que les données affichées se limitent à quelques paramètres de prise de vue et informations sur le matériel.
 - Sous **Windows** : cliquez du bouton droit sur l'image, allez dans « propriétés » puis sur l'onglet « Détail ».
 - Sous **Mac OS** : cliquez également du bouton droit puis allez sur « Lire les informations ».
2. Via votre logiciel de retouche photo favori. Là aussi, si les données affichées sont généralement plus nombreuses (ça dépend du logiciel), elles ne sont pas non plus affichées en totalité
3. Via l'un des logiciels gratuits: Exif Reader. C'est la seule solution pour avoir accès à l'ensemble des données.
4. Via le site internet **Fotoforensics** (voir plus loin) : **solution la plus efficace !**

Conclusion : Connaître les données EXIF, c'est connaître les conditions initiales de la prise de vue.

➤ Les outils pour décoder une image truquée

Il existe deux solutions logicielles pour détecter les photos retouchées.

1. Jpegsnoop

La vérification automatique de l'authenticité d'une photo va être rendue possible par l'utilisation d'un petit logiciel gratuit : **JPEGsnoop**.

Comment fonctionne JPEGsnoop ?

Ce logiciel va examiner les données Exif de votre image (données techniques intégrées dans votre photo au moment de la prise de vue et lors du traitement par votre logiciel de retouche photo) et comparer son taux de compression à sa base de données regroupant des informations sur des milliers d'appareils photos. De cette analyse, JPEGsnoop déterminera si votre image est brute ou pas.

Du coup, l'examen des données Exifs par le logiciel va vous permettre d'apprendre pas mal de choses sur la photo (appareil photo et logiciel de retouche utilisé, paramètres de prise de vue, etc...)

Utilisation de JPEGsnoop

Son utilisation est archi simple : après avoir installé le logiciel sur votre PC, il vous suffit d'ouvrir la photo (File/Open Image...) et de cliquer sur OK. Allez ensuite au bas des inscriptions qui apparaissent à l'écran et regardez les dernières lignes

Une classe allant de 1 à 4 apparaît et vous permet de savoir ce qu'il en est :

- **class 1** : la photo a été retouchée (*image is processed/edited*)
- **class 2** : l'image a une grande probabilité d'avoir été retouchée (*image has high probability of being processed/edited*)
- **class 3** : l'image a une grande probabilité d'être une photo originale (*image has high probability of being original*)
- **class 4** : incertitude de savoir s'il s'agit d'une photo originale ou retouchée (*uncertain if processed or original*)



Prenons l'exemple de cette photo de langouste géante trouvée sur le net. L'analyse de la photo par **JPEGSnoop** laisse apparaître qu'il s'agit d'une photo truquée (class 1).



Searching Compression Signatures: (3347 built-in, 0 user(s))

EXIF.Make / Software	EXIF.Model	Quality	Subsamp Match?
CAM: [SONY]	[CYBERSHOT U]	[]	[] Yes
SW : [Adobe Photoshop 7.0]	[]	[Save As 07]	[]
SW : [Apple Quicktime]	[]	[0466-0467]	[]
SW : [Digital Photo Professional]	[]	[05]	[]
SW : [IJG Library]	[]	[075]	[]
SW : [MS Paint]	[]	[]	[]
SW : [MS Visio]	[]	[]	[]
SW : [ZoomBrowser EX]	[]	[Low]	[]

The following IJG-based editors also match this signature:

SW : [GIMP]	[]	[075]	[]
SW : [IrfanView]	[]	[075]	[]
SW : [IdImager]	[]	[075]	[]
SW : [FastStone Image Viewer]	[]	[075]	[]
SW : [NeatImage]	[]	[075]	[]
SW : [Paint.NET]	[]	[075]	[]
SW : [Photomatix]	[]	[075]	[]
SW : [XnView]	[]	[075]	[]

Based on the analysis of compression characteristics and EXIF metadata:

ASSESSMENT: Class 1 - Image is processed/edited

This may be a new software editor for the database.
If this file is processed, and editor doesn't appear in list above,
PLEASE ADD TO DATABASE with [Tools->Add Camera to DB]

2. FotoForensics

L'autre solution de détection automatique est de se rendre sur **FotoForensics** pour une analyse en ligne de votre image.



<http://fotoforensics.com/>

Submit a JPEG or PNG for Forensic Analysis

Image URL:

or

Upload File:

b. Comment fonctionne FotoForensics ?

FotoForensics a une méthode d'analyse radicalement différente de **Jpegsnoop** puisqu'il examine les différences de compression de votre image. Il en ressort une représentation graphique ou apparaît le **ELA**.

ELA : (Error Level Analysis), l'analyse du niveau d'erreur est l'analyse des artefacts de compression dans les données numériques avec une compression avec perte telle que JPEG.

c. Utilisation de FotoForensics

Entrez simplement l'adresse URL de l'image ou uploadez-la sur le site puis cliquez sur le bouton « Upload URL » ou « Upload Picture ». Une image globalement noire apparaît sous la photo d'origine : c'est la représentation ELA.

Pour analyser cette représentation graphique, il convient de la comparer à l'image d'origine.



Les zones de texture ou de couleurs similaires (le ciel, l'herbe, un vêtement etc.) doivent apparaître de la même façon et uniformément. Si par exemple une zone de ciel apparaît différemment, cela signifie que le niveau de compression est différent et que par conséquent, cette zone a été retouchée.

Exemple :

Je supprime la barque rouge présente au premier plan sur cette photo.



On voit clairement en bas à droite que la **représentation ELA de la mer n'est pas uniforme**. Celle-ci est plus foncée et indique la zone qui a été retouchée.

De plus FotoForensics permet d'afficher l'ensemble des métadonnées de la photo ainsi que les pixels cachés !

d. Les limites de FotoForensics

La détection n'est pas optimale sur les images Jpeg enregistrées plusieurs fois (ce qui est malheureusement souvent le cas des photos trouvées sur le net). La mauvaise qualité Jpeg perturbe la détection ELA qui apparaît alors majoritairement en noir. L'analyse des images ne peut se faire que sur des photos au format Jpeg ou Png.

➤ Conclusion

Vous l'avez compris, il n'existe pas de solution miracle pour identifier à coup sûr, une photo retouchée. FotoForensics offre malgré tout, une analyse plus poussée et plus intéressante que Jpegnoop car il permet de localiser la ou les zones suspectes.



➤ Exercice

Pour chacune des images ci-dessous, déterminez si elle a été truquée et comment.

Les images se situent dans le dossier « Images » de votre activité.

Image 1 - Jesus dans de l'herbe	Image 2 - Les 3 singes
	
Contexte	Contexte
Un utilisateur de Reddit poste la photo de son hashish	Photo illustrant le mythe des 3 singes : https://fr.wikipedia.org/wiki/Singes_de_la_sagesse

Image 3 - Kim Jung Un	Image 4 - Un pilote de la Nasa
	
Contexte	Contexte
Le dictateur Kim Jung Un expose la disquette contenant les codes de l'arme nucléaire Nord-Coréenne	Pilote de la NASA posant devant son appareil

Image 5 - Président Polonais	Image 6 - Exotropie
	
Contexte	Contexte
Le 13 décembre 2014, Pressmix.eu a publié un éditorial satirique (de l'auteur "drhumor") montrant le président polonais Komorowski en train d'embrasser la main de l'ancien dirigeant communiste Jaruzelski.	L'exotropie, ou avoir les deux yeux tournés vers l'extérieur, est parfois appelée "yeux de coq" ou "yeux de mur".



Image 7 - L'affaire du trône d'or



Contexte

Des semaines de troubles et de violences en Ukraine ont été suivies d'un bref coup d'Etat, le dirigeant ukrainien, Viktor Ianoukovitch, ayant fui son pays le 22 février 2014. Les photos de son palais somptueux ont commencé à apparaître dans les réseaux sociaux. Malheureusement, les médias ont du mal à contrôler les images trouvées sur Twitter et Facebook.

L'un des tweets présentait une toilette ornée.
[https://twitter.com/JF991/status/437258805340934145/photo/](https://twitter.com/JF991/status/437258805340934145/photo/1)

1

Image 8 - M. Sanchez sur l'Everest



Contexte

https://www.instagram.com/p/B4SH1Jwo2dT/?utm_source=ig_web_copy_link

➤ Décoder les média

Activité débat sur wooclap

<https://www.wooclap.com/SIZPQE>



**Le centre pour l'éducation
aux médias et à l'information**

