Protéger ses sources, sécuriser ses données

Manach Jean-Marc
jmm@rewriting.net
30/05/2022

Décrypter le monde pour mieux le raconter

Depuis 1969, le **CFPJ (Centre de Formation et de Perfectionnement des Journalistes)** est l'organisme de formation référent en journalisme et en Communication.

Nous sommes associés au CFJ, l'école de journalisme reconnue par l'État et faisons partie du groupe Abilways, multi-spécialiste de la formation continue.

7 BONNES RAISONS DE CHOISIR LE CFPJ

1 L'offre la plus complète et experte du marché

Le CFPJ accompagne les journalistes et tous ceux qui souhaitent transposer et adapter les techniques journalistiques à leurs pratiques professionnelles, dans le respect de règles éthiques et déontologiques.

2 Des professionnels qui forment

- Et non des formateurs professionnels.
- Des professionnels en activité, sélectionnés pour leur expertise, formés à la pédagogie via notre label ABILWAYS ACADEMY et évalués à chaque formation.

3 Des concepteurs de formation experts

- Responsables de l'actualisation des formations, ils assurent une veille permanente pour anticiper les évolutions du marché et maîtrisent les dernières techniques de pédagogie interactive et participative.
- L'offre de formation est actualisée chaque année.

4 Une pédagogie innovante

- Des techniques pédagogiques actives pour être acteur de sa formation.
- Des jeux pédagogiques pour apprendre en s'amusant.
- Des modalités distancielles pour se former où et quand on veut.

5 Une digitalisation de l'expérience apprenante

- Quiz, formations en ligne, blended learning, supports de cours dématérialisés pour suivre un parcours qui favorise l'engagement.
- Toutes les sessions peuvent être suivies à distance.

6 Un accompagnement jusqu'au financement

Un interlocuteur dédié pour vous conseiller dans vos choix de formation et de financement.

7 Une démarche qualité orientée clients et résultats

- Note Avis Vérifiés en 2020 **4,4/5** Avis Vérifiés
- Des critères qualité légaux respectés avec la qualification ISQ-OPQF et le référencement DATADOCK.
- Une e-évaluation de nos formations à chaud et à froid pour mesurer votre montée en compétences.

CFPJ, UNE MARQUE DU GROUPE ABILWAYS

ABILWAYS regroupe 6 marques complémentaires.
Ensemble, nous sommes plus forts. Chacune de nos marques est spécialisée dans un domaine de compétence ou sur une expertise métier.

SOMMAIRE

1. Une brève histoire de la sécurité informatique
   - Enigma & Alan Turing
   - Darpa & TCP/IP
   - PGP & les crypto wars (+ on dit chiffrer, par « crypter »)
   - Signal & E2EE & Telegram #Fails
2. Comprendre son modèle de menace
   - Snowden VS «Tous sur écoute »
   - Pegasus VS « 50 000 cibles potentielles »
   - Hygiène (de sécurité) informatique
   - Oubliez les « mots de passe »
3. Le kit de survie numérique
   - Le passeport de conseils aux voyageurs de l'ANSSI
   - EFF's Surveillance Self-Defense
   - Backup, Air Gap
   - Tor VS Darkweb + 1/4h d'anonymat
4. Comment gérer les lanceurs d'alerte
   - Primum non nocere + être joignable/à l'écoute
   - Lui faire comprendre son propre modèle de menace
   - Anonymiser les méta-données
   - La maison des lanceurs d'alerte

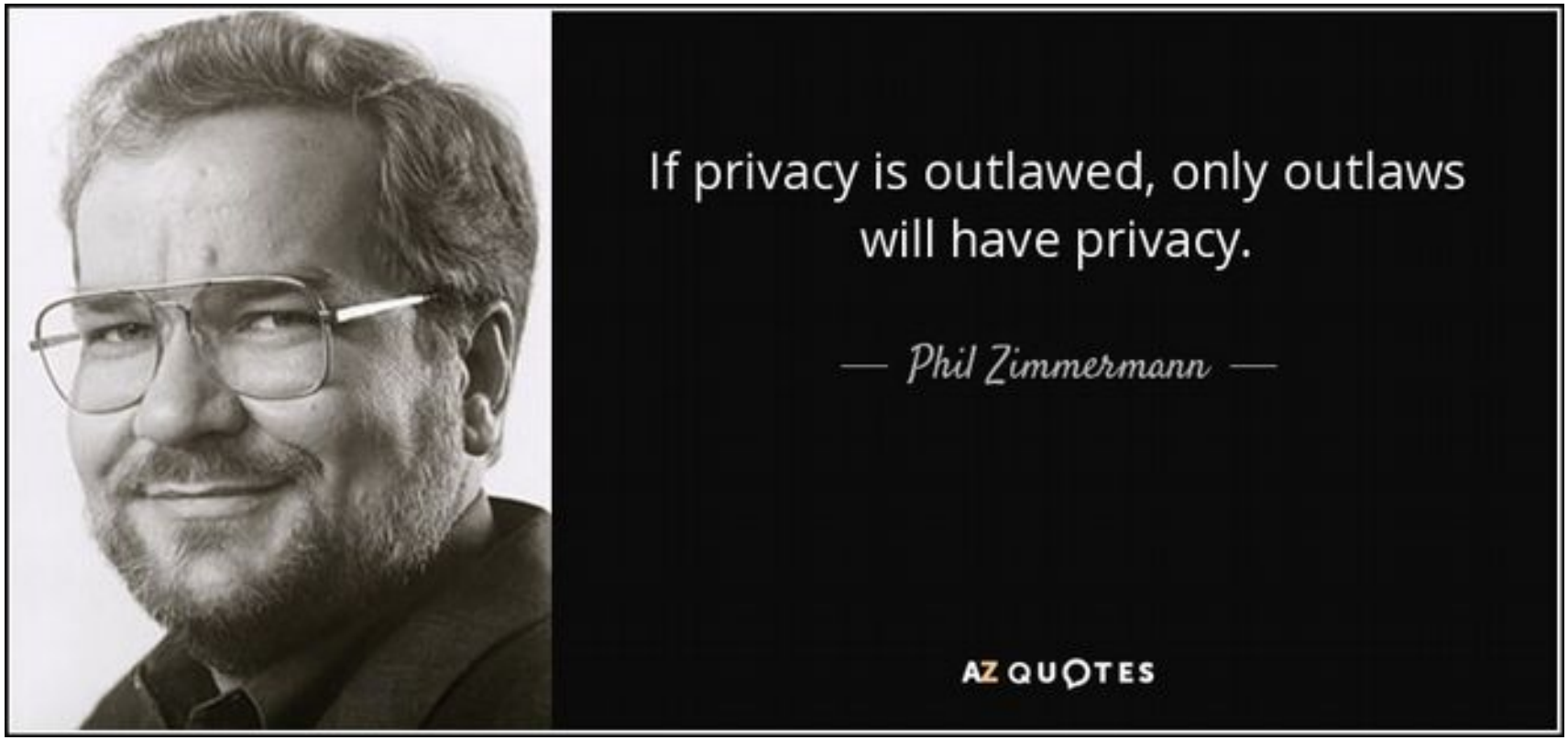
UNE BRÈVE HISTOIRE DE LA SÉCURITÉ INFORMATIQUE

- **https://www.franceculture.fr/emissions/lenigmatique-alan-turing**

UNE BRÈVE HISTOIRE DE LA SÉCURITÉ INFORMATIQUE

https://vimeo.com/311894477

UNE BRÈVE HISTOIRE DE LA SÉCURITÉ INFORMATIQUE



https://fr.wikipedia.org/wiki/Crypto_Wars

UNE BRÈVE HISTOIRE DE LA SÉCURITÉ INFORMATIQUE

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE

FEDERAL BUREAU OF INVESTIGATION

LAWFUL ACCESS

(U//FOUO) FBI's Ability to Legally Access Secure Messaging App Content and Metadata

(U//LES) As of November 2020, the FBI's ability to legally access secure content on leading messaging applications is depicted below, including details on accessible information based on the applicable legal process. Return data provided by the companies listed below, with the exception of WhatsApp, are actually logs of intent data that are provided to law enforcement in a non-real-time manner and may impact investigations due to delivery delays.

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE

App	iMessage	Line	Signal	Telegram	Threema	Viber	WeChat	WhatsApp	Wickr
Information Accessed									
Legal Process & Additional Details	• Message Content: Limited • Subpoena: can provide basic subscriber information • 18 U.S.C. §2703(d): can provide 25 days of iMessage lookups to and from a given number • Pen Register: no capability* • Search Warrant: can provide backups of a target device if target uses iCloud backup, the encryption keys should also be provided with content return; can also acquire iMessages from iCloud returns if target has enabled iMessages in iCloud	• Message Content: Limited* • Suspect's and/or victim's registered information (profile image, display name, email address, phone number, LINE ID, date of registration, etc.) • Information on usage "Maximum of seven days' worth of specified users' text chats [Only when LINE has been elected and applies and only when receiving an effective warrant; however, video, picture, files, location, phone call picks and other such data will not be disclosed]	• No Message Content • Date and time a user registered • Last date of a user's connectivity to the service	• No Message Content • No content information provided for law enforcement to pursue a court order. As per Telegram's privacy statement, for confirmed terrorist investigations, Telegram may disclose IP address and phone number to relevant authorities	• No Message Content • Hash of phone number and email address, if provided by user • Push Token, if push service is used • Public key • Date (in time) of Threema ID creation • Date (in time) of last login	• No Message Content • Provider account (i.e. phone number) registration date and IP address at time of creation • Message history: time, date, source number and destination number	• No Message Content • Accepts preservation letters and subpoenas, but cannot provide records for accounts created in China • For non-China accounts, they can provide basic information (name, phone number, email, IP address), which is retained for as long as the account is active	• Message Content: Limited* • Subpoena: can provide basic subscriber records • Court Order: Subpoena return as well as information like blocked users • Search Warrant: Provides address book contacts and all WhatsApp users who have the target in their address book contacts • Pen Register: Sent every 15 minutes, provides source and destination for each message *If target is using an iPhone and iCloud backups enabled, iCloud returns may contain WhatsApp data, to include message content	• No Message Content • Date and time account created • Type of device(s) account is tied to • Date of last use • Total number of messages • Number of inbound/outbound (email addresses and phone numbers) connected to the account, but not platform external IDs themselves • Avatar image • Limited records of recent changes to account, setting such as adding or suspending a device (does not include message content or routing and delivery information) • Wickr Version Number

SUBSCRIBER DATA	MESSAGE SYNDICATE/RECEIVER DATA	DEVICE BACKUP	IP ADDRESS	ENCRYPTION KEYS	DATE/TIME INFORMATION	REGISTRATION TIME DATA	USER'S CONTACTS

(U) Prepared by Science and Technology Branch and Operational Technology Division

7 January 2021

(U//LES) Apple provided logs only identify if a lookup occurred. Apple returns include a disclaimer that a log entry be

(U) LAW ENFORCEMENT SENSITIVE: The information marked (U//LES) in this document is the property of FBI and may be distri with a need to know. Distribution beyond these entities without FBI authorization is prohibited. Precautions should be taken to ens used in legal proceedings without first receiving authorization from the originating agency. Recipients are prohibited from subsequ

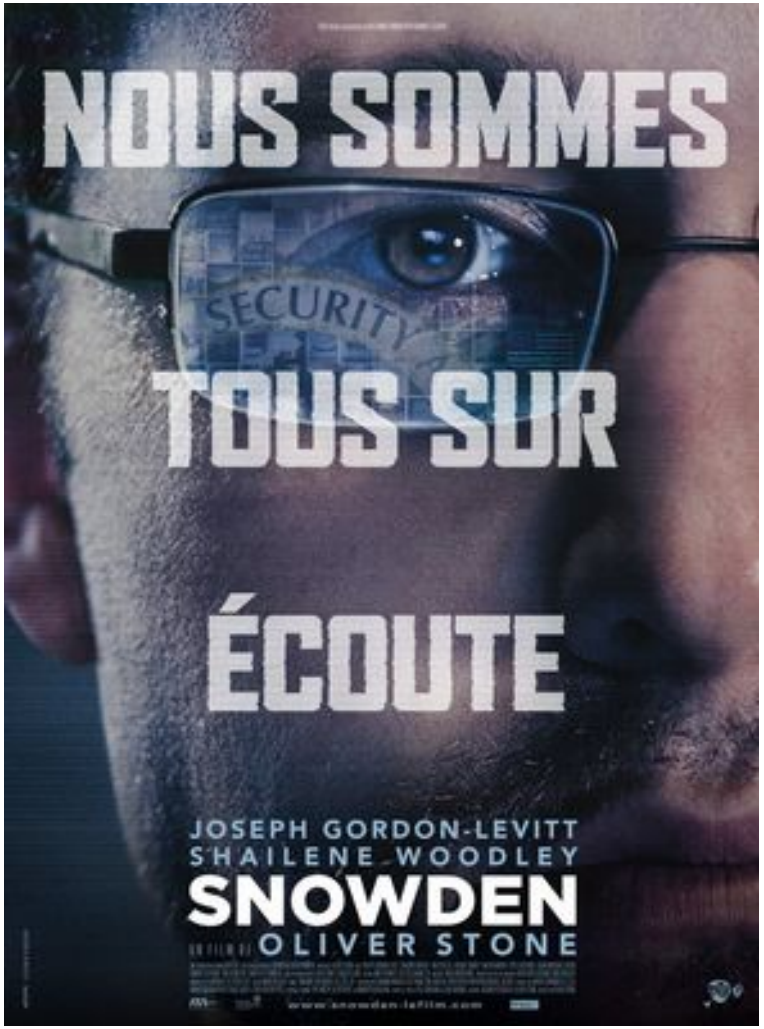
UNCLASSIFIED//LAI

Account	Information
[redacted]	N/A
[redacted]	Last connection date: [redacted] Unix millis Account created: [redacted] Unix millis

https://www.01net.com/actualites/
ent-revele-les-donnees-que-le-fbi

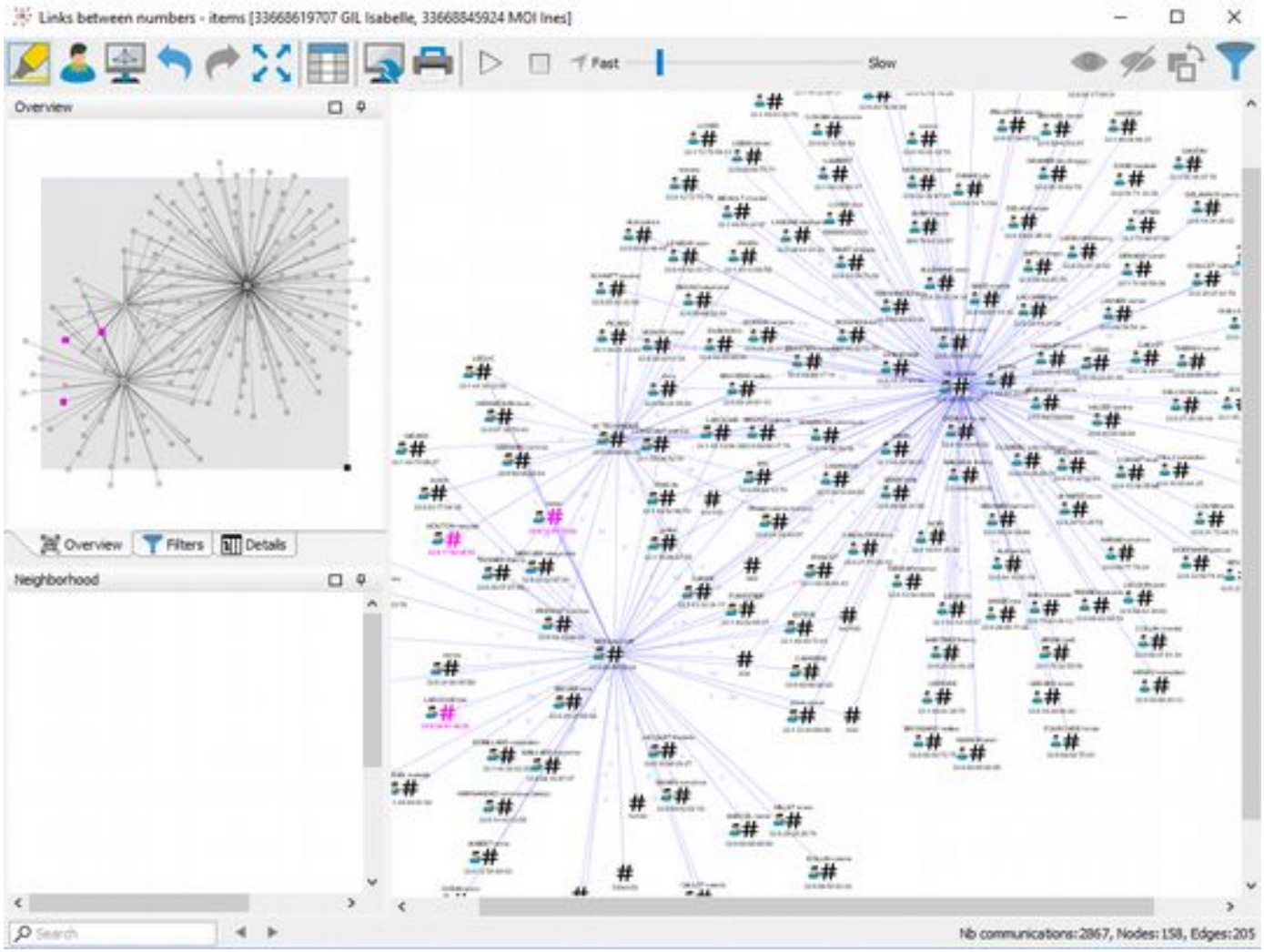
CFPJ

COMPRENDRE SON MODÈLE DE MENACE



http://bugbrother.blog.lemonde.fr/2015/01/03/de-la-surveillance-de-masse-a-la-paranoia-generalisee/

COMPRENDRE SON MODÈLE DE MENACE

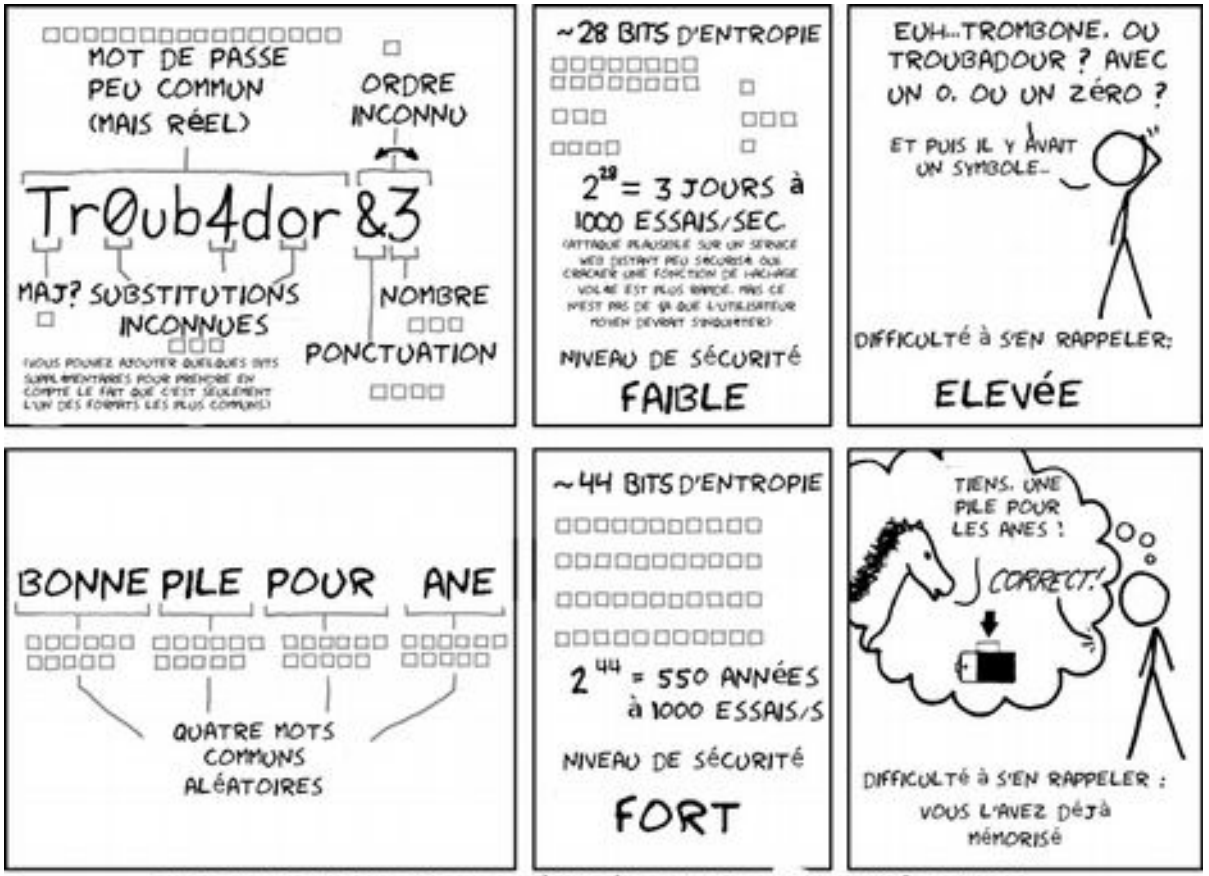


https://www.nextinpact.com/article/47791/pegasus-50-000-cibles-potentielles-12

COMPRENDRE SON MODÈLE DE MENACE

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/10-mesures-essentielles-assurer-securite-numerique

COMPRENDRE SON MODÈLE DE MENACE



https://www.nextinpact.com/article/48544/phrases-passe-cnil-passe-elle-aussi-en-mode-2-0

LE KIT DE SURVIE NUMÉRIQUE

https://www.ssi.gouv.fr/guide/partir-en-mission-avec-son-telephone-sa-tablette-ou-son-ordinateur-portable/

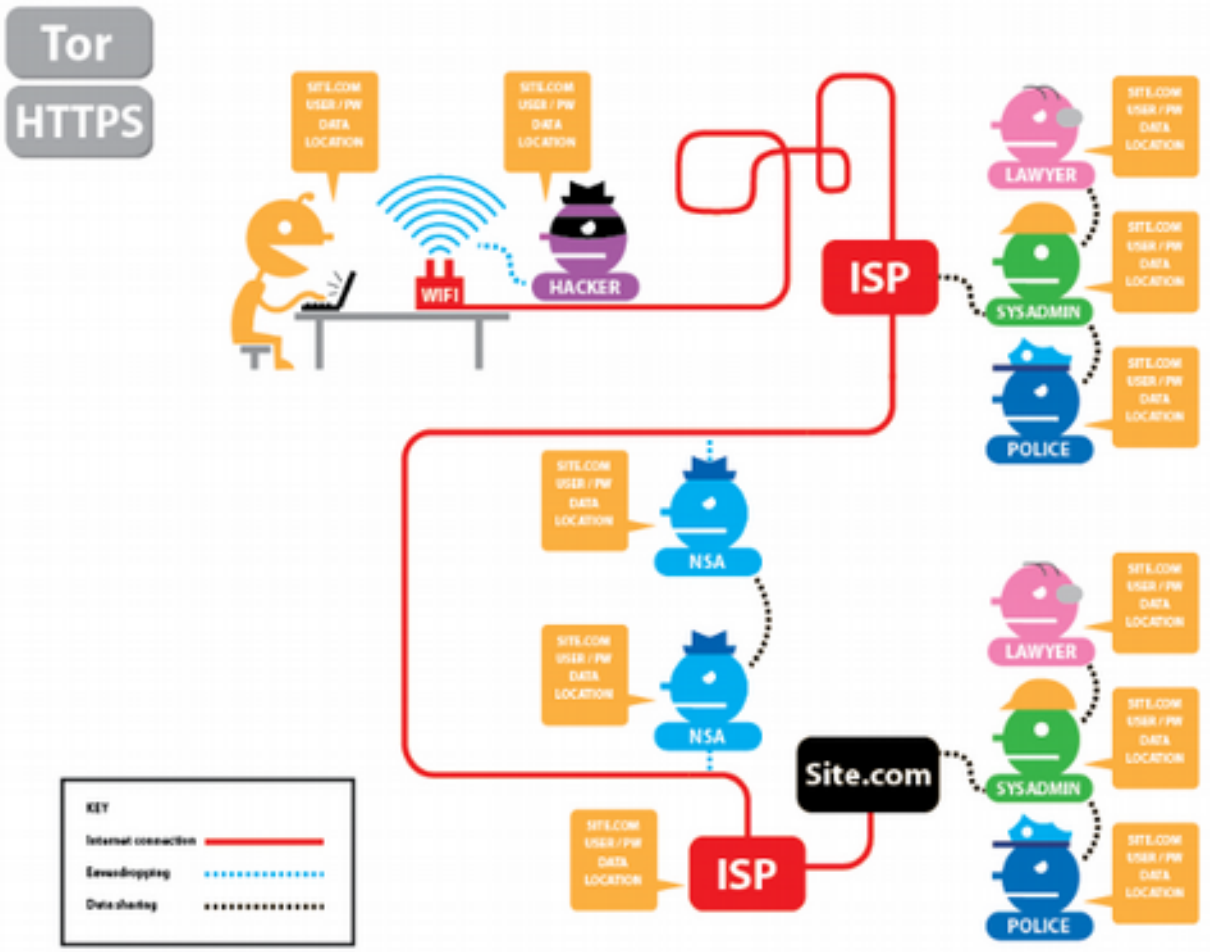
LE KIT DE SURVIE NUMÉRIQUE

https://ssd.eff.org/en

LE KIT DE SURVIE NUMÉRIQUE

https://anonymousplanet-ng.org/

LE KIT DE SURVIE NUMÉRIQUE

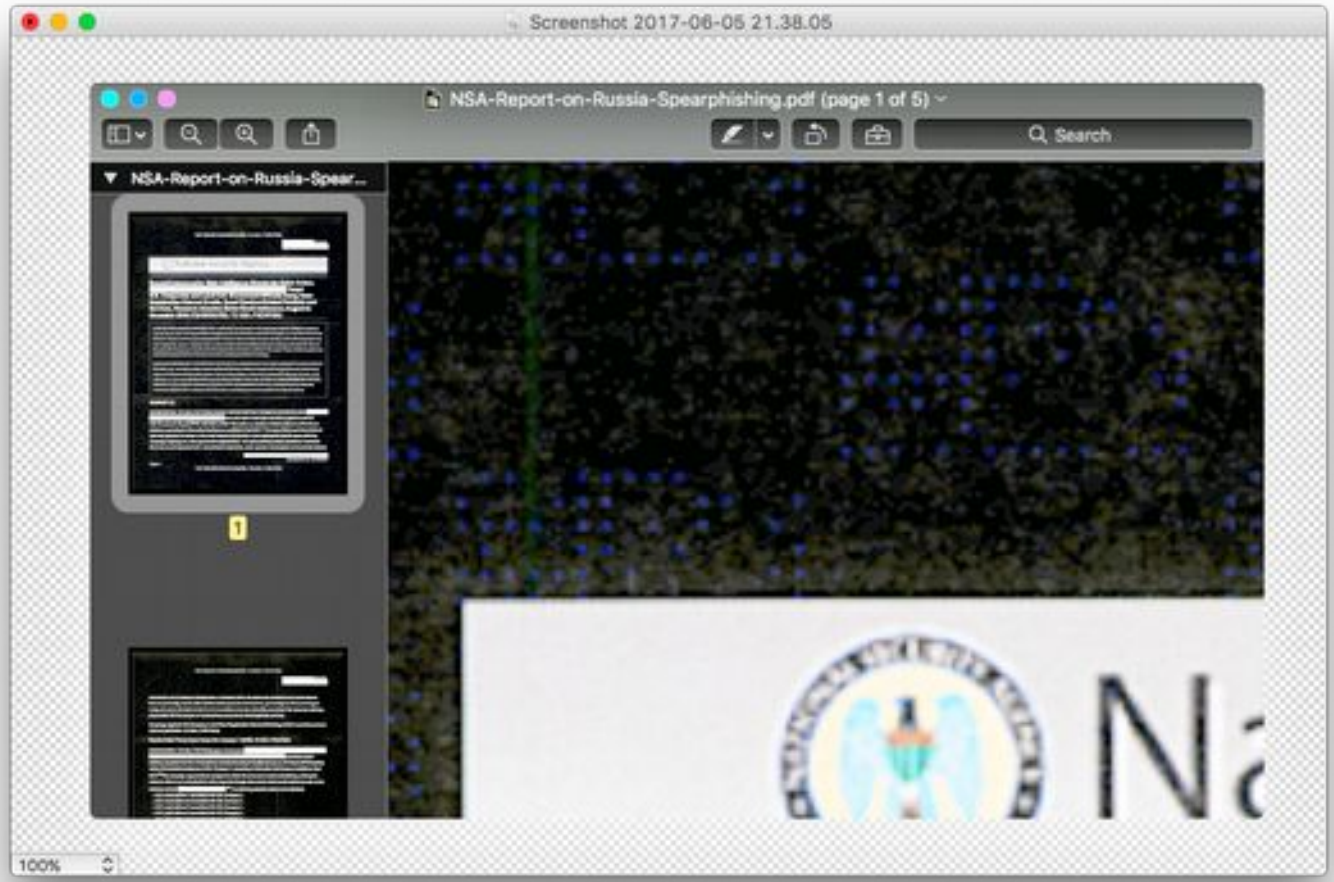


https://www.eff.org/pages/tor-and-https

COMMENT GÉRER LES LANCEURS D'ALERTE

http://web.archive.org/web/20171130074638/http://www.wefightcensorship.org/fr/online-survival-kithtml.html

COMMENT GÉRER LES LANCEURS D'ALERTE



https://blog.erratasec.com/2017/06/how-intercept-outed-reality-winner.html

Basic Image Information

Camera:	Apple iPhone 4S
Lens:	4.3 mm
Exposure:	Auto exposure, Program AE, 1/20 sec, f/2.4, ISO 125
Flash:	Off, Did not fire
Date:	**December 3, 2012** 12:26:08PM (timezone not specified) (2 hours, 44 minutes, 59 seconds ago, assuming image timezone of 6 hours behind GMT)
Location:	Latitude/longitude: **15**° 39' 29.4" North, **88**° 59' 31.8" West (15.658167, -88.992167) Photos on Jeffrey's blog that are near this location. Map via embedded coordinates at: Google, Yahoo, WikiMapia, OpenStreetMap, Bing (also see the Google Maps pane below) Altitude: 7.152159468 m Timezone guess from earthtools.org: 6 hours behind GMT
File:	**480 × 640** JPEG 132,481 bytes (0.13 megabytes) Image compression: 88% 4% crop of the 3,264 × 2,448 (8.0 megapixel) original
Color Encoding:	WARNING: Color space tagged as sRGB, without an embedded color profile. **Windows and Mac browsers and apps treat the colors randomly.** Images for the web are most widely viewable when in the sRGB color space and with an embedded color profile. See my Introduction to Digital-Image Color Spaces for more information.
Image URL:	http://assets.vice.com/content-images/contentimage/no-slug/[illegible].jpg Apply other tools to this image via ImgOps.com.

Main image displayed here at 70% width (49% the area of the original)

https://thenextweb.com/news/vice-leaves-metadata-in-photo-of-john-mcafee-pinpointing-him-to-a-location-in-guatemala

COMMENT GÉRER LES LANCEURS D'ALERTE

https://mlalerte.org

VOTRE FORMATEUR

(data)journaliste « hacker » d'investigation

Pionnier du journalisme d'investigation sur Internet, traducteur et auteur de nombreux manuels de sécurité informatique, « éleveur » de lanceurs d'alerte depuis l'an 2000 (dont aucun n'a jamais été identifié a posteriori).

Manach
Jean-Marc
jmm@rewriting.net

https://jean-marc.manach.net/
https://fr.wikipedia.org/wiki/Jean-Marc_Manach
https://twitter.com/manhack
https://www.linkedin.com/in/manhack

MERCI DE NOUS AVOIR CHOISI

Media Media

Communication Communication

Ceci pourrait vous intéresser :

Bloc au choix :

CONFÉRENCE

- De la surveillance de masse à la paranoïa généralisée
  https://video.passageenseine.fr/w/fe1f61cf-cc78-452a-8e4b-8a

WEBINARS

- Internet : la liberté sous contrôle ?
  http://communication-ccas.fr/jou

FORMATION

- Le MOOC de l'ANSSI
  https://secnumacademie.gouv.fr/

FORMATION CERTIFIANTE

- Défis et enjeux de la cybersécurité
  https://www.fun-mooc.fr/fr/cours/defis-et-enjeux-de-la-cybersecurite/

LIVRES BLANCS

- Guide d'auto-défense numérique
  https://guide.boum.org/

BLOGROLL

- Bug Brother
  https://www.lemonde.fr/blog/bugbrother/