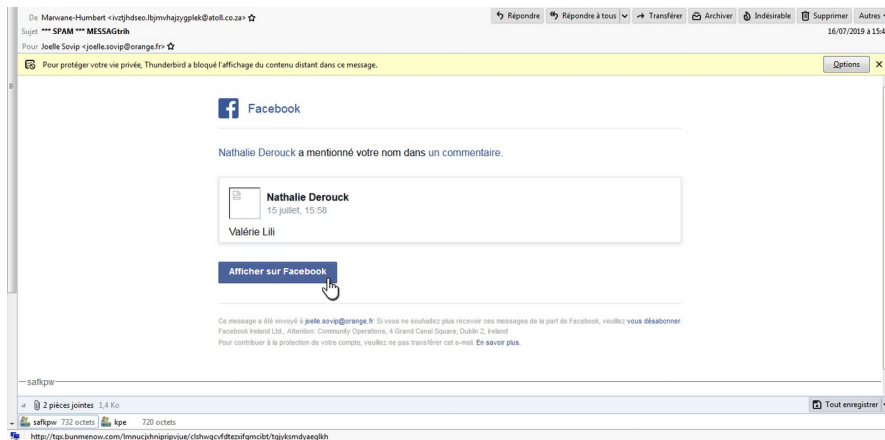


UN PREMIER MAIL SUSPECT

Voici un email que j'ai reçu →

Pour ouvrir la capture d'écran, cliquer sur [ce lien](#).



1. À quelle date et quel horaire ai-je reçu l'email ? _____
2. Quel logiciel de messagerie j'utilise ? _____
3. D'après ce mail, ai-je un compte Facebook ? _____
4. Entourer en vert sur l'image les éléments qui doivent vous sembler suspects.
5. Quel est l'intérêt que Thunderbird ait bloqué l'affichage du contenu distant ? _____
6. Pourquoi est-il écrit *** SPAM *** dans le sujet ? _____

7. En cliquant sur le menu *Affichage* du logiciel de messagerie, puis sur *Code source du message*, cela ouvre un fichier contenant du texte :

Je fais *clic droit* puis *Enregistrer sous*.

Je fais **Ctrl+S** pour enregistrer ce fichier sur mon ordinateur : le logiciel le nomme QUARANTAINE)8226.

Je décide de ne pas le renommer et l'enregistre.

Vous pouvez trouver ce fichier [ici](#).

Débrouillez-vous pour ouvrir ce fichier.

8. a) Déterminer l'adresse IP de l'émetteur. _____

b) Dans quel pays est « située » cette adresse IP ? _____

Comment avez-vous répondu à cette question ? _____

c) Est-il possible qu'à la date où j'ai préparé ce TP, l'adresse IP ne renvoie pas vers le même endroit ? _____

```

Source de : imap/johannathieu@orange.fr@imap.orange.fr@95f6c4%3EUID%3E/NBOXQUARANTAINE)8226 - Mozilla Thunderbird
Fichier : Affichage ?
Return-Path: <ivztjhdeo.lbjmhajzygplek@atoll.co.za>
Received: from minifsc05 (minifsc05 [10.223.111.55])
    by mail01708 with SMTPS;
    Tue, 16 Jul 2019 16:08:13 +0200
X-Sieve: GNU Sieve 2.3
Received: from atoll.co.za ([181.120.188.203])
    by minifsc05 with HE
    id 0575208@minifsc05; Tue, 16 Jul 2019 16:08:08 +0200
X-bcc: johannathieu@orange.fr
X-NE-bounce-domain: orange.fr
X-NE-origname: default
X-NE-spamcause: (285)(1800)gggrugvucftvghtrhhocutddrgduvduledtdgdejhecutefuodetggdotefrodftvcufvfhrohhfihhivgenucufog
X-NE-spamlevel: low
X-NE-IP: 181.120.188.203
X-NE-identity: off
X-holireno-Customer-Gid: shypqgvvrurkpoepoazn
X-nsccv-SIS-Outgoing: 1
Date: Tue, 16 Jul 2019 13:43:45 +0000
X-Abuse-Reports-To: abuse@bryanshelton.com
Message-Id: <CACAC1687A0818A0887054C4705EC12@atoll.co.za>
X-1-Mailer: 1
To: "Joelle Sovip" <joelle.sovip@orange.fr>
Subject: *** SPAM *** <utf-8?MSS&trish>
From: "Marvane-Humbert" <ivztjhdeo.lbjmhajzygplek@atoll.co.za>
X-mailin-client: 87573
Content-Type: multipart/mixed;
    boundary="-----91097806384ce311ed167fe89231ca09ca617f-----"
MIME-Version: 1.0
X-Livedata-To: psdjadngl:v3vyanwlbj:splio
  
```

COMPLÉMENTS : UN PROFIL FB PUBLIC ASSEZ FOURNI

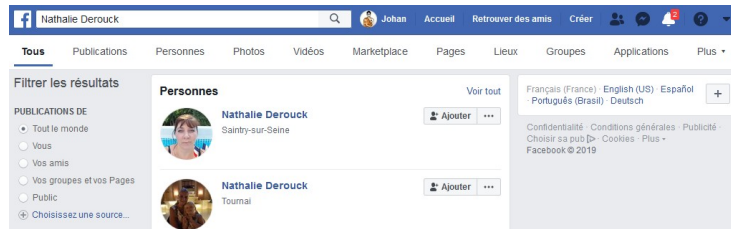
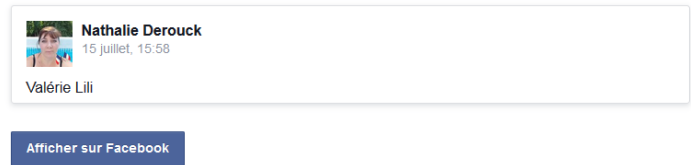
En ouvrant ce mail directement via la messagerie Orange, cela m'affiche :

[lien](#) vers la capture d'écran

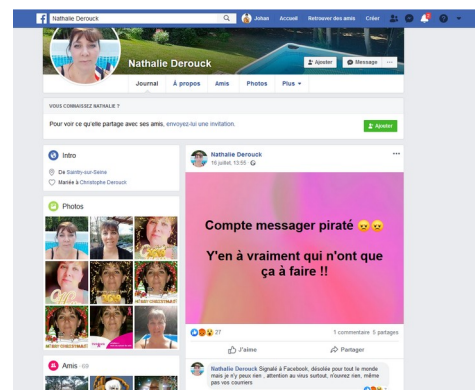
Mais qui est cette Nathalie Derouck ? Selon vous, est-ce une vraie personne ?

Je fais une recherche directement sur Facebook →

Nathalie Derouck a mentionné votre nom dans un commentaire.



e clique sur la première personne, dont l'image correspond →

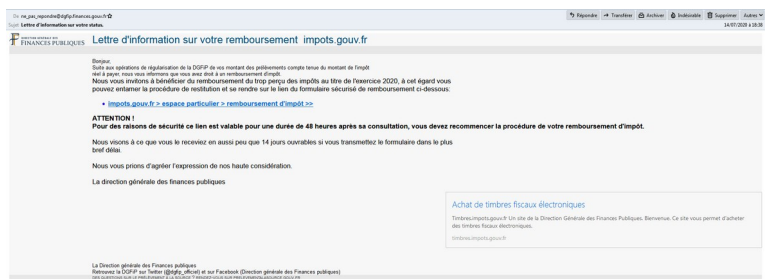


UN DEUXIÈME MAIL PLUS ÉLABORÉ

Voici un autre email, reçu le 14 juillet 2020 →

Pour ouvrir la capture d'écran, cliquer sur [ce lien](#).

Vous pouvez télécharger le code source de ce mail [ici](#).



1. Que pensez-vous de cet email ?

2. Le site <https://www.ip2location.com/free/email-tracer> est intéressant, car il permet de copier directement le code source d'un mail afin de visualiser son trajet, et donc de voir de quel pays il a été envoyé (à priori). Tester ce site (ou un autre « email tracer ») avec le code source de cet email.

3. Choisir un pourriel (*spam*) dans votre boîte de réception de mails, et l'analyser avec ces outils. Si vous n'en trouvez pas, je vous en fournis quatre : les télécharger [ici](#).