# Analyser les headers d'un Mail

**Date de dernière mise à jour : 19/05/2015 à 22:00**



Analyse de l'entête (Header) d'un Mail

Qu'est-ce qu'un header ?
Le header, (ou en-tête en français) c'est l'entête (CQFD) d'un fichier informatique ou d'un paquet transitant sur un réseau informatique, ce sont aussi les données contenues au début de ce fichier ou du paquet.En transmission de données, les données qui suivent le header sont souvent appelées charge utile ou **body**.source Wikipédia.fr : http://fr.wikipedia.org/wiki/Header

Les éléments du Header :
Dans un **Mail** (courrier électronique
), le texte (corps ou body
) est précédé par des lignes de header indiquant :

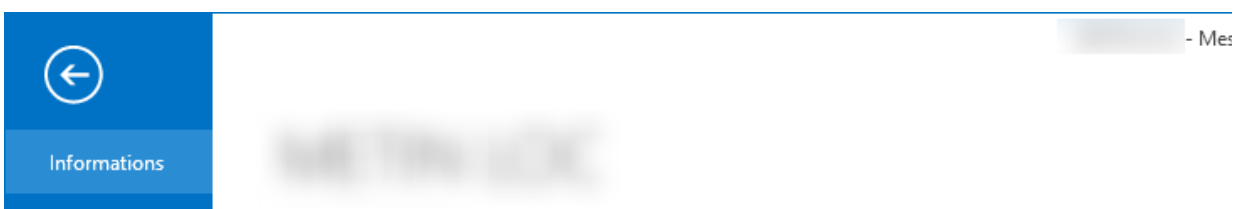
-l'expéditeur.
-le destinataire.
-le sujet.
-les timestamps
- d'envoi et de réception.
-le serveur de messagerie électronique final.
-etc...

Pour ceux qui veulent en savoir encore plus et que l'anglais ne rebute pas, vous pouvez toujours consulter la RFC 2822 "Format standard des messages sur Internet
" au tout début Internet s'appelait **ARPANET** NET pour contraction d'Internet , ce n'était pas "la toile
" immense que l'on connait maintenant.**- L'analyse par l'exemple :** Prenons l'exemple type d'un mail nous paraissant suspect, avec en objet du message un titre très racoleur, le but étant de déstabiliser, faire peur, faire croire à un gain, etc. au lecteur que vous êtes.On part du principe que vous avez rapatrié ce courrier dans votre client mail (Outlook, Thunderbird, etc...). Avant d'ouvrir le message, allons faire un tour dans les en-têtes (headers).

**- Comment récupérer l'entête d'un Mail dans son client mail ?**Selon votre client mail (logiciel que vous utilisez pour réceptionner vos emails), la procédure peut légèrement différer. Voici les procédures à utiliser pour les clients mails les plus courants :

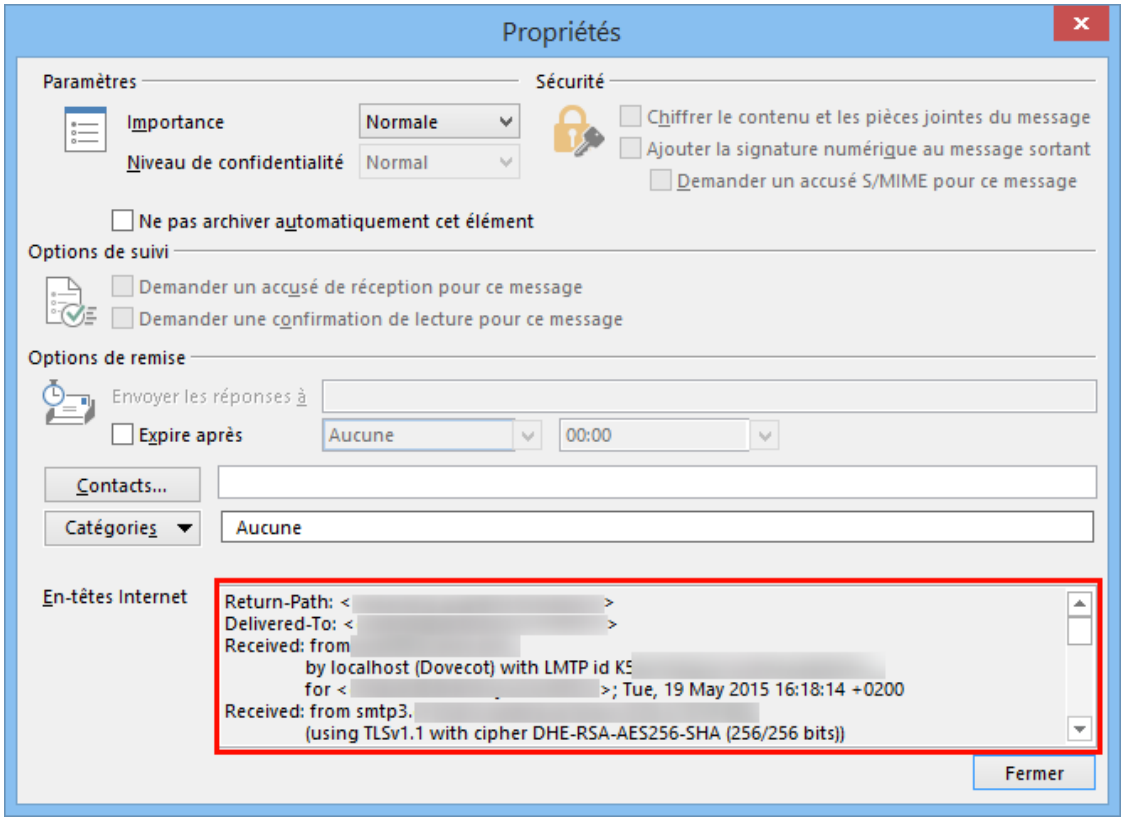
Outlook 2007
Effectuez un clic avec le bouton droit sur le mail, puis cliquez sur **Options des messages**. Dans la fenêtre qui s'ouvrira, en bas vous avez le fameux header (l'entête Internet).

Outlook 2010 et 2013
Vous devez ouvrir votre email dans une fenêtre séparée (et non pas dans le volet de lecture). Ensuite, cliquez sur le menu **Fichier => Informations**, puis sur le bouton **Propriétés**.



Propriétés d'un email (Outlook 2013)

Les en-têtes se trouvent dans la partie **En-têtes Internet** :




En-têtes d'un email (Outlook 2013)

Thunderbird

Allez dans l'onglet **Affichage**, et sélectionnez **Code source du message**.

Renseignements

Dans les en-têtes, on trouve les renseignements suivants :

Received: from server.exemple.fr(190.13.06.15) by smtp.votre-FAI.fr with ESMTP(SMTPD32-4.06)id A09D3203BC; Mon, 15 Nov 2010 14:19:42 EST
Received: from vilainpirate ([192.288.14.1]) by server1.exemple.fr (8.7.5) ID LAA28548; Mon, 15 Nov 2010 14:19:42 -0700 (MST)Message-Id:
Reply-To: hadopi@hadopi.frFrom: bisounours@chezlui.comTo: votre-adresse@votre-FAI.frSubject: Message important a votre attention ! - vous avez gagnezDate: Mon, 15 Nov 2010 13:19:38 +0100MIME-Version: 1.0Content-Type: text/plain;charset="ISO-8859-2"X-Priority:3X-MSMail-Priority:Normal
X-Mailer: Microsoft Outlook Express 4.72.3110.5

**note :**toutes les références de l'exemple sont fictives, toute ressemblance avec des éléments existants ou qui pourraient exister ne serait que pure coïncidence.

Nous allons détailler point par point la composition de cet en-tête.

Received: from server.exemple.fr(**190.13.06.15**)by smtp.votre-FAI.fr with ESMTP(SMTPD32-4.06)id A09D3203BC;Mon, 15 Nov 2010 14:19:42 EST
**Adresse IP du serveur par lequel à transité le message.**

Received: from vilainpirate ([**192.288.14.1**])
**Adresse IP du pirate.**

by server1.exemple.fr (8.7.5) ID LAA28548
**Serveur SMTP utilisé par le pirate.**

Message-Id:
**Nom réseau de l'ordinateur du pirate.**

Reply-To: **hadopi@hadopi.fr**
**Adresse ou sera acheminée votre réponse éventuelle.** (vous aurez remarqué la petite pointe d'humour)

From: **bisounours@chezlui.com**
**Adresse présumée du pirate (qui a sans doute été falsifiée).**

To: **votre-adresse@votre-FAI.fr**
**Votre adresse E-mail.** (F.A.I= Fournisseur d'Accès Internet)

Subject: Message important a votre attention !- vous avez gagnez
**Objet du mail.** (déjà avec ce genre de titre, moi je reste très suspicieux : attention aux fautes d'orthographe).

X-Mailer: Microsoft Outlook Express 4.72.3110.5
**Client mail utilisé par le pirate.**

Là, on dispose de l'essentiel, mais si on veut pousser un peu plus loin, on peut encore obtenir d'autres renseignements.

Received: from server.exemple.fr(190.13.06.15)by smtp.votre-FAI.fr with ESMTP(SMTPD32-4.06)id A09D3203BC;**Mon, 15 Nov 2010 14:19:42 EST**
Received: from vilainpirate ([192.288.14.1])by server1.exemple.fr (8.7.5) ID LAA28548;
**Mon, 15 Nov 2010 14:19:42 -0700 (MST)**

En gras, ce sont les "timestamp
" (littéralement parlant "timbre de temps
" c'est vrai que même en Français ce n 'est pas plus parlant)en fait pour être bref, c'est tout ce qui a trait aux éléments temporels sur les serveurs :

-le jour
-la date
-le mois
-l'année
-l'heure
-le décalage horaire
-le fuseau horaire

MIME-Version: 1.0
Sous cette abréviation ce cache le nom suivant : **Multipurpose Internet Mail Extension**, la définition sur Wikipedia nous dit ceci :

Wikipédia a écrit :
C'est un standard internet qui étend le format de données des courriels pour supporter des textes en différents codage de caractères autres que l'ASCII, des contenus non textuels, des contenus multiples, et des informations d'en-tête en d'autres codages que l'ASCII. Les courriels étant généralement envoyés via le protocole SMTP au format MIME, ces courriels sont souvent appelés courriels SMTP/MIME

Pour faire simple, dans notre cas **cela indique que le contenu du message est formaté en MIME. Sa valeur est typiquement "1.0"** en fait on est pas vraiment plus avancé

charset="ISO-8859-2"
**Renvoie le type de codage des caractères utilisés.**

On ne vas pas rentrer dans les détails, ça deviendrait trop technique.Dans le cadre de ce tutoriel, les derniers éléments n'ont pas grande importance, tout au plus cela vous permet de savoir quand le message à transité sur les différents serveurs, s'il y a un décalage horaire, au quel cas on peut connaitre le fuseau horaire, et enfin le type de codage de caractère qui à été utilisé.

Cet exemple est évidement très basique en soi, et ce serait vraiment trop réducteur de résumer en disant que tout les headers sont aussi simples.

Le principal y est, mais il y a bien plus sournois.

-le mail peut avoir transité par un ou des proxy,
-il peut y avoir une multitude de destinataires, leur boite mail servant de relais.
-il peut ne pas y avoir d'objet d'indiqué (auquel cas il faut être encore plus méfiant).
-Il peut y avoir des liens cliquables, qui vous renvoient sur une page d'un site détourné (phishing)
-il peut y avoir des pièces jointes avec des fichiers **.exe, .pdf, .jpeg, etc...**- (dans ce cas, avoir la certitude (**signature numérique et/ou cryptage**-) de la provenance, sinon n'ouvrez pas !)

A quoi peuvent servir les principaux éléments fournis par le header ?
On reste dans notre exemple type. Le fait de connaître l'adresse IP du serveur par lequel à transité le message permet de voir le chemin qu'il a emprunté, et mieux encore de connaître l'adresse IP du fameux pirate.

Avec ces éléments, il n'y a plus qu'a envoyer votre plainte à **abuse@exemple.fr** et/ou à **postmaster@exemple.fr** (bien évidement vous remplacerez exemple.fr
par le nom de domaine du F.A.I ou du serveur SMTP utilisé par le pirate), **abuse** et **postmaster** étant valides avec n'importe quel F.A.I.

La lecture de l'entête nous permet aussi de voir vers quelle adresse sera envoyé notre éventuelle réponse.

Comment éviter de rapatrier certains mails ?
Le principe c'est le filtrage en amont, donc directement sur le serveur mail de votre F.A.I.

2 solutions s'offrent à vous :

-Vous prenez le temps d'aller sur l'espace mail de votre F. A. I pour faire le tri, de vous à moi c'est assez fastidieux car cela vous contraint de passer par votre navigateur, aller sur le site votre F. A. I, puis dans votre espace client dans lequel vous devrez entrer votre login et mot de passe du compte, pour enfin accéder à votre boite mail. Franchement y a quand même plus simple.
-Vous passez par un petit logiciel, qui se chargera après configuration de lire vos emails situés directement sur le serveur de votre F. A. I et dans le cas ou vous ne souhaiteriez pas rapatrier certains mails, de les supprimer purement et simplement, sans avoir à ouvrir votre navigateur.

3 logiciels qui accomplissent parfaitement cette tache :

PopTray- : l'ancêtre dans le bon sens du terme
POP Peeper**3.8.1.0 Fr Free**-: le petit frère de PopTray (c'est celui que j'utilise actuellement) La dernière version est **<a href="http://www.esumsoft.com/download/?prod=pppro" rel="nofollow">POP Peeper Pro 4.0.1** mais uniquement disponible en shareware
Magic Mail Monitor- : un nouveau (enfin pour moi, car pas encore testé), ne nécessite pas d'installation.

Le principe reste le même pour les 3, ce qui peut faire la différence ce sont les options fournies, la facilité de prise en main, l''utilisation au quotidien, et enfin l'interface graphique, qui reste plus subjective, les goûts et les couleurs étant propres à chacun.

Voi  e pense qu'avec cette base vous serez plus attentifs dans la réception et la lecture de vos mails.