

# Como encontrar el origen de un email

## ***Siguiendo un e-mail – ¿Quién le envió ese e-mail?***

"¿Quién, y desde donde, le envió ese e-mail?"

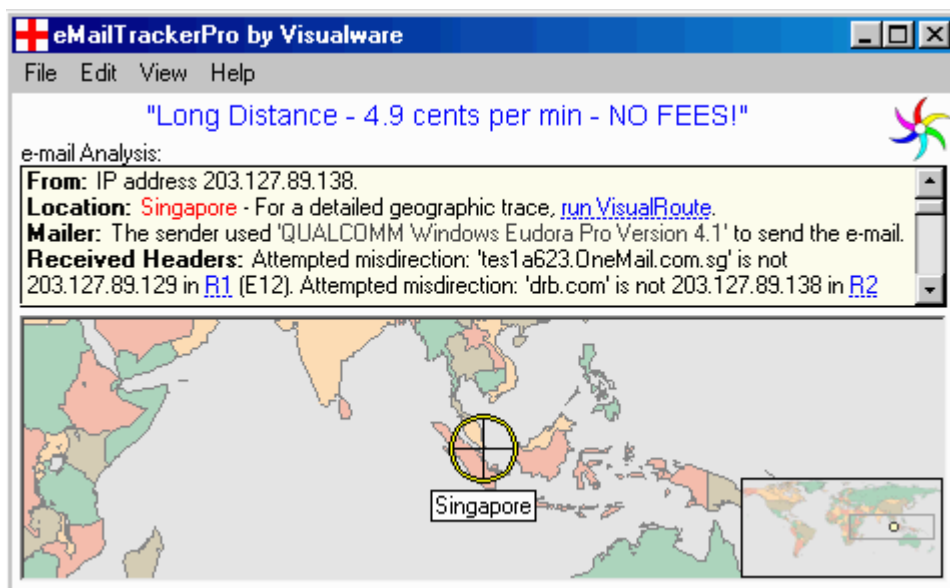
Con este tutorial como guía, un poco de investigación en el lugar exacto, una herramienta de rastreo de direcciones IP tal como [eMailTrackerPro](#) o [VisualRoute](#), Ud. Podrá, en muchos casos, imaginarse quién fue el que le envió ese e-mail inadecuado y reportarlo a las autoridades correspondientes...

De hecho, las personas que utilizan el correo de **Yahoo** o **Hotmail**, creyendo que sus identidades y ubicaciones permanecerán ocultas, podrían verse sorprendidas al saber que la dirección IP de la computadora que utilizó para enviar el e-mail puede ser descubierta con eMailTrackerPro y rastreada con VisualRoute (U otros utilitarios ampliamente difundidos actualmente), y que esa dirección, muchas veces conduce directamente a una persona.

¿Qué debe hacer? :

### 1. Use eMailTrackerPro

El Primer paso es utilizar una herramienta de análisis de e-mail como puede ser [eMailTrackerPro](#), que automáticamente analiza un e-mail y sus encabezados, proveyendo resultados gráficos como los siguientes:






**Identification Report for 'Cheap Pharmacy el'**

Host [211.125.211.2](#) has been found. It is probably located in or around **Japan** as this is where the organization or individual who manages the system is located.

This system is a web and secure web server (click [here](#) for details).

---

**Network Contact Information:** The following details refer to the network that the system is on.

 [hostmaster@nic.ad.jp](mailto:hostmaster@nic.ad.jp)  
 +81-3-5297-2312  
 Kokusai-Kougyou-Kanda Bldg 6F, 2-3-4 Uchi-Kanda Chiyoda-ku, Tokyo 101-0047, Japan

[Report a hacker, spammer or other type of Internet abuser.](#)

☐ [Click here to hide the in-depth information on this email](#) ([more info](#))

- This email is sent from the computer identified on the Internet by **211.125.211.2** (or hccd37dd302.bai.ne.jp).
- The sender claims to be **garyie@verizon.net**, but this is very easily forged and as such not necessarily reliable.
- At the time of sending, one email server (identified on the Internet by **211.125.211.2**) to which this email was apparently passed claimed to be known as **verizon.net**, but it does not currently have that name. Its name could have changed, but this is a common method used by hackers and spammers to misdirect users to their true location.

Si Ud. No tuviera un e-mail, pero posee una dirección de e-mail, podría usar la herramienta **eMailTracker** para rastrear cual es el e-mail server de ese usuario. Un beneficio extra es que Ud. Podrá ver cuál es el software de SMTP que ese mail server está ejecutando (muchas veces con información de la versión, también).

## 2. e-mail Internet Headers

Cada e-mail que se recibe tiene los "Internet Headers". Utilizando Microsoft Outlook como ejemplo (Otros programas son muy similares), con solo hacer lo siguiente, podrá ver los headers:

- Haga click con el botón derecho sobre el mensaje de mail que está en su bandeja de entrada del Outlook.
- Seleccione 'Options...' en el menú emergente que aparece
- Examine 'Internet Headers' (ó "Encabezados de Internet") en el diálogo 'Message Options', que aparece.

**TIP:** Haga click con el botón derecho sobre el campo 'Internet Headers' y haga click en 'Select All' en el menú emergente (o type ctrl-A). Luego, nuevamente haga click con el botón derecho en 'Copy' en el menú emergente (o type ctrl-C). Finalmente, paste (pegue) todos los "Internet Headers" en su editor de texto favorito para verlos completos (Podría usar el 'Notepad', incluido con Windows).

**Ejemplo:** Lo que Ud. verá será muy similar a lo siguiente (Nosotros le agregamos los números de línea para claridad y poder referenciarlas más adelante):

```

1: Received: from tes1a623.OneMail.com.sg ([203.127.89.129]) by visualroute.com
(8.11.6) id f9CIVSk24480; Fri, 12 Oct 2001 12:31:29 -0600 (MDT)
2: Message-Id: <200110121831.f9CIVSk24480@s2.domain.com>
3: Received: from drb.com (IIM1608 [203.127.89.138]) by tes1a623.OneMail.com.sg with
SMTP (Microsoft Exchange Internet Mail Service Version 5.5.2448.0)
4: id 4XNK9ATR; Sat, 13 Oct 2001 01:19:10 +0800
5: From: paylesslongdistance@somedomain.com
6: To: <>
7: Subject: Long Distance - 4.9 cents per min - NO FEES!
8: Date: Fri, 12 Oct 2001 13:24:26 -0400
9: X-Sender: paylesslongdistance@yahoo.com
10: X-Mailer: QUALCOMM Windows Eudora Pro Version 4.1
11: Content-Type: text/plain; charset="us-ascii"
12: X-Priority: 3
13: X-MSMail-Priority: Normal
14: X-UIDL: 8`Y!!0GR!!"?"H"!k:O!!
15: Status: U

```

**Sintaxis de la línea de encabezamiento:** Los campos “Internet Header” son solamente una serie de líneas de texto que pueden verse como sigue:

**Header-Name: Header-Value**

Y si una línea comienza con tab o espacios, como en la línea 4 de arriba, esa línea es una continuación de la línea *Header-Value* previa. Por lo tanto, El “Header-Name” “**Received**” en la línea 3 tiene un “Header-Value” que continúa las líneas 3 y 4.

### 3. 'Received' Headers

El campo de encabezado más importante para los propósitos de rastreo del e-mail es el **Received**, que usualmente tienen una sintaxis similar a:

**Received: from ? by ? via ? with ? id ? for ? ; date-time**

Donde **from**, **by**, **via**, **with**, **id**, y **for** son todos tokens con valores dentro de un único *Header-Value*, que puede extenderse en múltiple líneas. Nota: Algunos servidores de mail podrían no incluir todos esos tokens – o podría ser que se agreguen tokens/valores adicionales a este campo, pero ahora Ud. Está preparado para identificarlos y comprenderlos.

Cada vez que un e-mail se desplaza a un nuevo mail server, se le agrega una nueva línea de encabezado **Received** (y posiblemente otras líneas de encabezados, como por ejemplo la línea 2 de arriba), al comienzo de la lista de encabezados.

Esto implica que Ud. Deberá leer los encabezados **Received** desde arriba hacia abajo, de manera que Ud. se vaya desplazando gradualmente hacia la computadora/persona que le envió el e-mail.

Pero, por favor tome nota que cuando lee el encabezado **Received** y llega cerca de la computadora/persona que le envió el e-mail, debe considerar la posibilidad que el emisor haya agregado uno o más líneas de encabezado **Received** falsas (al momento en que el emisor encabezaría la lista) en un intento de redirigirlo a Ud. a otra ubicación y prevenir que encuentre el verdadero emisor. Pero, ahora que sabe de esa posibilidad, esté alerta a esta operativa.

Probablemente encuentre que es muy útil separar una única línea **Received** en múltiples líneas con un token por línea, por ejemplo la línea de encabezado:

**Received: from tesla623.OneMail.com.sg ([203.127.89.129]) by visualroute.com (8.11.6) id f9CIVSk24480; Fri, 12 Oct 2001 12:31:29 -0600 (MDT)**

Es mucho más fácil de leer e interpretar cuando se formatea de manera que cada token esté en su propia línea, como:

**Received:**  
    **from** tesla623.OneMail.com.sg ([203.127.89.129])  
    **by** visualroute.com (8.11.6)  
    **id** f9CIVSk24480  
    **;** Fri, 12 Oct 2001 12:31:29 -0600 (MDT)

### 4. The Sender's IP Address

Para los propósitos del rastreo, estamos más interesados en los tokens **from** y **by** existentes en la línea de encabezado **Received**. En general Ud. buscará un pattern similar a:

**Received: from BBB (dns-name [ip-address]) by AAA ...**  
**Received: from CCC (dns-name [ip-address]) by BBB ...**  
**Received: from DDD (dns-name [ip-address]) by CCC ...**

En otras palabras, el mail server AAA recibió el e-mail desde BBB y suministra toda la información sobre BBB que BBB utilizó para conectarse a AAA, incluyendo el IP Address que BBB usó para conectarse. Este patrón se repite de la misma manera en cada línea **Received**. La syntax del token **from** muchas veces se ve así:

**name** (dns-name [ip-address])

Donde: **name** es el nombre que la computadora dijo que tenía. Muchas veces no debemos tomar como muy significativo este nombre porque puede ser cambiado intencionadamente en un intento de confundir la búsqueda (inclusi-

ve podría no tener el nombre de la computadora). **dns-name** es la conversión de la dirección IP al nombre DNS. **ip-address** es la dirección IP de la computadora utilizada para conectarse al servidor de mail que generó esta línea de encabezado **Received**. Por lo tanto, la dirección IP es oro para nosotros, a los fines del rastreo.

La sintaxis del token **by** solo nos dice el nombre que el mail server informó como suyo. Pero dado que el último mail server podría estar bajo el control del spammer, no deberíamos confiar en ese nombre.

Por lo tanto, es lo que es crucial para el rastreo, es poner atención al **ip-address** en el token **from** y no necesariamente al nombre de host provisto por el token **by**.

En este ejemplo se ve el motivo:

```
1: Received: from tesla623.OneMail.com.sg ([203.127.89.129]) by visualroute.com
(8.11.6) id f9CIVSk24480; Fri, 12 Oct 2001 12:31:29 -0600 (MDT)
3: Received: from drb.com (IIM1608 [203.127.89.138]) by tesla623.OneMail.com.sg with
SMTP (Microsoft Exchange Internet Mail Service Version 5.5.2448.0)
```

Si se ignora la línea 1, desde la línea 3 se concluye que el mail server **tesla623.OneMail.com.sg** es el que envió el e-mail y entonces usaríamos el VisualRoute para rastrear ese host, pero podría ser un error. Cuando se rastrea el nombre del host **tesla623.OneMail.com.sg**, en realidad estamos buscando el IP que corresponde a ese host name, que es **192.9.200.230**. Pero como se puede observar en la línea 1, el IP Address usado realmente, fue **203.127.89.129**. Evite ser engañado por esos intentos de confundirlo que suelen usar los spammers.

**Determine el IP Address del emisor:** Usando el ejemplo anterior, del encabezado de e-mail y analizando las líneas **Received** podemos concluir:

- Un empleado de Visualware recibió un e-mail
- El mismo viene desde **visualroute.com** (línea 1)
- Que viene desde **tesla623.OneMail.com.sg** (línea 1; línea 3 lo confirma)
- Pero el ip-address usado fue **203.127.89.129** (línea 1)
- Que viene desde **drb.com/IIM1608** (línea 3)
- Pero cuyo ip-address usado fue **203.127.89.138** (línea 3)

Por lo tanto, solo hemos rastreado este e-mail hasta la fuente -- IP Address **203.127.89.138**. El próximo paso es rastrear ese IP Address.

**TIP:** Practique! Rastree los e-mails recibidos desde amigos y familiares. Dado que conoce donde están ubicados, eso le ayudará a analizar los encabezados de internet. De esa manera obtendrá experiencia y seguridad en su habilidad para rastrear el origen de los mensajes de e-mail.

## 5. Rastree the IP Address

En el caso anterior, ese IP Address **203.127.89.138**. El resultado del trace se verá algo así como:

Hop	%Loss	IP Address	Node Name	Location	Tzone	ms	Graph	Network	
0		12.88.115.23	-	*			0 528	AT&T ITS	
1		199.70.3.58	-	Parsippany, NJ		94		AT&T EasyL	
2		199.70.3.49	-	Parsippany, NJ		139		AT&T EasyL	
3		12.122.253.24	gbr6-p21.n54ny	New York, NY, U	-5.0	128		AT&T ITS	
4		12.122.5.114	gbr3-p90.n54ny	New York, NY, U	-5.0	185		AT&T ITS	
5		12.123.1.121	ggr1-p360.n54r	New York, NY, U	-5.0	157		AT&T ITS	
6		192.205.32.17	att-gw.ny.verio.r	New York, NY, U	-5.0	174		AT&T Data C	
7		129.250.2.14	p4-1-3-0.r01.ch	Chicago, IL, US	-6.0	203		Verio, Inc.	
8		129.250.2.253	p4-6-0.r00.chcg	Chicago, IL, US	-6.0	197		Verio, Inc.	
9		129.250.4.89	p4-4-0.r00.dllst	Dallas, TX, USA		234		Verio, Inc.	
10		129.250.3.74	p4-1-0-0.r01.dll	Dallas, TX, USA		221		Verio, Inc.	
11		129.250.2.41	p1-0-0-0.r01.ore	Orem, UT, USA	-7.0	269		Verio, Inc.	
12		129.250.29.20	pvu1.wwhpvu1.y	Provo, UT, USA	-7.0	252		Verio, Inc.	
13		192.41.43.189	visualroute.com	Highland, UT 8		265		Icon Develo	
Roundtrip time to visualroute.com, average = 265ms, min = 195ms, max = 448ms -- 20-Apr-01									

Luego, use el dominio o la red cuando lo encuentre en el rastreador para encontrar el contacto para ese dominio o red de manera que pueda enviarle un reclamo.

## 6. Si falta información del emisor

Los encabezados de internet para un e-mail pueden contener información ciertamente interesante sobre el emisor.

**A) Nombre de la computadora Windows:** A veces aparenta que en nombre de la computadora no existe. Considere la información parcial de los encabezados de un e-mail:

Received: from **hanksdell** (11-22-33-44.xyz.net [11.22.33.44]) by visualroute.com (8.8.5) id SAA26331; Thu, 11 Oct 2001 18:46:53 -0600 (MDT)

Donde se puede ver claramente el IP Address del emisor, pero también podemos ver el nombre de la computadora **hanksdell**. Sabiendo que el nombre de la computadora puede ser cualquiera, en este caso, podemos suponer que la persona se podría llamar Hank y utiliza una computadora Dell ...

**B) Información de la zona de tiempo (Timezone Information):** Considere la línea 3 y 4 de los encabezados de internet que hablamos antes:

3: Received: from drb.com (IIM1608 [203.127.89.138]) by tes1a623.OneMail.com.sg with SMTP (Microsoft Exchange Internet Mail Service Version 5.5.2448.0)  
4: id 4XNK9ATR; Sat, 13 Oct 2001 01:19:10 +0800

Note que en los encabezados, cuando una hora es mostrada, muchas veces es seguida por un (+) o un (-) y por cuatro dígitos, que representa HHMM (horas y minutos) desde GMT (Greenwich Mean Time), o el horario de Londres. Plus significa al Este del GMT. Minus significa al Oeste de GMT.

Por lo tanto, de acuerdo a +0800, El server está a 8 horas al Este de GMT. TIP: Vaya al panel de control de Windows e ingrese en el diálogo Date/Time, donde la zona de tiempo se lista. Esta zona de tiempo aparece como localizada en Singapore. Entonces el .sg en **tes1a623.OneMail.com.sg** significa Singapore, lo cual es una confirmación adicional a esa información. Una confirmación final vendría de rastrear **203.127.89.129** (La dirección IP de **tes1a623.OneMail.com.sg**). TIP: Rastree la dirección IP, no el host name.

**C) X-Mailer:** Usualmente, esto le indica el software usado por el emisor para enviarle el correo. Considere:

10: X-Mailer: QUALCOMM Windows Eudora Pro Version 4.1

Esto podría (o no) ser de utilidad, Pero es de mucha utilidad para confirmar al final de las investigaciones.

**D) X-Originating-IP:** Si está intentando rastrear un e-mail recibido desde una cuenta de **Hotmail**, observe el campo de encabezado **X-Originating-IP**, que le indicará el IP Address de la computadora que le envió el e-mail. Observe:

1: Received: from hotmail.com (f105.pav1.hotmail.com [64.4.31.105]) by s2.xyz.com (8.11.6) id f9BIvve34655; Thu, 11 Oct 2001 12:58:00 -0600 (MDT)  
2: Received: from mail pickup service by hotmail.com with Microsoft SMTPSVC; 3: Thu, 11 Oct 2001 11:57:51 -0700 4: Received: from **202.156.2.147** by pvlfd.pav1.hotmail.msn.com with HTTP; 5: Thu, 11 Oct 2001 18:57:51 GMT 6: **X-Originating-IP: [202.156.2.147]**

Recuerde que podríamos obtener la misma información de ese IP examinando el encabezado **Received**. Pero es bueno tener confirmación extra.

## 7. Tenga en cuenta:

**A) Host Names vs IP Addresses:** Siempre base sus decisiones de rastreo en la dirección IP que encuentre en el encabezado y no en los nombres de Hosts.

**B) Información de encabezados falsas:** Advierta que los spammers podrían insertar falsos **Received:** en los encabezados para confundirlo. Utilice el sentido común cuando la información no tiene sentido.

**C) IP Address falsos:** La dirección IP que Ud. Encuentre como la máquina que le envió el correo es la dirección del real emisor o una computadora que fue violada por un hacker, por lo que se podría haber enviado un falso e-mail. O también, el emisor pudo esconderse detrás de un servicio 'anonymizer' – En ese caso tenemos la dirección IP de la compañía del 'anonymizer'.

**D) Cambio en las direcciones IP:** No suponga que la computadora del emisor tiene un IP fijo. Esto puede ser real en determinados casos, pero muchas personas se conectan mediante el discado y se les asigna una IP diferente en cada caso. Sin embargo no todo está perdido, muchas veces se puede reportar el Ip al administrador del ISP, enviando el encabezado completo y ellos pueden identificar al usuario mediante el análisis de los logs.

**E) Virus:** No presuponga lo peor de la persona que le está enviando el e-mail. Podría suceder que esa computadora estuviera infectada con un virus, que hace que la computadora envíe el correo por sí misma para distribuir el virus.

**F) Open Mail Servers:** No presuponga que la compañía le está enviando el e-mail. Podría suceder que solamente tienen mal configurados sus servidores y eso permitió a un spammer que viole la seguridad y pueda enviar sus correos a través del mail server.