Tracking e-mail -- who sent you that e-mail?

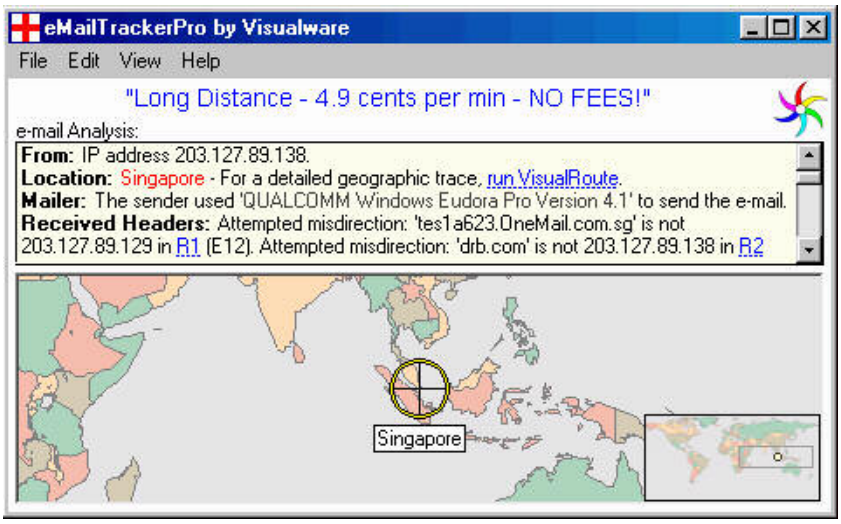
"Who sent you that e-mail and where are they located?"

With this tutorial as your guide, a little digging in the right places, and an Internet tracking tools like eMailTrackerPro and VisualRoute, you can in many cases figure out who sent you that nasty e-mail and report them to the proper authorities!

In fact, people who use **Yahoo** or **Hotmail** e-mail, thinking that their true identity and location are hidden, might be very surprised to find out that the IP Address of the computer used to send the e-mail can be uncovered and then traced, many times leading directly to a person.

1. Use e-mail tracking program

The first step is to use an e-mail analysis tool like eMailTrackerPro, which will automatically analyze an e-mail and its headers and provide graphical results similar to the following:



If you do not have an actual e-mail, but only have an e-mail address, you can use a tool like VisualRoute to track the user to their e-mail server. An added benefit is that you are able to see what SMTP software the mail server is running (many times with version information as well).

In most cases, using an e-mail tracking tool like eMailTrackerPro is your best option. But, if you want to understand how these tracking tools work, continue reading...

2. e-mail Internet Headers

Every received e-mail has Internet Headers. Using Microsoft Outlook as an example (other mail programs are very similar), just follow these steps to view the headers:

1. Right-click on the mail message that is still in your Outlook Inbox
2. Select 'Options...' from the resulting popup menu
3. Examine the 'Internet Headers' in the resulting 'Message Options' dialog

TIP: Right-click in the 'Internet Headers' field and click on 'Select All' in the popup menu (or type ctrl-A). Then right-click again and click on 'Copy' in the popup menu (or type ctrl-C). Finally, paste all the Internet Headers into your favorite text editor for full examination (such as 'Notepad', included with Windows).

Example: What you see will be very similar to the following (with 'line numbers' added for clarity and discussion in following sections):

```
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
```

Header Line Syntax: The Internet Header Fields are just a series of text lines, where each line looks like:

Header-Name: *Header-Value*

And if a line starts with a tab or spaces, like line 4 above, that line is a continuation of the previous *Header-Value* line. So, the *Header-Name* **Received** in line 3 has a *Header-Value* that spans lines 3 and 4.

3. 'Received' Headers

The most important header field for tracking purposes is the **Received** header field, which usually has a syntax similar to:

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

Where **from**, **by**, **via**, **with**, **id**, and **for** are all tokens with values within a single *Header-Value*, which may span multiple lines. Note: Some mail servers may not include all of these tokens -- or additional tokens/values may be added to this field, but now you are prepared to break it apart and understand it.

Every time an e-mail moves through a new mail server, a new **Received** header line (and possibly other header lines, like line 2 above) is added to the *beginning* of the headers list. *This is similar to FedEx package tracking, when your package enters a new sorting facility and is 'swiped' through a tracking machine.*

This means that as you read the **Received** headers from top to bottom, that you are gradually moving closer to the computer/person that sent you the e-mail.

But please note that as you read through the **Received** header fields and get closer to the computer/person that sent you the e-mail, you need to consider the possibility that the sender added one or more false **Received** header lines to the list (at the time, the senders beginning of the list) in an attempt to redirect you to another location and prevent you from finding the true sender. But, now that you know false header lines are possible, just stay alert.

You will probably find it very useful to break a single **Received** line into multiple lines, with one token per line. Namely, the header line:

```
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)
```

is much easier to read and understand when formatted so that each token is on a new line, as in:

```
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)
```

4. The Sender's IP Address

For tracking purposes, we are most interested in the **from** and **by** tokens in the **Received** header field. In general, you are looking for a pattern similar to:

```
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 ...
```

In other words, mail server AAA received the e-mail from BBB and provides as much information about BBB, including the IP Address BBB used to connect to AAA. This patterns repeats itself on each **Received** line. The syntax of the **from** token most times looks like:

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

Where: **name** is the name the computer has named itself. Most of the time we never look at this name because it can be intentionally misnamed in an attempt to foil your tracking (but it may leak the windows computer name). **dns-name** is the reverse dns lookup on the ip-address. **ip-address** is the ip-address of the computer used to connect to the mail server that generated this **Received** header line. So, the **ip-address** is gold to us for tracking purposes.

The **by** token syntax just provides us with the name that the mail server gives itself. But since the last mail server could be under the control of a spammer, we should not trust this name.

So, what is crucial for tracking, is to pay attention to the trail of **ip-address** in the **from** tokens and not necessarily the host name provided to us in the **by** tokens. Hopefully an example will make the reason why very clear:

```
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)
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)
```

If you ignore line 1, you would conclude from line 3 that mail server **tes1a623.OneMail.com.sg** sent you an e-mail and then use VisualRoute type program to trace to that host, but you would be wrong. When you trace to the host name **tes1a623.OneMail.com.sg**, you are actually tracing to the IP Address lookup on that host name, which is **192.9.200.230**. But as you can see from line 1, the IP Address used was really **203.127.89.129**. Do not be fooled by this attempted misdirection by spammers.

Determine the IP Address of the Sender: Using the example e-mail headers above and analyzing the **Received** header lines we can conclude:

- A Visualware employee received an e-mail
- which came from **visualroute.com** (line 1)
- which came from **tes1a623.OneMail.com.sg** (line 1; line 3 confirms)
- but whose ip-address used was **203.127.89.129** (line 1)
- which came from **drb.com/IIM1608** (line 3)
- but whose ip-address used was **203.127.89.138** (line 3)

So, we have just tracked this e-mail to the source -- IP Address **203.127.89.138**. The next step is to track down this IP Address.

TIP: Practice! Track down the e-mails received from friends and family. Since you know where they are really

located, that will help you to analyze the Internet Headers. You will quickly gain experience and confidence in your ability to track down the computer/person that sent you an e-mail message.

5. Track the IP Address

Use a tool like VisualRoute to track the IP Address. Track down the person. In the case above, this is IP Address `203.127.89.138`. The resulting trace will look somewhat like this generic trace:

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.n54n	New York, NY, U	-5.0	128		AT&T ITS
4		12.122.5.114	gbr3-p90.n54n	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 (
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.or	Orem, UT, USA	-7.0	269		Verio, Inc.
12		129.250.29.20	pvu1.vwhpvu1.v	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								

Then, use the domain (by clicking on 'Node Name' rows) or network (by clicking on 'Network' rows) popup WHOIS capability of VisualRoute to discover the domain (company) or network (ISP) contact information -- to file a complaint or report the abuser.

Ideally, you want domain or popup WHOIS information for the IP Address of interest. But, if that is not possible, just move up the list and obtain 'Network' WHOIS information for the next network up in the list and report the abuse to them -- since the abuser is connected through them.

6. Leaked Sender Information

The Internet Headers for an e-mail message may contain some really interesting information about the sender.

A) Windows Computer Name: It appears that the Windows computer name is sometimes leaked. Consider the following partial header information from an actual 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)
```

Where we can clearly see the IP Address of the sender, but we can also see the computer name of **`hanksdell`**. While the computer name can be named *anything*, in this case, I might assume that the person is named Hank and uses a Dell computer.

This computer name may be intentionally misleadingly named or not be meaningful but it can become very useful confirming information if law enforcement can confirm that the name of the suspect's computer matches the name in the e-mail header.

B) Timezone Information: Consider lines 3 and 4 from the Internet Header discussion above:

```
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
```

Notice that in the Internet Headers, when a time is displayed, many times it is followed with a plus/minus and four digits, which represent HHMM (hour and minutes) from GMT (Greenwich Mean Time), or London, UK time. Plus means east of GMT. Minus means west of GMT.

So, according to **+0800**, the server is 8 hours east of GMT. TIP: Go into the Windows Control panel and enter into the Date/Time dialog, where there is a Time Zone list. This time zone appears to be in Singapore. Then, the **.sg** in **tes1a623.OneMail.com.sg** means Singapore, which is one more confirmation of this information. A final confirmation comes from performing a trace **203.127.89.129** (the IP Address for **tes1a623.OneMail.com.sg**). TIP: Trace to the IP Address, not the host name.

C) X-Mailer: This will usually tell you the mailer software used by the sender of the e-mail. Consider:

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

This may or may not be immediately useful, but it can be very useful if there is a follow-up investigation by authorities.

D) X-Originating-IP: If you are attempting to track down an e-mail received from a **Hotmail** e-mail account, look for the **X-Originating-IP** header field, which will tell you the IP Address of the computer that sent the e-mail. Consider:

```
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 pv1fd.pav1.hotmail.msn.com with
HTTP; 5:     Thu, 11 Oct 2001 18:57:51 GMT 6: X-Originating-IP: [202.156.2.147]
```

However, notice that we could have obtained the same IP Address information by examining the **Received** header fields. But it is nice to have this extra confirmation.

7. Final Warnings

Please pay attention to these warnings when attempting to track e-mail messages:

A) Host Names vs IP Addresses: Always base your tracking decisions based upon the IP Addresses that you find in the header information and not on host names (which are a lookup from the IP Address anyway). Because mapping an IP Address into a host name and then back into an IP Address may yield a different IP Address.

B) False Header Information: Be aware that spammers *may* try to insert fake **Received:** header lines into the Internet Headers of the e-mail message to confuse you. Just follow the trail through the **Received:** header fields from mail server to mail server and use some common sense when the information makes no sense.

C) False IP Address: The IP Address that you finally end up at is the IP Address of the computer that sent the e-mail. But is that computer the real sender, or a computer that was broken into, so that a false e-mail could be sent. Or the sender could try to hide behind an 'anonymizer' service -- where you will get to the IP Address of the 'anonymizer' company.

D) IP Addresses Change: Do not assume that the sender's computer has a fixed, constant IP Address. This may be true in some cases, but most people who dial into the Internet almost always get a different IP Address each and every time they connect into the Internet. However, all is not lost. Many times you can report the IP Address and full e-mail Internet Headers (which many times contain time-of-day information) to the person's ISP and the ISP can track this down to a unique end-user (by examining login and logout logs) and take action.

E) Viruses: Do not assume the worst of the person sending the e-mail. They may have just been infected with a virus, which is using a person's computer to spread itself.

F) Open Mail Servers: Do not assume the worst of the company whose mail sever was used to send the original e-mail. They may be involved in the spam, but they also may just have a misconfigured e-mail server, which is allowing a spammer to send the e-mail through their mail server.