

# TRACING EMAILS

By Chetan Gupta

Have you ever received an anonymous email and wondered who it was from? Ever conducted business via email and wanted to know if the other party is who they say they are? As you can imagine, the uses for this type of investigation are endless. Not only is it possible to find the **sender** of the anonymous email but it is also possible to **locate** the sender

With the ever-increasing penetration of computers in our lives, emails have become a vital source of communication. It is quickly becoming the prime medium for business and personal correspondence and is undoubtedly the most popular way we communicate with others on a daily basis. As with any popular technology, email technology is also prone to abuse. While most people use email for its intended purpose, a very large number use this medium for a completely different goal: anonymous threats, fraudulent transactions, unsolicited commercial messages, blackmail and even ransom notes. As these cases rise day-by-day, it becomes imperative that the Forensics Investigator have the required skills and tools to follow the electronic traces left by an email and nab the culprit(s).

## Preparing the Ground

First step in tracing an e-mail is having a thorough understanding of the e-mail process. A broad outline of the steps is given below:

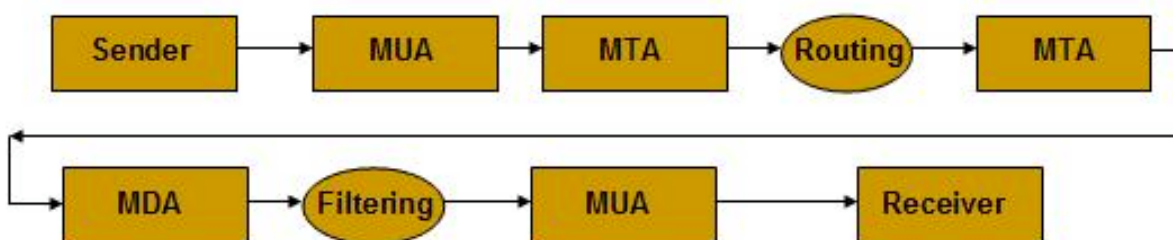


Figure 1: Email process

**Mail User Agent (MUA)** - A program such as Outlook, Thunderbird, or Outlook Express run by the user to read, reply to, compose and dispose off emails.

**Mail Transport Agent or Message Transfer Agent (MTA)** - The program responsible for storing and forwarding or delivering emails.

**Mail Delivery Agent (MDA)** - The actual program responsible for delivering emails to a user. MDAs usually handle one specific type of mail delivery.

When you send an e-mail, each intermediate device (MUA, MTA and MDA) may insert some headers in the message. These headers can help an investigator reconstruct the path that the e-mail took to the receiver. The last MUA may apply a filter to the stored mail causing selected headers to be omitted from the display. In a way, this filtering 'removes' the headers from the user's view (although no headers are actually removed by the MUA). This is reason that the user doesn't see all the headers in the normal mail view. The headers typically omitted are those inserted by the MTAs, and those having to do with the transport process and less with the contents.

# TRACING EMAILS

By Chetan Gupta

The email headers not shown usually can be viewed by clicking on 'Show all headers', 'View source' or 'Full Headers' link depending upon the mailing program. If you use Microsoft Outlook, 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

## Putting on the Gloves

### Step 1: Examine all the headers of the incoming message

**Example:** This is an e-mail sent to my e-mail address by Verisign. When I click "View Source", I get all the headers. What you see will be very similar to the following (with 'line numbers' added for clarity and further discussion)

1. Return-Path: [clarify@gravity.verisign.com]
2. Delivered-To: chetan@niiconsulting.com
3. Received: (qmail 14341 invoked from network); 28 Oct 2005 06:52:05 -0000
4. Received: from mismailer2.verisign.com (HELO mismailer2) (65.205.251.72) by qmail-d.directi.com with SMTP; 28 Oct 2005 06:52:05 -0000
5. Received: from gravity.verisign.com (gateway1.verisign.com [65.205.251.51] by mismailer2 (Postfix) with ESMTTP id 3B33751AE1B for [chetan@niiconsulting.com]; Thu, 27 Oct 2005 23:52:04 -0700 (PDT)
6. Received: (from clarify@localhost) by gravity.verisign.com (8.12.8/8.12.8) id j9S6q3hV009117 for chetan@niiconsulting.com; Thu, 27 Oct 2005 23:52:03 -0700 (PDT)
7. Date: Thu, 27 Oct 2005 23:52:03 -0700 (PDT)
8. Message-Id: [200510280652.j9S6q3hV009117@gravity.verisign.com]
9. To: chetan@niiconsulting.com
10. From: "VeriSign Inc." [salesteam@verisign.com]
11. Subject: Thanks for Downloading Your Guide - (OP21767985)
12. Content-Type: text

The most important header field for tracking purposes is theReceived header field, which usually has pattern similar to:

Received: from BBB (dns-name [IP address]) by AAA ...

# TRACING EMAILS

By Chetan Gupta

Every time an email moves through a new mail server, a new Received header line (and possibly other header lines, like line 3 above) are added to the beginning of the header's 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 email.

You also 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.

The syntax of the **from** token in the Received Header mostly looks like:

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

Where:

"name" is the name of the computer.

"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 the one which helps us to track the culprit.

The **by** token syntax just provides us with the name of the mail server. An important point is to pay attention to the trail of IP addresses in **from** tokens and not necessarily the host name provided to us in the **by** tokens. The host name could easily be a forged one!

## Determine IP Address of the sender

Using the example email headers above and analyzing the Received header lines we can conclude:

- An NII employee (chetan@niiconsulting.com) received an email (line 2)
- which came from mismailer2.verisign.com (line 4) and received by qmail-d.directi.com
- which came from gateway1.verisign.com (line 5; line 6 confirms)
- which came from clarify@localhost (line 6)
- but whose IP-address used was 65.205.251.51 (line 5)

Voila, we have just tracked this email to the source IP Address - 65.205.251.51

The final step is to map the identified domains to their corresponding IPs and verify the IPs in the header. For this you need a DNS resolver program. If you haven't got one of your own, you can use the DNS Lookup service at [www.dnsstuff.com](http://www.dnsstuff.com) A whois on qmail-d.directi.com gives the following result and confirms that it's the NII mail server from where I downloaded the e-mail:

# TRACING EMAILS

By Chetan Gupta

Registrant: Direct Information Pvt. Ltd  
Domain Manager (domain.manager@directi.com)

A whois on the IP address 65.205.251.51 confirms the origin of the mail and also gives the location of the IP address:

Location: United States [City: San Jose, California]  
NOTE: More information appears to be available at NET-65-205-248-0-1.  
UUNET Technologies, Inc. UUNET65 (NET-65-192-0-0-1) 65.192.0.0 - 65.223.255.255  
Verisign UU-65-205-248 (NET-65-205-248-0-1) 65.205.248.0 - 65.205.251.255

A domain name whois gives a lot more information including the address of Verisign Inc. as well as the Administrative contact and Technical contact for the domain. An alternative to the manual whois would be to use sophisticated tools. The preferred ones are SmartWhois by Tamosoft(www.tamos.com) and WhereisIP by JufSoft (www.jufsoft.com)

The second alternative is to use an email analysis tool which will automatically analyze an email and its headers and provide a report similar to the following:

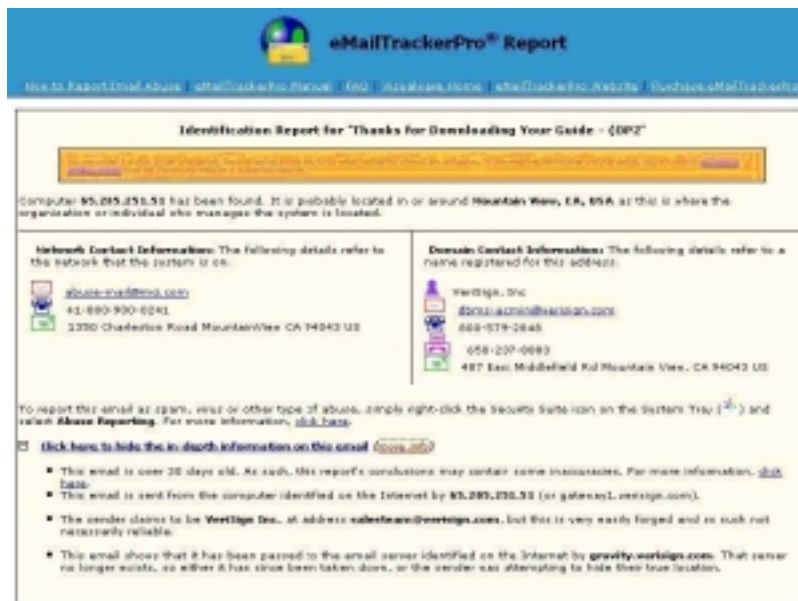


Figure 2: eMailTracker Report

## What If...

### I do not have the full headers?

If you do not have an actual email message, but only have an email address, you can trace the address of its email server. However it should be noted that email addresses can be easily forged, the results from tracing an email address may not be related to the true sender.

### The sender was using a dynamic IP address?

The time and date on which the message was sent is included in the headers (line 6). Even if the culprit was using dynamic IP, you can check with the ISP for their DHCP logs on the date and time the e-mail was sent. That would lead you to the person/organization to whom the IP was leased for that duration.

# TRACING EMAILS

By Chetan Gupta

## Conclusion

Once you have identified the IP address of the sender's computer, the sender's geographical location, and the company providing Internet service (or ISP) for the IP address, you should report the incident to the appropriate authorities. There are two possible outcomes of the above trace. You'll either have an address of a company's mail server, or the address of a dial-up port. Either way, you may want to contact the responsible administrator. Reports for email abuse such as spam, email-borne viruses and email threats should be directed to the sender's ISP if it was from a dial-up port. If it was from a company's mail server, then the contact received from the "whois" on the company's domain should help you to contact the concerned authority for handling e-mail abuse.