

How to trace an e-mail, part 1: An overview
by Robert Lebowitz, Digital Freedom Network

(April 19, 2002) Even without professional software, it is possible to trace an e-mail back to its sender, or at least learn a lot about him or her, by examining the information embedded within the text. This two-part article will describe the basic method of such a process. The basic overview of the steps involved are:

1. View full header
2. Read the Received: fields in the header, with the bottom field the oldest MTA and the top the most recent
3. Use Internet Registries to determine which companies own the IPs
4. Contact the companies to ask that they check their user and message logs to see who was logged into that particular IP at that time

First, let's look at an actual "joke" e-mail that the Digital Freedom Network received recently as an example. A certain "Grace Lawal" from Nigeria wrote DFN with a business proposition. Ms. Lawal had written DFN before with similar e-mails. A response to the e-mail showed her (or his) address to be fake. A search for a "Grace Lawal" on the Internet proved fruitless, as did a search for her with Zenith Bank, for whom Ms. Lawal claims she works.

The text of the e-mail, slightly edited for length, appears below. (Some terms have been bolded and colored for later reference.)

Return-Path: <graceelawal@yahoo.com>
Received: from [207.202.32.37] (HELO
mailscan1.corp.idt.net) by mail.corp.idt.net
(CommuniGate Pro SMTP 3.5.7) with SMTP id 3290036
for rlebow@corp.idt.net; Sat, 13 Apr 2002 11:49:42
-0500
Received: from 169.132.232.57 by
mailscan1.corp.idt.net (InterScan E-Mail VirusWall
NT); Sat, 13 APR 2002 12:54:55 -0400
Received: from mq.idtweb.com ([216.53.71.121]
verified) by mail.idtweb.com (CommuniGate Pro SMTP
3.5.7) with ESMTP id 30370009 for rlebow@dfn.org;
Sat, 13 APR 2002 12:51:44 -0400
Received: from [80.247.137.24] (HELO ab97c381.com)
by mq.idtweb.com (CommuniGate Pro SMTP 3.5.7) with
SMTP id 29632626 for rlebow@dfn.org; Sat, 13 APR
2002 11:51:46 -0500
From: "Dr. Grace Lawal" <graceelawal@yahoo.com>
Reply-To: graceelawal@yahoo.com
To: rlebow@dfn.org
Date: Sat, 13 APR 2002 05:52:35 +1000
Subject: #Contact urgently#
X-Mailer: Microsoft Outlook Express 5.00.2919.6900
DM
MIME-Version: 1.0
Content-Type: multipart/mixed;
boundary="===_LikeYe_888_2fptuofrlwIhIh"
Message-ID: <auto-000029632626@mq.idtweb.com>
X-Mozilla-Status: 8003
X-Mozilla-Status2:
00000000
X-UIDL:
1169

Dear Sir,

I am Dr. Grace Lawal (Phd) Bank Manager of Zenith Bank, Lagos, Nigeria. I have urgent and very confidential business proposition for you. On June 6, 1997, a Foreign Oil consultant/contractor with the Nigerian National Petroleum Corporation, Mr. Barry Kelly made a numbered time (Fixed) Deposit for twelve calendar months, valued at US\$25,000,000.00, (Twenty-five Million, Dollars) in my branch. Upon maturity, I discovered from his contract employers, the Nigerian National Petroleum Corporation that Mr. Barry Kelly died from an automobile accident. On further investigation, I found out that he died without making a WILL, and all attempts to trace his next of kin was fruitless. This sum of US\$25,000,000.00 has carefully been moved out of my bank to a security company for safekeeping. No one will ever come forward to claim it. Consequently, my proposal is that I will like you as a Foreigner to stand in as the owner of the money I deposited it in a security company in two trunk boxes though the security company does not know the contents of the boxes as I tagged them to be photographic materials for export. I want to present you as the owner of the boxes in the security company so you can be able to claim them with the help of my attorney. This is simple. I will like you to provide immediately your full names and address so that the Attorney will prepare the necessary documents which will put you in place as the owner of the boxes. The money will be moved out for us to share in the ratio of 70% for me and 30% for you.

Thanks and God bless.

Dr. Grace Lawal (p.h.d)

1. View full header

Every e-mail comes with information attached to it that tells the recipient of its history. This information called a header.

The header contains the information essential to tracing an e-mail. The main components to look for in the header are the lines beginning with "From:" and "Received:"

However, it might be instructive to look at what various different lines in the header mean.

Return-Path: is the address to which your return e-mail will be sent. Different e-mail programs use other variations of Return-Path: . These might include Return-Errors-To: or Reply-To: . In the example above, the e-mail was received by info@dfn.org, and was then forwarded to rlebow@dfn.org. Were the recipient at rlebow@dfn.org to hit "reply" to this e-mail, the response would be sent to info@dfn.org. Obviously, this piece of information is irrelevant in trying to trace an e-mail.

The Message-ID: is assigned uniquely to every piece of e-mail by the mail system when the message is first created. It looks like an e-mail address, but it isn't. The Message-ID: often identifies the system from which the sender is logged in, rather than the actual system where the message originated.

One might think then that the Message-ID: would give some revealing information about from where the e-mail originated. However, it is too easy to forge, and is consequently not reliable.

From: is also useless in tracing an e-mail. It reveals the e-mail address of the sender, but this can obviously be a fake, as is the case in our example.

MIME-Version: tells the recipient if what type of attachments are included. MIME stands for Multipurpose Internet Mail Extensions. It is a format that allows people to send attachments that do not contain standard English words, but rather graphics, sounds, and e-mails written with other characters. The Mime-Version field merely confirms that the version of MIME used corresponds to the standard version (which is currently 1.0)

Content-Type: This line tells the receiving e-mail client exactly what MIME type or types are included in the e-mail message. In the example above, text/plain; charset="us-ascii" just tells us that the message contains a regular text message that uses English characters. ASCII is the American Standard Code for Information Interchange and is the system used to convert numbers to English characters.

Received: is really the key to finding out the source of your e-mail. Like a regular letter, your e-mail gets postmarked with information that tells where it has been. However, unlike a regular letter, an e-mail might get "postmarked" any number of times as it makes its way from its source through any number of mail transfer agents (MTAs) The MTAs are responsible for properly routing messages to their destination.

The MTAs are "stamped" on the e-mail's header so that the most recent MTA is listed on the top of the header and the first MTA through which the e-mail has passed in listed on the bottom of the header. In the above example, "Grace Lawal's" e-mail first passed through 80.247.137.24, and lastly passed through 207.202.32.37.

2. Read the Received: fields in the header

So, for example, we can translate the bottom Received: line as follows:

```
Received: from [80.247.137.24] (HELO ab97c381.com) by
mq.idtweb.com (CommuniGate Pro SMTP 3.5.7) with SMTP id
29632626 for rlebow@dfn.org; Sat, 13 APR 2002 11:51:46 -0500
```

The e-mail came from 80.247.137.24 into mq.idtweb.com using Simple Mail Transfer Protocol (SMTP), which is the language used by all Internet e-mail software to transfer e-mail messages. The mail was received by mq.idtweb.com on Saturday, April 13, 2002 at 11:51:46 New York Time. [The 4-digit number "-0500" indicates how far away from Greenwich Mean Time (GMT) the time is. In this case, this clock is 5 hours away from GMT.]

The HELO function in parentheses following the initial IP code indicates the computer that sent the message, but its accuracy is not reliable.

3. Use Internet Registries to determine which companies own the IPs

80.247.137.24 is called an IP address. IP stands for Internet Protocol. Every machine on the Internet receives such an identification number. It is composed of a series of four numbers separated by a period (.). Each of the four numbers is in the range of 0 to 255. Consequently, if you come across an IP address that has as one of its 4 numbers one that exceeds this range, you know it is a fake IP (For example, the IP address 123.278.87.23 is fake, since 278 is greater than 255.)

Organizations with many computers hooked up to the Internet rent out blocks of IP addresses. Every IP address is assigned by one of the registries on the Internet, and, as a result, the name of the organization using that IP (or series of IPs) is stored in a database in one of these registries.

There are three major registries covering different parts of the world. The American Registry of Internet Numbers (ARIN), located at www.arin.net, assigns IPs for the Americas and for sub-Saharan Africa; Asia Pacific Network Information Centre (APNIC), at www.apnic.net, covers Asia; R'seaux IP Europiens (RIPE NCC), at www.ripe.net, covers Europe. Thus, to find out what organization owns a particular IP, you can search the database at any of these registries. You do this by typing the IP number into the WHOIS box that appears on each Web site.

In looking for the IP above, we might first search ARIN, since the letter purports to be from Nigeria, a region covered by ARIN. It turns out, however, that 80.247.137.24 is registered with RIPE. We can then retrieve the information of the company that owns 80.247.137.24. It turns out to be an Internet Service Provider (ISP) located in Nigeria called Simba Technology.

4. Contact the companies to ask that they check their user and message logs to see who was logged into that particular IP at that time

Once you find out which company owns that particular IP, it is then possible to contact the company itself. They have user and message logs of who logged into of each of their computers at any given time. By supplying the company with the e-mail header of the offending e-mail, they can check these logs and hopefully produce information of the user of that machine.

After some e-mail exchange with Simba, we determined that the Nigerian company assigned the block of IPs that include 80.247.137.24 to a cyber cafe in Lagos. We have thus traced the offending e-mail to its place of origin, although the identity of the particular sender still eludes us.

Go to [How to trace an e-mail, part 2: A case study](#)