

How to trace an e-mail, part 2: A case study  
by Robert Lebowitz, Digital Freedom Network

(April 19, 2002) We have previously become familiar with what to look for in an e-mail header in order to trace an e-mail. We will now use the example from the last lesson to clarify the procedure in more detail.

The e-mail we wish to trace is a spam message actually received by the Digital Freedom Network from one "Grace Lawal." In her message, Ms. Lawal asks for money for a business transaction. A reply to Ms. Lawal's e-mail address bounces back, revealing that is fake. Additionally, there is no record of any Grace Lawal connected with Zenith bank. Using the e-mail tracing methods broadly described thus far, how close can we get to finding out who this Ms. Lawal is? The original e-mail from "Grace Lawal" appears below. (The Received: fields 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\_2fptuofrlwlh"  
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 sl 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

We see from the From: and Reply to: fields that the e-mail address of the sender of this annoying solicitation is graceelawal@yahoo.com. A reply, however, reveals that this is not a valid e-mail address. So, we now look at the Received: field.

#### 2. Read the Received: fields in the header, with the bottom field the oldest MTA and the top the most recent

Explaining these fields is quite straightforward.

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

First, the e-mail came from 80.247.137.24 into mq.idtweb.com. (HELO identifies the sending machine. This cannot be relied upon however for accurate information.) The mail was received on Saturday, April 13, 2002 at 11:51:46 New York Time.

Next, the e-mail passed from mq.idtweb.com into mail.idtweb.com. The mail was received on Saturday, April 13, 2002 at 11:51:44 New York Time.

Next, the e-mail traveled from 169.132.232.57 to

mailscan1.corp.idt.net. The mail was received on Saturday, April 13, 2002 at 11:54:55 New York Time.

Finally, the e-mail traveled from 207.202.32.37 to mail.corp.idt.net. The mail was received on Saturday, April 13, 2002 at 11:49:42 New York Time.

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

The e-mail originated from 80.247.137.24. We must look up the IP in one of the Internet registries on the Web. The place we will start is the American Registry of Internet Numbers (ARIN) at [www.arin.net](http://www.arin.net), which the registry for the Americas and sub-Saharan Africa. We choose to begin our search on ARIN only because "Grace Lawal" states that she is from Nigeria. We don't know this for sure, of course, but it is a good a place to start as any.

After going to the ARIN Web site, we perform a WHOIS search on the IP address (See figure below).

Figure 1: The WHOIS search on ARIN is on the upper right corner.

The WHOIS search tells us that in fact this IP address is not in the ARIN database, but rather can be found in the database of European Regional Internet Registry (RIPE), located at [www.ripe.net](http://www.ripe.net). As its name implies, RIPE is responsible for IP addresses of European organizations.

We now perform the same WHOIS search on the RIPE Web site, entering the IP address, 80.247.137.24. This time, our search is successful. RIPE outputs the following data:

```
inetnum: 80.247.137.0 - 80.247.137.255
netname: SIMBATECH
descr: Simba Technology ltd is a Licensed ISP located Lagos
Nigeria
country: NG
admin-c: ID116-RIPE
tech-c: NIL3-RIPE
status: ASSIGNED PA
notify: anil@simbaonline.net
mnt-by: AS17175-MNT
changed: scooper@newskies.com 20020208
source: RIPE
```

```
route: 80.247.128.0/20
descr: New Skies Satellites
origin: AS17175
mnt-by: AS17175-MNT
changed: scooper@newskies.com 20011116
source: RIPE
```

```
person: Segun Adekoya
address: Simba Technology Limited.
address: 77/79 Eric Moore Road, Surulere, Lagos
address: Nigeria.
phone: +23417740120
fax-no: +23415851016
e-mail: segun@simbaonline.net
nic-hdl: ID116-RIPE
notify: support@simbaonline.net
mnt-by: AS17175-MNT
changed: scooper@newskies.com 20020208
```

source: RIPE

person: Anil Kumar  
address: Simba Technology Limited.  
Address: 77/79 Eric Moore Road, Surulere, Lagos  
phone: +23417740120  
fax-no: +23415851016  
e-mail: anil@simbaonline.net  
nic-hdl: NIL3-RIPE  
notify: anil@simbaonline.net  
mnt-by: AS17175-MNT  
changed: scooper@newskies.com 20020208  
source: RIPE

We can thus determine that Simba Technology is the Internet Service Provider (ISP) that took up "Grace Lawal's" e-mail after she sent it off to DFN. We also note that while "Grace Lawal" is almost certainly a false name, she (or he) might not have lied about being in Lagos, Nigeria, since that is where Simba is located. At any rate, Simba must have a record in the form of a mail or user log that will inform us from where the e-mail originated.

Before we do this, let's go back and trace the remaining path of the e-mail. We can see that after it left Nigeria, it went directly to mq.idtweb.com. IDT Corporation hosts DFN, so already, we see the mail has arrived with no stopovers. From there, it went into mail.idtweb.com. The header then reports that the mail went from 169.132.232.57 to mailscan1.corp.idt.net, and then from 207.202.32.37 to mail.corp.idt.net.

These IP addresses seem to come out of nowhere, but a WHOIS search on ARIN reveals that they are just IP addresses owned by IDT.

Thus the mail arrived at IDT and then went through various scanning procedures to make sure it was not spam and did not contain a virus before it arrived in DFN's mailbox.

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

This is the letter we sent to Simba Technology. It was addressed specifically to Anil Kumar and Segun Adekoya, the two contacts listed in the RIPE database entry above. (Note: The original message from "Grace Lawal" was attached to this e-mail to Simba, but is not reprinted again here.)

From: Robert Lebowitz [mailto:rlbow@dfn.org]  
Sent: Wednesday, April 17, 2002 3:02 PM  
To: anil@simbaonline.net, segun@simbaonline.net  
Subject: Can you please check mail and user logs stats?

Dear Sirs,

Hi. I received the following mail that passed through your machines. Would you be kind enough to check the mail logs on simbaonline.net for Sat, April 13, 2002 05:52:35 +1000? (This would be 5:52:35 Sydney or Melbourne time). I highlighted the line of the header that indicates that the message passed through your system at this time.

There does not appear to be any "grace lawal" at Zenith, and we have received quite a few "spam"

messages from her. Perhaps you can tell me the identity of--or at least any information about--this person.

Thanks so much,  
Robert Lebowitz

<message attached>

The message to Simba was sent out in the morning. By the late afternoon, we received the following reply from Simba's general manager:

Dear Mr.Robert

This has reference to the concerns raised by you regarding the spam mails. We are basically a ISP in Nigeria.

The IP involved belongs to one of our customer who runs a cyber cafe in Lagos. Since it is a cyber cafe we are not able to identify who is the person doing the same. Still we are taking all efforts to identify the person doing this mischief.

Pls also let me know, if you have any suggestions on how this person could be isolated.

Regards  
Viswanathan.D  
General Manager  
SimbaNET Nigeria Ltd.  
77/79, Eric Moore Road  
Surulere, Lagos  
Nigeria.

We know now that the e-mail was sent from a cyber cafe in Lagos, Nigeria. However, since one can send messages from a cyber cafe with complete anonymity, we are prevented from finding out more concrete information.

If this were an e-mail of much greater importance—such as the ransom note sent from the kidnappers of U.S. journalist Daniel Pearl—we could take further steps to track our quarry. For instance, we could get the name of the Lagos cyber cafe from our contact at Simba. Then, on the assumption that the person sends out e-mail periodically from the same location, we could install key-sniffing devices in the computers at the cafe. These programs register a user's keystrokes, thus creating a record of everything that was typed at a particular terminal. Another recourse would be to make sure IDs were taken for the period in which a person was using a computer in a public cluster.

But while these methods would aid greatly in identifying an e-mail sender, they also would impinge on the rights of others using the computers to conduct their personal business. Such a conflict defines the ongoing struggle between the fight against terrorism over the Internet and the right to privacy, which will continue to evolve in the years ahead.

Go to [How to trace an e-mail, part 1: An overview](#)