Tracing Email

Roughly 16 Billion emails are sent on the Internet each day. Much of that email is in the form of unwanted spam and junk email. Using common networking utilities and programs, a forensics investigator can usually trace the origins of an email to the originating IP address of the sending computer. These techniques can also be used to track the origin of unknown, spoofed or harassing emails and for tracking down criminals.

You do not need to use the forensics lab to complete this exercise. Any Internet connected computer can be used to complete this lab.

In order to trace the origins of an email, you will have to examine the email message headers to determine that information. Viewing the headers for a particular email message is different on each email program. For example, in MS Outlook, you have to open the email and select View, Options. Other email clients will require a different set of steps to view the headers.

Identifying the sending machine hostname and IP address

Here is a sample email header from a message sent to Professor Murray by the departmental secretary Val. The line that is bolded and underlined shows the hostname and IP address of the machine that the message was sent from.

Return-Path: <limpert@buffalo.edu>
Received: from murder ([unix socket])
  (authenticated user=djmurray bits=0)
  by email1.acsu.buffalo.edu (Cyrus v2.2.12-UB_mail1_2005_03_01) with LMTPA;
  Wed, 08 Feb 2006 14:37:58 -0500
Delivered-To: djmurray@mailspool08.dyn.acsu.buffalo.edu
Received: (qmail 11306 invoked from network); 8 Feb 2006 19:37:58 -0000
Received: from unknown (HELO mailscan7.acsu.buffalo.edu) (128.205.6.158)
  by mail1 with SMTP; 8 Feb 2006 19:37:58 -0000
Received: (qmail 12527 invoked by uid 22493); 8 Feb 2006 19:37:57 -0000
Delivered-To: djmurray@buffalo.edu
Received: (qmail 12514 invoked from network); 8 Feb 2006 19:37:57 -0000
Received: from smtp1.acsu.buffalo.edu (128.205.6.84)
  by front2.acsu.buffalo.edu with SMTP; 8 Feb 2006 19:37:57 -0000
Received: (qmail 29820 invoked from network); 8 Feb 2006 19:37:57 -0000
Received: from jac335-limpert.mgt.buffalo.edu (HELO JAC325VALERIE) (128.205.203.82)
  by smtp1.acsu.buffalo.edu with SMTP; 8 Feb 2006 19:37:57 -0000
From: "Valerie Bartkowiak" <limpert@buffalo.edu>
To: "'David J. Murray'" <djmurray@buffalo.edu>
Subject: RE: Conference Room Furniture
Date: Wed, 8 Feb 2006 14:37:49 -0500
MIME-Version: 1.0
Content-Type: text/plain;
  charset="us-ascii"
Content-Transfer-Encoding: 7bit
X-Priority: 3 (Normal)

X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook, Build 10.0.6626
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2180
Importance: Normal
X-UB-Relay: (jac335-limpert.mgt.buffalo.edu)
X-PM-EL-Spam-Prob: : 7%
X-DCC-Buffalo.EDU-Metrics: email1.acsu.buffalo.edu 1029; Body=0 Fuz1=0 Fuz2=0

Using Nslookup to find a hostname

Sometimes the message header will only have an IP address and not a hostname. In the previous example, both the machine name and IP address were included in the message header. But what can you do to track down a machine if you only know the IP address? Here is another sample email header which includes only an IP address. See below the message for some specific things you can do.

Return-Path: <mgs351@hotmail.com>
Received: from murder ([unix socket])
(authenticated user=djmurray bits=0)
by email1.acsu.buffalo.edu (Cyrus v2.2.12-UB_mail1_2005_03_01) with LMTPA;
Thu, 9 Feb 2006 23:21:45 -0500
Delivered-To: djmurray@mailspool08.dyn.acsu.buffalo.edu
Received: (qmail 14244 invoked from network); 10 Feb 2006 04:21:45 -0000
Received: from unknown (HELO mailscan5.acsu.buffalo.edu) (128.205.6.137)
by mail1 with SMTP; 10 Feb 2006 04:21:45 -0000
Received: (qmail 19652 invoked by uid 22493); 10 Feb 2006 04:21:45 -0000
Delivered-To: djmurray@buffalo.edu
Received: (qmail 19642 invoked from network); 10 Feb 2006 04:21:45 -0000
Received: from bay105-f39.bay105.hotmail.com (HELO hotmail.com) (65.54.224.49)
by front3.acsu.buffalo.edu with SMTP; 10 Feb 2006 04:21:45 -0000
Received: from mail pickup service by hotmail.com with Microsoft SMTPSVC;
Thu, 9 Feb 2006 20:21:44 -0800
Message-ID: <BAY105-F3985E65AD8211242644D0281FA0@phx.gbl>
Received: from 65.54.224.200 by by105fd.bay105.hotmail.msn.com with HTTP;
Fri, 10 Feb 2006 04:21:44 GMT
X-Originating-IP: [69.163.26.172]
X-Originating-Email: [mgs351@hotmail.com]
X-Sender: mgs351@hotmail.com
From: "Dave Murray" <mgs351@hotmail.com>
To: djmurray@buffalo.edu
Bcc:
Subject: Check the email header
Date: Thu, 9 Feb 2006 23:21:44 -0500
Mime-Version: 1.0
Content-Type: text/plain; format=flowed
X-OriginalArrivalTime: 10 Feb 2006 04:21:44.0284 (UTC) FILETIME=[53FB91C0:01C631E7]
X-UB-Relay: (bay105-f39.bay105.hotmail.com)
X-PM-Spam-Prob: : 7%
X-DCC-Buffalo.EDU-Metrics: email1.acsu.buffalo.edu 1028; Body=0

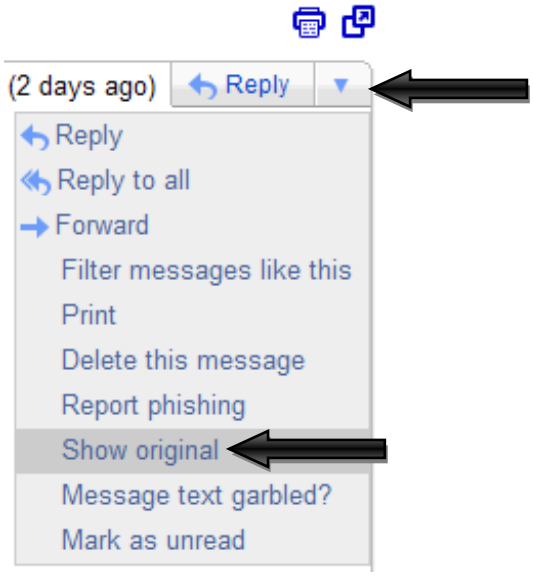
There is a DOS command called **nslookup** and a parallel command in UNIX called **host** which will lookup a hostname based on an IP address and vice versa. Open a

DOS command prompt and run the **nslookup** command to determine the hostname of the machine that sent the email message above. The syntax of the command is: **nslookup IPaddress** (where IPaddress is the IP of the machine you want to lookup)

Record the IP address of the sending computer: _____
Record the hostname of the sending computer: _____

Testing this in UB Webmail

Your next task is to analyze the email headers of any message you have received in your UB Webmail account. Do not select a message sent from another Gmail account since they normally remove some of the header information. First, open the message you would like to view the headers for. Next, click the **down arrow** next to Reply and select **Show Original**. The full message headers will appear in another window.



Include a copy of the message headers to submit. Also:

Record the IP address of the sending computer: _____
Record the hostname of the sending computer: _____

Next, go to the following website and try the **IP Locater** and **Spam Locater** tools with your message. http://www.geobytes.com/FreeServices.htm Record your findings.

You can also perform a whois query of the data on the geobytes.com website. Using the website, try a query on different whois databases and record your findings.

Alternatively, there is also a **whois** command in UNIX which can be used to lookup the domain registration information for a particular domain. The syntax is:
whois Domainname | more (where Domainname is the domain you want to check)

Additional Questions

1) What is DHCP? Does using DHCP make tracing email more or less difficult? Why?

2) What are the IP addresses for www.mgt.buffalo.edu? What tool did you use to find this information?

3) What domain name is associated with 128.205.4.175? What tool did you use?

4) Provide an example of one other network tool, utility or website that would be useful when investigating email.

5) Given the spam message below, who should be contacted about the email abuse? Hint: You might have to check multiple whois databases for this information

```
Return-Path: <PrFriedrickGxkF3TriggianoV@centex.net>
Received: from edge2.adelphia.net ([196.207.204.30]) by mta3.adelphia.net
        (InterMail vM.6.01.05.02 201-2131-123-102-20050715) with ESMTP
        id <20060203171446.WGDR2031.mta3.adelphia.net@edge2.adelphia.net>;
        Fri, 3 Feb 2006 12:14:46 -0500
Received: from [68.168.78.104] (really [196.207.204.30])
        by edge2.adelphia.net
        (InterMail vG.2.00.00.02 201-2161-108-103-20050713) with SMTP
        id <20060203171445.NRNT24782.edge2.adelphia.net@[68.168.78.104]>;
        Fri, 3 Feb 2006 12:14:45 -0500
Received: from highspeed.com (s660-402-58-007.stalk.net.nz[196.207.204.30])
        by cigi58.bt.com (zsvauqme18) with SMTP
        id <29365405902v32550fur7w>; Fri, 03 Feb 2006 14:14:38 -0300
Message-Id: <8285753468.12051608316@lgcy.com>
From: "Mycah Heinonen" <MmNialTeiO7PiecaitisN@firstva.com>
To: "Dheisler" <dheisler@adelphia.net>
Subject: Re: dusenbury
Date: Fri, 03 Feb 2006 10:08:38 -0700
MIME-Version: 1.0

Dear HomeOwner,

Your credit doesn't matter to us! If you OWN real estate and want IMMEDIATE cash to spend ANY way
you like, or simply wish to LOWER your monthly payments by a third or more, here are the deals we have
TODAY (hurry, these offers will expire TONIGHT) :  Low as

$432,000.00 at a 3.30,% fixed-rate        $381,000.00 at a 3.72,% variable-rate
$407,000.00 at a 3.00,% interest-only     $290,000.00 at a 3.49,% fixed-rate

Hurry, when these deals are gone, they are gone!  Simply fill out this one-minute form  Don't worry about
approval, your credit will not disqualify you!

http://<.pyrolyse.ref789.com


Sincerely,
Verna Steeves
Approval Manager
```