6.2.1

Tracing Email Headers

(YAHOO and VISUAL TRACE)

Previous | Next | Back to Messages Printable View - Brief Headers

Delete | Reply | Forward | Spam Move to folder... OK

This message is not flagged. [Flag Message - Mark as Unread]

X-Apparently-To: emailheaders@yahoo.com via 216.155.196.94; Sun, 07 Mar 2004 20:01:06 -0800
Return-Path: <timbucktwo@virtualmail.com>
Received: from 205.158.62.67 (EHLO webmail-outgoing.us4.outblaze.com) (205.158.62.67) by mta142.mail.scd.yahoo.com with SMTP; Sun, 07 Mar 2004 20:01:05 -0800
Received: from spf9.us4.outblaze.com (spf9.us4.outblaze.com [205.158.62.169]) by webmail-outgoing.us4.outblaze.com (Postfix) with QMQP id D92351801388 for <emailheaders@yahoo.com>; Mon, 8 Mar 2004 04:01:05 +0000 (GMT)
X-OB-Received: from unknown (205.158.62.148) by wfilter.us4.outblaze.com; 8 Mar 2004 04:00:52 -0000
Received: by ws5-6.us4.outblaze.com (Postfix, from userid 1001) id E511221AF4D; Mon, 8 Mar 2004 04:01:04 +0000 (GMT)
Content-Type: text/plain; charset="iso-8859-1"
Content-Disposition: inline
Content-Transfer-Encoding: 7bit
MIME-Version: 1.0
X-Mailer: MIME-tools 5.41 (Entity 5.404)
Received: from [66.191.121.99] by ws5-6.us4.outblaze.com with http for timbucktwo@virtualmail.com; Mon, 08 Mar 2004 12:01:04 +0800
From: "John Doe" <timbucktwo@virtualmail.com> Add to Address Book
To: emailheaders@yahoo.com
Date: Mon, 08 Mar 2004 12:01:04 +0800
Subject: Test Email Headers
X-Originating-Ip: 66.191.121.99
X-Originating-Server: ws5-6.us4.outblaze.com
Message-Id: <20040308040104.E511221AF4D@ws5-6.us4.outblaze.com>
Content-Length: 168

This is a test email from VirualMail.com
--

Laboratory Overview

Objective

At the end of this lab, students will be able to view and trace email headers to determine the original sender using software utilities and internet tracking.

Information for Laboratory

A. Students will use Yahoo web-based email client, or similar product, to send and receive email.
B. Students will use the internet websites to lookup IP addresses.
C. Students will use Visual Trace software and additional network tools to aide in determining e-mail sender.

Student Preparation

The student will have completed requisite reading. The student will require paper for notes and should be prepared to discuss the exercises upon completion. The student should have familiarity with email in general and protocols.

Students will prepare PCs with a copy of Visualware's eMailTrackerPro version 4 and VisualRoute 2005 Personal Edition. Students will also need to obtain a SPAM email to forward to themselves in step 9.

Estimated Completion Time

60 Minutes

Email has become a mission critical application for our daily business and personal transactions. It has become the most cost-efficient method of communication. It is used around the world to conduct business. Downtime for email has become a costly factor to many businesses. These messages may contain critical or confidential data that are transferred through many computer systems and across many networks.

Email has also become the transport of choice to pass unsolicited advertising (spam), DOS (Denial of Service) attacks, viruses and worms.

Due to the low cost, spammers are taking advantage of email vulnerabilities to send their advertising messages to millions of people. These messages often referred to as 'junk mail,' take up a great volumes of resources on servers, bandwidth and time for removal.

Email addresses can be easily harvested and used to gain information or access to other company resources. They have also been used to represent major corporations and eventually to steal data, passwords or other personal information.

DOS (Denial of Service) attacks occur when a site or domain is flooded with more traffic than the systems can handle. This has been another avenue for email.

Viruses use email as the preferred method to transfer and replicate themselves. They have become sophisticated enough to 'spoof' or mask the real address to make the receiver believe it is a message from a friend or family member.

To determine who is sending the emails or where they originate may take a considerable amount of time, investigation and tools. It will also take some knowledge about who to notify once the email originator is determined.

For purposes of simplicity we will use Yahoo.com to demonstrate.

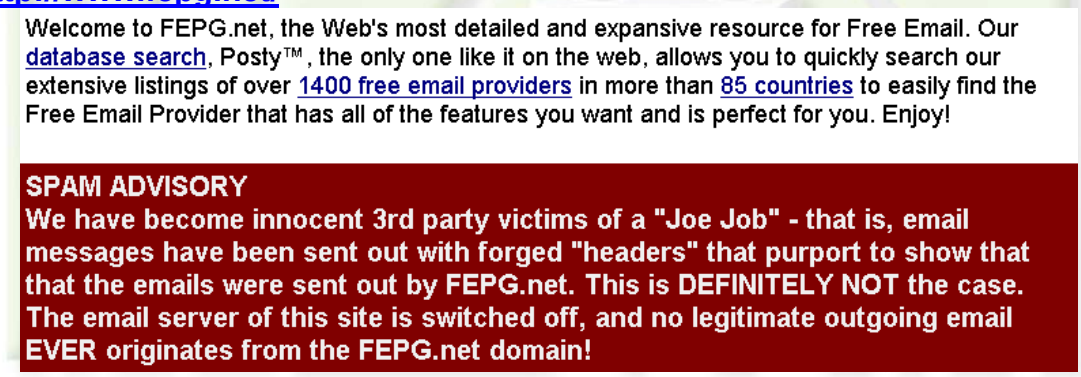
Step 1: Create Email Account(s)

To Begin this lab, you will need to create a web-based email account. Web-based email is preferred since we do not have to setup a mail server and clients. A PC that is using Mozilla (Netscape), Outlook, or any other email client may also be used, but is not discussed in this lab. To view headers from these applications go to this site:
http://www.abika.com/Reports/Samples/emailheaderguide.htm

If this lab is performed with other participants, email accounts should be used from various providers to aide in the diversity of email header information. If this lab is performed alone, it is recommended to create accounts from two separate providers.

Some examples of free web-based email clients include Yahoo.com, hotmail.com and virualmail.com. If you still have difficulties finding a free email provider, look at:

http://www.fepg.net/

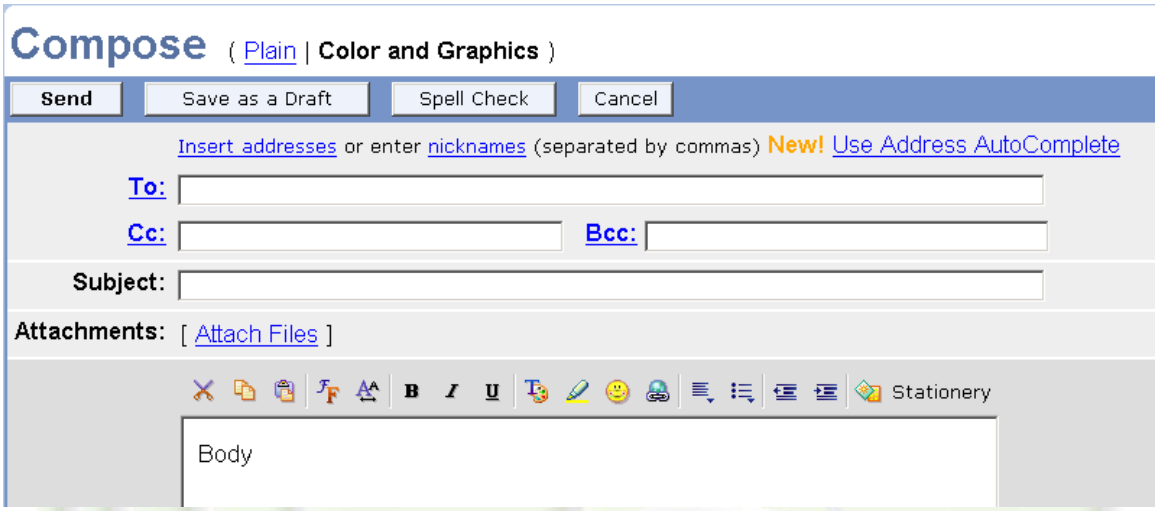


Note that this company has a posting on their homepage to warn people about 'forged' headers, which we will discuss later. If you plan to use Yahoo.com, follow these steps:

- Open your browser and type www.yahoo.com in the URL.
- Click on the Mail icon at the top of the page.
- Click on the Sign Up Now link if you do not already have an account.
- Continue the setup process until you have successfully created an email account and you are logged into the account.

Step 2: Sending Email

While in your web-based email, send an email to several of your classmates and copy yourself.



The email is comprised of a header and a body. The header is the information about the email such as the To:, Cc: and Subject, while the body is the content of what is being sent (payload).

Although most messages are sent through standard client applications, this information can be modified, entered via a webpage or manually.

Step 3: Understanding SMTP

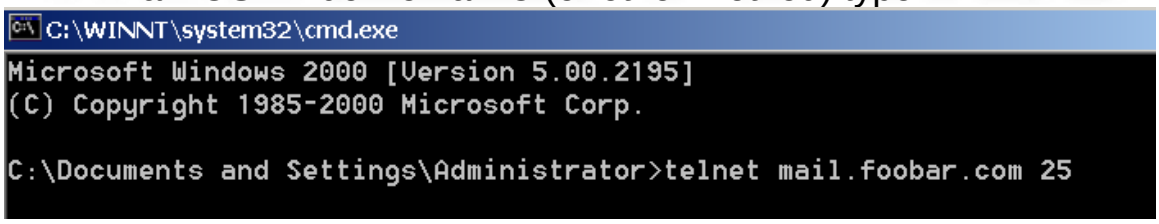
To better understand email, we need to know the basics on how it works. When receiving email through our email client, we use TCP with POP3 (Post Office Protocol, port 110) or IMAP (Internet Mail Access Transport, port 143). When sending an email, we use SMTP (Simple Mail Transfer Protocol, port 25).

SMTP is based upon the standard RFC 822 (Request For Comments), which is now superceded by RFC 2822, http://www.faqs.org/rfcs/rfc2822.html . SMTP is generally used to send messages from a mail client to a mail server. Receiving mail through POP3 and IMAP are outside the scope of this lab at this time.
It is also referenced in RFC 1123.

When an SMTP client has a message to transmit, it establishes a two-way transmission channel to an SMTP server. The SMTP server will either transfer the message to one or more SMTP servers or report the failure.

Channels are opened and closed using commands:
HELO <SP> <domain> <CRLF>
and
QUIT <CRLF>

Channels can be opened manually by telneting into the mail server:
In a DOS window on a PC (or other method) type:



where mail.foobar.com is the mail server.

The telnet software connects and the mail server responds with a message similar to...
Trying 204.251.174.179...

Connected to mail.foobar.com.
Escape character is '^]'.
220 mail.foobar.com ESMTP Sendmail 8.8.3/8.6.12 ready

At the prompt, type: *Helo mail.foobar.com*

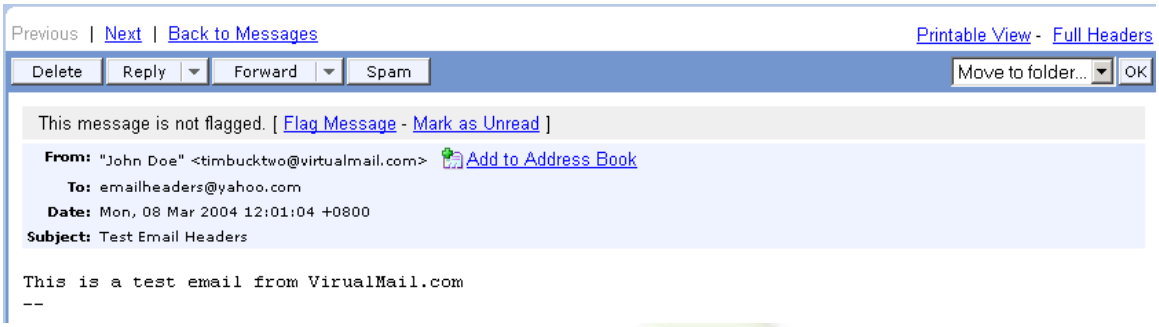
To end the session, type *QUIT <CRLF*

Try this exercise. It is important to note that many mail servers do not allow this kind of direct connection to their servers. This includes Yahoo and MSN.

A full email message could be sent using this method, but is not discussed here. For more information about sending email via this method, follow this link: http://www.fmp.com/spam_patrol/ .

Step 4: Examining Received Email

Open your web browser and open one of the emails that were sent by another student. If you are using Yahoo.com, there is a link on the right side that when clicked, will expand the header information.



Becomes

Notice that the original From, To, Date, and Subject are still incorporated in the expanded version. Additional information in this view is going to assist us in determining the original sender.

Let's examine some of these fields individually:

X-Apparently-To: emailheaders@yahoo.com via 216.155.196.94; Sun, 07 Mar 2004 20:01:06 -0800

This shows the person who apparently receives the email.

Return-Path: <timbucktwo@virtualmail.com>

This is where the email reply will be sent.

From: "John Doe" <timbucktwo@virtualmail.com> Add to Address Book
To: emailheaders@yahoo.com
Date: Mon, 08 Mar 2004 12:01:04 +0800
Subject: Test Email Headers

This information was created when the email was created. It may not reflect accurate information; even the date can be rewritten.

X-Originating-Server: ws5-6.us4.outblaze.com
Message-Id: <20040308040104.E511221AF4D@ws5-6.us4.outblaze.com>

This is the sender's server and message information. The message ID is a unique identifier on the server listed. Since the email was sent via an email provider, this shows outblaze.com as the provider for virtualmail.com.

X-Originating-Ip: 66.191.121.99

This is the originating IP address of the sender. It is not available in all header emails. It is identical to one of the IP addresses found in the Received section, which is one clue.

Content-Type: text/plain; charset="iso-8859-1"

This section describes how the receiver should interpret the email. This example is plain text, but it could also be rich text (HTML) or both.

The most important header information for tracking purposes is the Received header field, which is usually in one of:
Received: from by via with id for

Remember to trust nothing here. We could be fooled that this email was sent from a user "John Doe" or timbucktwo@virtualmail.com, but we know that this email

address could be 'spoofed,' or faked from anyone.

Received: from 205.158.62.67 (EHLO webmail-outgoing.us4.outblaze.com) (205.158.62.67) by mta142.mail.scd.yahoo.com with SMTP; Sun, 07 Mar 2004 20:01:05 -0800

The received field that is closest to the top is the last one received. It was inserted by yahoo.com and was forwarded using SMTP on Sunday March 7th, 2004. The IP address used here is from yahoo.com and not from the original sender.

Received: from 205.158.62.67 (EHLO webmail-outgoing.us4.outblaze.com) (205.158.62.67) by mta142.mail.scd.yahoo.com with SMTP; Sun, 07 Mar 2004 20:01:05 -0800

Received: from spf9.us4.outblaze.com (spf9.us4.outblaze.com [205.158.62.169]) by webmail-outgoing.us4.outblaze.com (Postfix) with QMQP id D92351801388 for <emailheaders@yahoo.com>; Mon, 8 Mar 2004 04:01:05 +0000 (GMT)

X-OB-Received: from unknown (205.158.62.148) by wfilter.us4.outblaze.com; 8 Mar 2004 04:00:52 -0000

Received: by ws5-6.us4.outblaze.com (Postfix, from userid 1001) id E511221AF4D; Mon, 8 Mar 2004 04:01:04 +0000 (GMT)

The last received fields were sent from outblaze.com, which is the domain for virtualmail.com. The line *spf9.us4.outblaze.com (spf9.us4.outblaze.com [205.158.62.169])* might make us think that this may have come from outblaze.com, but we will need to verify that. In most cases, we would examine the last Received: field and would look at the IP address in [ ] . Since in this case that last address in [ ] is from outblaze.com, we want to use that information as a possible clue. Document the IP addresses, domains and other information as necessary in the received field.

Examine the email that you received from a classmate. Document:

Basic Information

From: _____

To: _____

Date: _____

Subject: _____

Last Received

Domain : _____

IP Address: _____

Other Information of Importance

_____
_____
_____

Step 4: Tracing to the Origin

The first step to remember is that there are many variables. We will present some of those here. Our class example shows the following:

Basic Information

From: "John Doe" <timbucktwo@virtualmail.com>
To: emailheaders@yahoo.com
Date: Mon, 08 Mar 2004 12:01:04 +0800
Subject: Test Email Headers

Last Received

Domain : ws5-6.us4.outblaze.com
IP Address: [205.158.62.169] by webmail-outgoing.us4.outblaze.com

Other Information of Importance

Postfix, from userid 1001 (which may be traceable to the web-mail client)

In most cases, the topmost Received: field is accurate, but the fields below it are suspect. Be careful because spammers will often spoof Received: headers. If you examine them, you may see IP addresses such as "325.182.999.500" or "000.000.000". If you have performed the IP address lab, you will note these addresses are not valid. If one Received: header is spoofed, it is likely that the remaining Received: headers below it will also be spoofs.

The most credible information is the IP address that comes closest the body of the document and is surrounded by [ ] . This IP address gives us a clue to the origin of the device that was creating the message.

The first address we examine is [205.158.62.169] . Since this address was from the mail server and insert during a relay, it is not likely to be our originator. This web server added a field that we should use:

X-Originating-Ip: 66.191.121.99

To determine who owns this address, we can open a web browser and go to the American Registry for Assigned Numbers:
http://www.arin.net

Enter this IP address and determine its origin.

Output from ARIN WHOIS

ARIN Home Page | ARIN Site Map | ARIN WHOIS Help | Tutorial on Querying ARIN's WHOIS

Search for : Submit Query

Search results for: 66.191.121.99

```
Charter Communications CHARTER-NET-5BLK (NET-66-188-0-0-1)
                                66.188.0.0 - 66.191.255.255
Charter Communications MDSN-WI-66-191-112 (NET-66-191-112-0-1)
                                66.191.112.0 - 66.191.127.255

# ARIN WHOIS database, last updated 2004-03-07 19:15
# Enter ? for additional hints on searching ARIN's WHOIS database.
```

This is the first step. But up we can also do an nslookup to determine if we can find the host. If you are using Windows 2000 or greater, open a DOS window and type NSLOOKUP. The results:

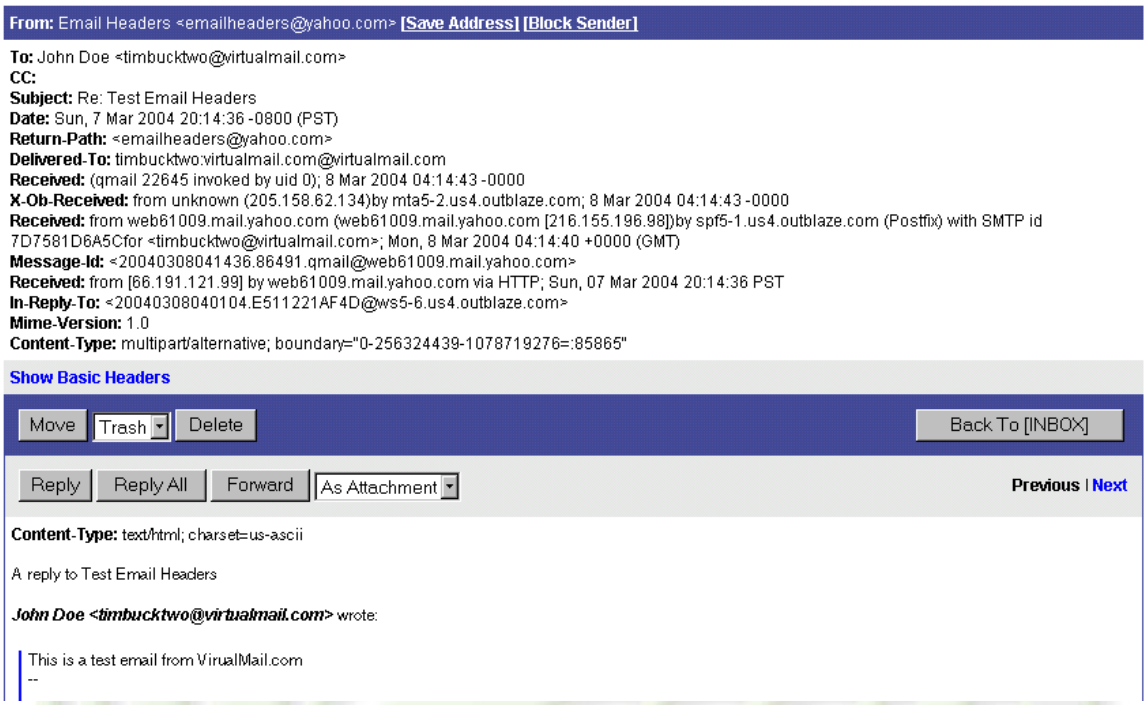
U:\>nslookup 66.191.121.99
Server: {your DNS server}
Address: {your DNS server IP Address}

Name: 66-191-121-99.mad.wi.charter.com

Address: 66.191.121.99

Be sure to verify names and IP addresses. If someone has ‘spoofed’ a name, the IP address may still be correct.

A reply email was sent using the same computer from Yahoo mail to the VirtualMail in this example and notice the virtualmail.com client also recognizes the same IP address.



The last received line show *from [66.191.121.99]*.

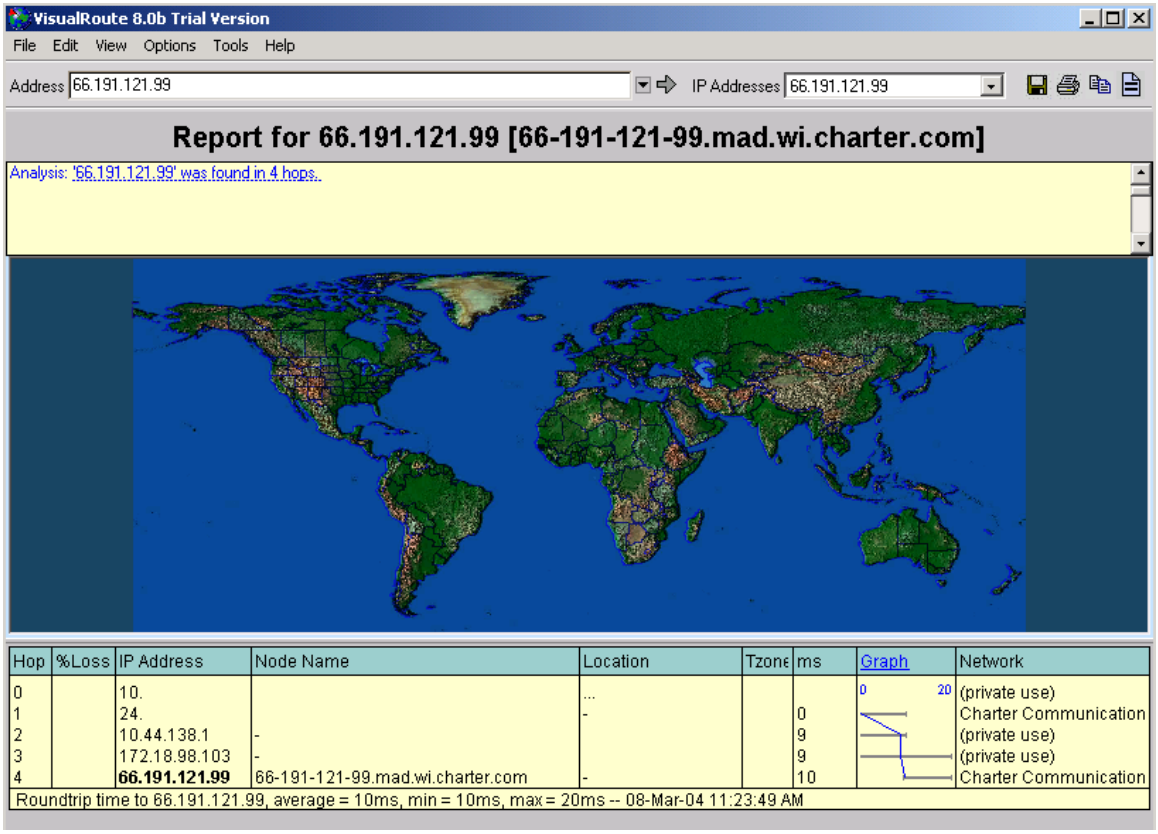
What information is similar to the Yahoo.com web mail client?

What information is different from the Yahoo.com web mail client?

What are the similarities / differences between and Outlook or Netscape mail client?

Step 5: Tools

One tool that may assist in finding the IP address is an application from visualware.com. If your PC does not have a copy of VisualRoute version 8, go to the visualware.com's website and download the tool. Enter the IP address in the previous example:



Note: Hop 0 and 1 were removed for privacy.

This information can then be used to contact the provider to report abuse. Note that the NetName is MDSN-WI-66-191-112. It gives further information that the sender is near Madison, Wi.

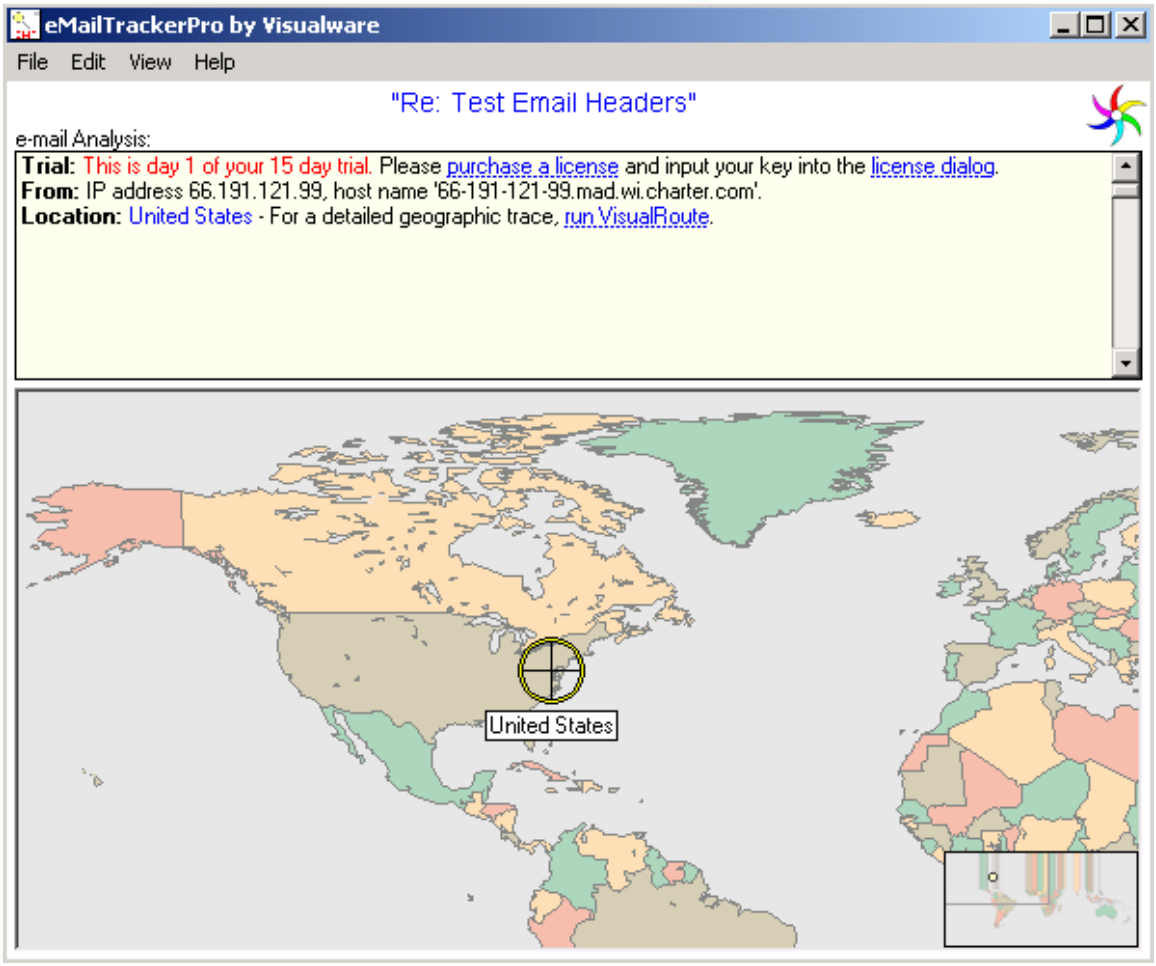
This tool is similar to tracert, but there are added features and lookups. This can be used to find the upstream provider,

should you decide to report abuse.

If you click on the Charter Communications Network under the Network heading, you'll find much of the same information the was gathered manually at www.arin.net:

Step 6: Another Tool by Visualware

Another tool by Visualware allows the user to enter the header information and it will attempt to locate the sender. This product, eMailTrackerPro, allows you to paste in the header information to trace the email. To enter header information, copy the header from your mail client, open EmailTrackerPro and click File – Import Headers. Paste the header into the window and click OK. Note: you can run Visual Trace from here.



Step 7: **Example 1**

This fraudulent email below was recently received. Review the information and complete the questions.

Received: from [24.15.159.131] (helo=c-24-15-159-131.client.comcast.net)
by xeon.servnow.com with smtp (Exim 4.24)
id 1AyZp5-0004ZP-Or; Wed, 03 Mar 2004 12:06:20 -0500
Received: from 136.40.236.44 by 24.15.159.131; Thu, 04 Mar 2004 11:05:34 +0300
Message-ID: <TAOVIRWWWXRPPZYHRWWXUKO@yahoo.com>
From: "Cornelius Groves" <kamvma@hotmail.com>
Reply-To: "Cornelius Groves" <kamvma@hotmail.com>
To: is@rowepottery.com
Subject: take control of the lending process
Date: Thu, 04 Mar 2004 10:03:34 +0200
X-Mailer: eGroups Message Poster
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary="--7661807057840260"
X-Priority: 3
X-MSMail-Priority: Normal
X-Spam-Exim: wTAjSJDaV3GaeUvAzXg5NXCbrwqerewqOpen your

Basic Information

From: _____
To: _____
Date: _____
Subject: _____

Last Received

Domain : _____
IP Address: _____

Other Information of Importance

_____
_____
_____

-

Step 8: Example 1 Solved

It may appear that this email was from someone at Hotmail or Yahoo. It also may appear that if we followed the IP address, 136.40.236.44, it would lead to Ford Motor Company, which is incorrect. We further see that the IP address in the brackets [24.15.159.131] is the originator.

NETWORK: NET-24-12-0-0-1 [262144] (whois.arin.net) Snap...

```
CustName:    Comcast Cable Communications
Address:     3 Executive Campus
Address:     5th Floor
City:        Cherry Hill
StateProv:   NJ
PostalCode:  08002
Country:     US
RegDate:     2003-12-01
Updated:     2003-12-01

NetRange:    24.12.0.0 - 24.15.255.255
CIDR:        24.12.0.0/14
NetName:     ILLINOIS-14
NetHandle:   NET-24-12-0-0-1
Parent:      NET-24-0-0-0-1
NetType:     Reassigned
Comment:     NONE
RegDate:     2003-12-01
Updated:     2003-12-01

OrgAbuseHandle: NAPO-ARIN
OrgAbuseName:   Network Abuse and Policy Observance
OrgAbusePhone:  +1-856-317-7272
OrgAbuseEmail:  abuse@comcast.net

OrgTechHandle: IC161-ARIN
OrgTechName:   Comcast Cable Communications Inc
OrgTechPhone:  +1-856-317-7200
OrgTechEmail:  cips_ip-registration@cable.comcast.com

# ARIN WHOIS database, last updated 2004-03-07 19:15
# Enter ? for additional hints on searching ARIN's WHOIS database.
```

Step 9 Example 2

Solve the source of the email below. Review the information and complete the questions.

```
Return-Path: <HadrianSammut@kpmg.com.mt>
Received: from maltanet.net (mailer6.maltanet.net [194.158.37.38])
        by wccnet.edu (8.12.11/8.12.11) with ESMTP id i337MfmZ022383
        for <mgalea@wccnet.org>; Sat, 3 Apr 2004 02:22:42 -0500 (EST)
Received: (qmail 25792 invoked by alias); 3 Apr 2004 06:28:05 -0000
Delivered-To: srch0401@maltanet.net
Precedence: bulk
Received: (qmail 31283 invoked by uid 511); 3 Apr 2004 06:13:26 -0000
Received: from unknown (HELO mail.kpmg.com.mt) ([194.158.44.250])
      (envelope-sender <HadrianSammut@kpmg.com.mt>)
      by 0 (qmail-ldap-1.03) with SMTP
      for <srch0401@maltanet.net>; 3 Apr 2004 06:13:25 -0000
Received: from mtpieexc01.mt.kpmg.com (mtpieexc01.kpmg.com.mt) by mail.kpmg.com.mt
 (Content Technologies SMTPRS 4.2.1) with ESMTP id
<T68bbd2efad0a14140218d@mail.kpmg.com.mt> for <srch0401@maltanet.net>;
 Sat, 3 Apr 2004 08:09:22 +0200
Received: by mtpieexc01.kpmg.com.mt with Internet Mail Service (5.5.2653.19)
        id <GMXND100>; Sat, 3 Apr 2004 08:19:43 +0200
Message-ID: <4CBE7C48623BD711847D00508B0F1DD50105F10E@mtpieexc01.kpmg.com.mt>
From: Hadrian Sammut <HadrianSammut@kpmg.com.mt>
To: srch0401@maltanet.net
Subject:
Date: Sat, 3 Apr 2004 08:19:42 +0200
MIME-Version: 1.0
X-Mailer: Internet Mail Service (5.5.2653.19)
Content-Type: multipart/alternative ; boundary="----_=_NextPart_001_01C41943.A6F083E0"
X-Scanned-By: MIMEDefang 2.39
X-Spam-Checker-Version: SpamAssassin 2.63 (2004-01-11) on orchard.wccnet.org
X-Spam-Level:
X-Spam-Status: No, hits=0.2 required=5.0 tests=EXCUSE_16,HTML_MESSAGE
        autolearn=no version=2.63
```

Basic Information

From: _____

To: _____

Date: _____

Subject: _____

Last Received

Domain : _____

IP Address: _____

Other Information of Importance

_____
_____

Step 10: Example 2 Solved

Using the header, we assume:

Basic Information

From: Hadrian Sammut <HadrianSammut@kpmg.com.mt>
To: mgalea@wccnet.org (via srch0401@maltanet.net)
Date: Sat, 3 Apr 2004 08:19:42 +0200
Subject: <blank>

Last Received

Domain : mail.kpmg.com.mt
IP Address: 194.158.44.250

Other Information of Importance

The use of Internet Mail Service

Using tools described above, we determine that the IP address and the domain name match the nslookup.

U:\>nslookup 194.158.44.250
Server: mydnsserver.com
Address: 192.168.1.1

Name: mail.kpmg.com.mt
Address: 194.158.44.250

U:\>nslookup 194.158.37.38
Server: mydnsserver.com
Address: 192.168.1.1

Name: mailer6.maltanet.net
Address: 194.158.37.38

We can further lookup the domain name using one the four regional internet registries. Since the .com.mt extension is a European domain, it is best to search using www.ripe.net. We may also want to review a universal 'WhoIs' to help us determine the TLD (Top Level Domain) and determine the best location to search for the owner. (http://www.uwhois.com/cgi/domains.cgi?User=NoAds)

There are currently four Regional Internet Registries:

- **ARIN**
  American Registry for Internet Numbers
  http://www.arin.net
- **APNIC**
  Asia Pacific Network Information Centre
  http://www.apnic.net
- **LACNIC**
  Latin American and Caribbean IP address Regional Registry
  http://lacnic.net/en/index.html
- **RIPE NCC**
  Réseaux IP Européens Network Coordination Centre
  http://www.ripe.net

Searching for the IP Address 194.158.44.250, we determine the owner is, in fact, KPMG and has the IP Address assigned to them.

Query the RIPE Whois Database

Search for 194.158.44.250 [Search] [Reset Form]

[Advanced search]

```
% This is the RIPE Whois server.
% The objects are in RPSL format.
%
% Rights restricted by copyright.
% See http://www.ripe.net/ripencc/pub-services/db/copyright.html

inetnum:        194.158.44.240 - 194.158.44.255
netname:        MT-TERRANET-20021024
descr:          KPMG
descr:          Malta
country:        MT
admin-c:        TM2960-RIPE
tech-c:         WF113-RIPE
rev-srv:        engine4.maltanet.net
rev-srv:        engine2.maltanet.net
status:         ASSIGNED PA
mnt-by:         AS5532-MNT
changed:        wilhelm@maltanet.net 20030328
source:         RIPE

route:          194.158.32.0/19
descr:          Terranet Ltd. Block
```

Further down the Ripe NCC page contact information can be found to report abuse or to contact the owner.

Step 11 Exercises

Choose emails from several classmates. Open their headers and trace them to the originating IP address and name.

Choose a SPAM email, if available, and determine its origin.

Step 12 Reporting

Once you have determined who you believe to be the originator, you can verify that this contact information is not the spammer or a company that ignores spam reports by checking on various websites (below). Those companies will likely not respond to your requests for action.

If they are legitimate companies, contact the administrator to inform them of a possible spammer or that someone has breached their mail systems. You should include a full copy of the email header, which will help them verify the source of the email.

To report abuse, go to one of these websites:

http://www.abuse.net/
http://www.fmp.com/spam_patrol/
http://www.cauce.org/

Test your server for vulnerability: http://www.abuse.net/relay.html

The examples shown here are basic and do not include headers that were inserted into a third party mail server. In those cases, the mail would appear to come from that source, but in reality, that provider has a problem with an open SMTP port 25.

Analysis

1) There are many header fields that can be changed to 'fool' the unsuspecting receiver to the originator's identity. What are they?

2) What tools and websites can assist you in finding the email originator?

3) Why is it important to notify vendors and ISPs of abuse?

Summary Discussion

A classroom discussion should follow the lab. Review the lab questions and your analyses as a group. Share your experiences and knowledge with the class.

If You Want To Learn More

Tracing email headers can lead you down many paths. There are many tools on the internet to assist in tracing the headers to an ISP and eventually to a person. The links below may provide some additional information to "Tracing Email Headers."

http://www.web-police.org/law_enforcement_information/general_information/Reading_email_headers.html

http://www.stopspam.org/email/headers.html

http://www.investigateanyoneonline.com/tracemail.shtml

http://pages.ebay.com/help/policies/rfe-spam-send-headers.html

http://spamcop.net/fom-serve/cache/19.html

http://www.haltabuse.org/help/headers/index.shtml

http://abuse.msu.edu/email-headers.html

http://www.spamabuse.org/content_TrackingSpammersâ€"DecipheringEmailHeaders.htm

http://www.dpo.uab.edu/technotes/FAQ.html

http://www.cibir.net/email/headers.htm

http://info-center.ccit.arizona.edu/~ccitinfo/newsletters/february2003/e-mail_headers.html

http://www.google.com/search?q=finding+e-mail+headers&hl=en&lr=&ie=UTF-8&oe=UTF-8&start=10&sa=N

Other useful websites:

IANA – Internet Assigned Numbers Authority	http://www.iana.org/
ARIN – American Registry for Internet Numbers	http://www.arin.net
ARIN – American Registry for Internet Numbers	http://www.arin.net
APNIC – Asian Pacific Network Information Centre	http://www.apnic.net
LACNIC – Latin America and Carribean Registry	http://www.apnic.net
RipeNCC – Reseaux IP European Network Coord. Centre	http://www.ripe.net

Appendix:

This lab was developed using Visualware's eMailTrackerPro version 4 and VisualRoute 2005 Personal Edition, both of which can be obtained from:

www.emailtrackerpro.com

The OS environment for this lab was Windows XP Professional, Version 2002, Service Pack 2 (8/04).