CHAPTER

Tracing IP Addresses Through the Internet

8

Everybody should want to make sure that we have the cyber tools necessary to investigate cyber crimes, and to be prepared to defend against them and to bring people to justice who commit it.
Janet Reno, Former Attorney General of the United States

Tracing IP addresses

Internet Protocol (IP) addresses provide the basis for online communication, allowing devices to interface and communicate with one another as they are connected to the Internet. As was noted in Chapter 3, IP addresses provide investigators a trail to discover and follow, which hopefully leads to the person(s) responsible for some online malfeasance. In Chapter 5 and 6, we discussed different tools that investigators can use to examine various parts of the Internet, including identifying the owners of domains and IP addresses. In this chapter, we are going to discuss tracing an IP address and the investigative advantages of this process. We have covered the tools to help us trace IP addresses in previous chapters, but here we want to walk through the process of identifying the IP to trace and who is behind that address.

Online tools for tracing an IP address

Tracing IP addresses and domains is a fundamental skill for any Internet investigator. There are many resources available on the Internet to assist in this process. Of primary importance are the entities responsible for the addressing system, namely, the Internet Assigned Number Authority (IANA) and its subordinate bodies the Regional Internet Registries (RIR). In addition to IANA and RIR, there are a multitude of other independent online resources that can assist the investigator in conducting basic IP identification.

IANA and RIR

Starting at the top is IANA. According to their website they are "...responsible for the global coordination of the DNS Root, IP addressing and other Internet protocol resources." What this means to the investigator is that they manage and

Investigating Internet Crimes.

assign the top level domains, that is, .com, org, mil, edu. (see Table 3.6 for additional examples) and coordinate the IP addresses and their allocation to the RIR. IANA established the RIR to allocate IP address in geographical regions.

The RIR system evolved over time, eventually dividing the world into the following five regions:

1. African Network Information Centre (AfriNIC) for Africa, http://www.afrinic.net/
2. American Registry for Internet Numbers (ARIN) for the United States, Canada, several parts of the Caribbean region, and Antarctica, https://www.arin.net/
3. Asia-Pacific Network Information Centre (APNIC) for Asia, Australia, New Zealand, and neighboring countries, http://www.apnic.net/
4. Latin America and Caribbean Network Information Centre (LACNIC) for Latin America and parts of the Caribbean region, http://www.lacnic.net/en/web/lacnic/inicio
5. Réseaux IP Européens Network Coordination Centre (RIPE NCC) for Europe, Russia, http://http://www.ripe.net/

Each site has a search "Whois" function that allows the investigator to identify IP registration information. IANA and the RIR are the official registrars and owners of the domain records and IP addresses. An investigator wishing to verify the owner of an IP can use the RIR to locate the records.

Internet commercial and freeware tools

There are also many Internet sites to look up IP and Domain registrations. Some provide the basic registration information and other sites combine additional tools that enable the investigator to identify an IP's physical location. The following websites, mentioned in Chapter 6, are easily accessible from the Vere Software Internet Investigators Toolbar, and are important utilities for the investigator:

DNS Stuff (http://www.dnsstuff.com/tools/tools): This website has been around for a number of years. It offers both free and pay options for assisting in IP addresses identification and other online information.
Network-Tools.com (http://network-tools.com): Another website with a simple user interface to assist in IP tracing.
CentralOps.net (http://centralops.net/co/): This is another website that assists with your IP tracing. One of its features, Domain Dossier, does multiple lookups on an IP address or domain.

In some circumstances, the investigator may look up a domain or and IP address with these commercial tools and find the address concealed by the commercial registrar. In these cases, the investigator may need to go to the commercial registrar's site and use the Whois search located there to determine the domain registration records. Each of the mentioned websites presents the domain

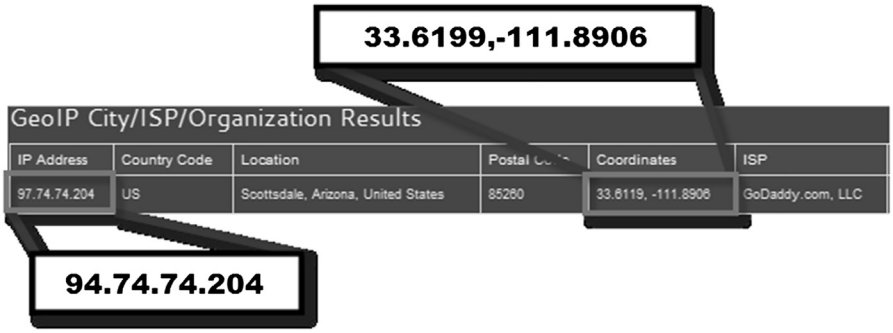

FIGURE 8.1

Maxmind demo search for IP address.

registration information in a slightly different manner and may have additional tools useful to the investigator. Experience with each will provide the investigator with a better understanding of each site's features.

Geolocation of an IP address

Geolocation in general refers to the identification of the real geographical area of an electronic device, such as a cell phone, IP addresses, WiFi, and MAC addresses. Now that being said that does not mean an IP address can be traced directly to a house. Geolocation particularly for IP addresses is not an exact science. Unlike cell phones that can be traced via their GPS coordinates or cell tower triangulation, IP addresses use a common database of address locations maintained by different companies. One of the most commonly used databases is maintained by Maxmind, Inc. which can be found at www.maxmind.com. Maxmind provides a free service to geolocate an IP address to a state or city. Purchasing their services can give the Internet investigator access to a more precise location, up to and including physical addresses. There are other online services that provide geolocation identification of IP addresses such as IP2Location.com. Some investigative tools, such as Vere Software's WebCase, include access to the Maxmind database as a feature of its domain lookup. On Maxmind's website you can use their demo function to identify an IP addresses location. An example of a Maxmind search for the geolocation of IP address 97.74.74.204 is shown in Figure 8.1.

Along with identifying the geolocation of the address as Scottsdale, Arizona, website provides the latitude and longitude based on this location and the Internet Service Provider (ISP) hosting the IP address, in this case GoDaddy.com LLC.

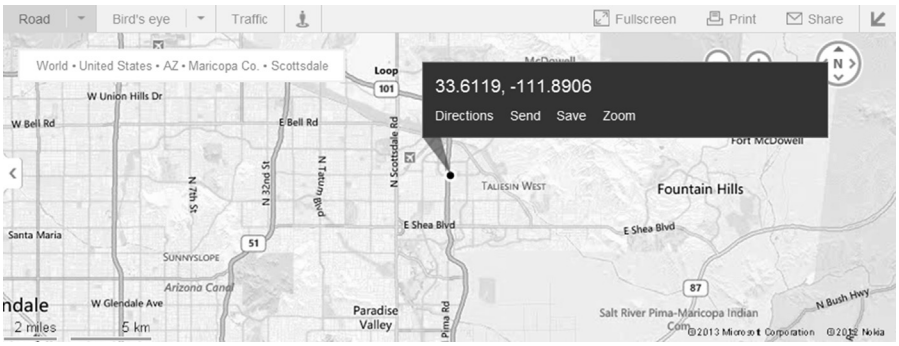

FIGURE 8.2

Bing Maps search for specific latitude and longitude.

TOOLS AND TIPS

Map the IP Address

With the latitude and longitude of an IP address provided through Maxmind, you can enter data into Google Maps, Bing Maps, or any of the online mapping programs to translate those coordinates into a physical location on a map (Figure 8.2).

Using geolocation to identify an IP address may get you close or it may not. What the geolocation will tell you is the identified location of the IP address. The databases get this information from a variety of sources including ISP) and self-reported data. Most often, the Geolocation will give you a general idea of the server location hosting the IP address and not the physical location of anyone committing a crime. However, this information does provide verification of ISP ownership of an IP address, which can further the investigation, including referrals to the appropriate local agency for assistance. Be aware that geolocation can identify an IP address if known, but this address may be to an ISP or could be a Tor exit node (see Chapter 9 for further information on Tor) and not actually related to the target.

Digging deeper into IP tracing—what the DNS tells us

The basics of IP tracing are finding out who owns a domain or who is registered to an IP address. Once that is found out, you contact the ISP for further information (usually through some means of legal service). But what other things can you find out about an IP address online without an attorney? Let's take a look at some of the things available to us that can be traced from a domain or an IP address through the DNS records.

DNS records

The Domain Name System (DNS) is a service on the Internet that translates the Uniform Resource Locators (URLs) or domain names into an IP address. Domain

names are alphabetic making them easier to remember. The Internet, however, is based on IP addresses and communicates using that number sequence. The DNS in its simplest form is a big telephone book. Computers use it to look up the location of the server to which the IP address is located. So what other potential information is available to the investigators on the DNS?

Using the online website CentralOps.net, we can identify additional information about a domain. As an example we have used www.veresoftware.com to search under "Domain Dossier" and selected the "DNS records" search. With that search, we are returned with a variety of additional information on the domain and the records contained on the DNS server (Table 8.1).

The "type" of record gives us certain additional information on the domain:

- CNAME stands for "Canonical Name" record:
  CNAME is a type of DNS record that identifies the domain name as an alias of another. This tells the investigator whether or not there are other services running on that domain (such as an FTP or a web server running on different ports) on a single IP address. Each of these services will have its own entry on DNS (such as ftp.veresoftware.com and www.veresoftware.com).
- SOA stands for "start of authority" record:
  This DNS entry specifies authoritative information about a DNS zone (DNS zones may be a single domain or several), including the primary name server, the email of the domain administrator, the domain serial number, and several timers relating to refreshing the zone.

Table 8.1 CentralOps.net DNS Records Search for www.veresoftware.com

Name	Class	Type	Data	
www.veresoftware.com	IN	CNAME	veresoftware.com	
veresoftware.com	IN	SOA	server:	ns43.domaincontrol.com
			email:	dns.jomax.net
			serial:	2007112000
			refresh:	28800
			retry:	7200
			expire:	604800
			minimum ttl:	86400
veresoftware.com	IN	MX	preference:	0
			exchange:	smtp.secureserver.net
veresoftware.com	IN	NS	ns43.domaincontrol.com	
veresoftware.com	IN	NS	ns44.domaincontrol.com	
veresoftware.com	IN	A	97.74.74.204	

- MX stands for "mail exchange" record:
  The DNS record maps the domain researched to the mail exchange servers registered to that domain.
- NS stands for "name server" record:
  This record identifies the authoritative name servers for the domain.
- A stands for "address" record:
  This DNS record identifies the IP address assigned to the domain researched.

So how can that be useful in your investigations? With the DNS records, we can identify the server that provides email service to the domain. This is the MX record. This record can provide us a lead to additional domains used or operated by the domain of interest. The CNAME can give potentially additional services running on an IP address. The NS record can give you further information about the upstream ISP that services the domain being researched.

TOOLS AND TIPS

So How Do We Ultimately Determine IP Address Assignment?

- Search the IP address through a domain identifying tool, such as Network Tools.
- Upon identifying the company that is assigned the IP address, determine the proper legal compulsion method to obtain the records being sought prior to contacting them (see Chapter 4).
- Beware the ISP may attempt to notify the target about your actions without an order from a court stating not to identify the account holder. Additionally, if the ISP believes that the account is being used for criminal activity, they may close the account. If you have an ongoing investigation, this may hinder your ability to track the suspect.
- Use the legal contact information available from the SEARCH.org website, or, click the "ISP" button on the Internet Investigators Toolbar.
- Contact the company that is assigned the IP address in question and obtain records, with appropriate legal procedures. From their records, determine the identity of the person using the IP address at the date and time in question.

Tracing emails

Email is as ubiquitous as any of the IPs we have discussed. Other than the World Wide Web, this is one of the most used tools for communication. It is commonly employed for everything from personal communications to business use. Unfortunately, it is also a favorite tool for threats and harassment by criminals and stalkers. This section will explain the basic parts of an email and how to effectively identify the sender or identify the pieces of the email that can further the investigation through additional follow-up.

We previously discussed the protocol in Chapter 3 that routes email, the Simple Mail Transfer Protocol (SMTP). The email itself has several features that are unique and make identification possible. These features provide initial

clues which may not identify a specific person or sender without additional investigative steps. To start email addresses, have the standard familiar format of the username, the @ symbol, the domain name used by the user and the top level domain associated with the domain name. For example:

username@domain (e.g., todd@veresoftware.com)

The email we see in our email program generally shows only the sender, the receiver, and the subject line. As we discussed in Chapter 3, there is a significant amount of data in the unseen headers of the email that gives the investigator important information that can be useful in possibly establishing an email's sender's identity. We know that in general an email travels from a sender's computer to their mail service to recipient's mail service, where it resides on a mail server (computer that stores and delivers mail). Each next time the receiver logs into his or her account, the mail reader retrieves the message to his or PC/workstation. As the email travels through the Internet, from email server to email server, it gathers data from each processing server. Each of these servers gives the investigator an idea of how the email traveled from sender to receiver. In Figure 8.3, we have shown the process of the email traveling through the Internet.

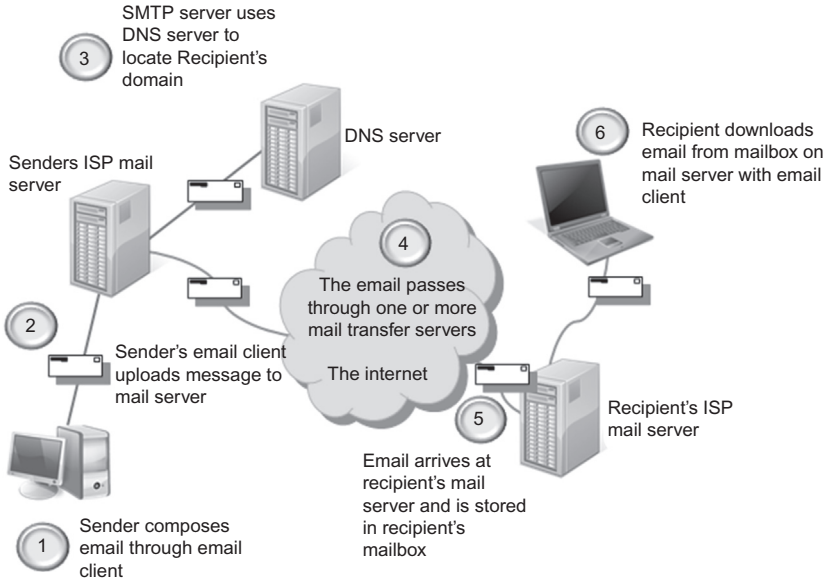

FIGURE 8.3

How email works.

Where is the evidence?

So if we are talking in general about where evidence could be, it could be in numerous places along that path (Figure 8.4). However, that does not mean a copy of the email will exist on each location when you attempt to locate it. Depending on the jurisdiction, records of the email transfer may not be required to be kept by government regulations. In the United States, there are no specific record retention requirements for tracking email. Each service provider sets its own standards for logging information. What we can generally identify are the copies of a previously sent email messages that may be stored at accessible locations. Those accessible locations include:

- The sender's device[1]
- The sender's mail server
- The recipient's mail server
- The recipient's device.

A record of the email transmission (date, time, source, and destination) can reside in these same locations. Accessing these records can be done through the sender's device or through a forensic examination of the device. Before

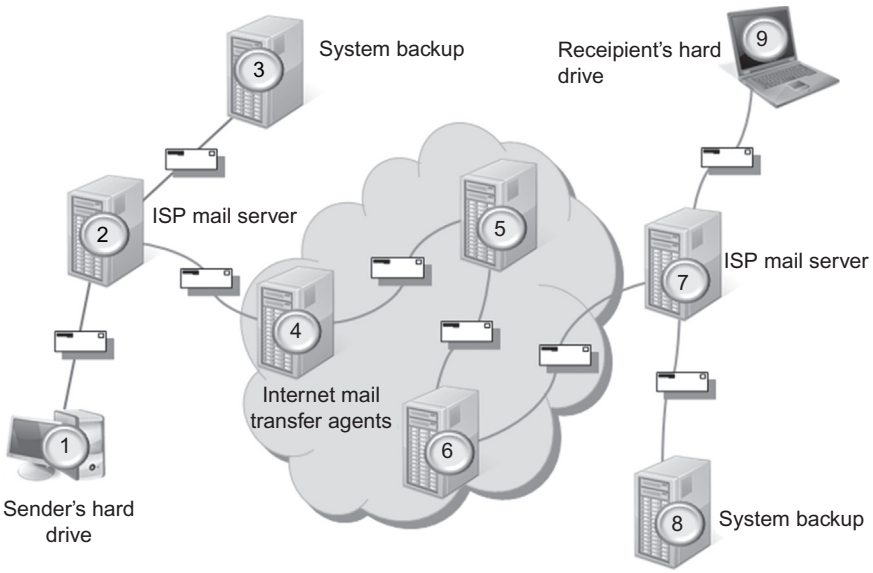

FIGURE 8.4

Where is the email evidence?

[1]Devices can be computers, tablets, or cell phones, or anything that can be used to send or receive email.

accessing data, be aware there are different legal requirements in play. Accessing data that resides on the sender's device requires consent or a traditional search warrant. However, in the United States, data that resides on a server requires compliance with the Stored Communications Act (SCA) (see Chapter 4). Of course, accessing any of the records requires the proper legal authority which can include consent, a subpoena, or search warrant. Additionally, depending on the laws in the investigator's country, other legal options for access may be available.

Viewing email headers

To determine the sender of an email, an investigator needs the email's header information. An email header is the information added to the beginning/top of the electronic message. Normally, email clients and web services only show an abbreviated form of the header. Email headers are created by the email servers that process the messages. Adding information depends on the email protocol used. Not every server adds detailed information to the header as it passes through the server. Viewing the email headers is different for each email program or service. In Chapter 4, we discussed using Spamcop from the Internet Investigators Toolbar to identify the specifics of accessing email headers for different email services and tools. From the Spamcop website, we can easily identify how to access full email headers to be reviewed for identifying information.

The information commonly displayed are the abbreviated headers. We normally see in an email:

From:
To:
CC:
Subject:
Date:

For the investigator, the identifying information is the "From" line which is the email address the message purportedly came from, the "To" line which is where the message was sent, and the "CC" line is where other email addresses receiving the message are included. Is this information enough to properly trace an email? The answer is it certainly no. There is more information which can be used to effectively identify email movement through the Internet.

The full header provides the investigator with significantly more data with which to determine the veracity of the email as well as its origin. What the full headers can help the investigator identify are:

- Who sent the email
- Which network it originated from
- Which email servers processed it

INVESTIGATIVE TIPS

Accessing Headers in Common Web Mail Services

Google Mail

1. Open the message you want to view the headers.
2. Click the down arrow next to the "Reply" link.
3. Select "Show Original" and a new window will open with the full headers.

Windows Live Mail

1. Right click on the message.
2. Select "View Source".
3. A new window with the full headers and HTML source of the email will open.

Yahoo! Mail

1. Click Actions dropdown.
2. Select "View Full Headers".
3. A new window with the full headers will open.

- Miscellaneous information:
  - Time stamps
  - Email client
  - Encoding information.

The investigator needs to also understand that not all the information in the header is useful to the investigation. Let's take a look at what the typical full email header can contain:

- The originator fields:
- *From:, Sender:, Reply-To*:
- Date:
- Received:
- X-Originating-IP:
- Message-ID:
- X-Mailer:
- X-MIMEOLE:

Headers are comprised of lines of information called header fields. Each field contains a field label, followed by a colon ":" and then the field body. The headers are "generally" layered bottom-to-top. For the investigator this means we start at the bottom of the full header and read up to determine how it traveled through the Internet mail services. The first field is on the bottom and subsequent fields added on top, in the order they are written by the mail server they were transferred through (Figures 8.2 and 8.3). In the full header, there are several header fields we can use to trace emails:

1. Sender's email address.
2. Email server information which includes the Message-ID. The SMTP relay information, which includes the sender's IP address or initial SMTP server's IP address.

3. Common in SMTP servers is the additional information not standard in the protocol. These fields are added to the header by the SMTP server and are unique to the server. They are easily identified as any field starting with an "X". In the SMTP standard, anything beginning with a "X" is nonstandard and has no direct translation in the standard.

A commonly used nonstandard field has been one called "X-Originating-IP". The "X-Originating-IP" has been used by SMTP servers to store the originating IP address of the email's sender. This field can identify the IP address assigned to the sender by their ISP for that session.

Another field of interest is the Message-ID. Every email sent through an SMTP server is assigned a unique ID by the originating SMTP email server. This Message-ID can identify the originating SMTP server from which the investigator can obtain logs (of course this is an issue of timeliness as the server may not retain the records for long periods of time). If the investigator provides this message-ID to the corresponding ISP, it can aid in locating the records needed to identify the sender. For the ISP it is easier, and usually faster, to search email server logs for the Message-ID then to find IP addresses associated with the email. The Message-IDs look very similar to email addresses, for example:

192809895-1238802958-cardhu_decombobulator_blackberry.rim.net-1937758735-@bxe1280.bisx.prod.on.blackberry

The information to the left of the "@" symbol is the unique identifier and the server it came through. The information to the right of the "@" identifies the domain to which the email server assigning the Message-ID belongs.

The Date Field in an email can come from different sources. The date and time can be from the sender's computer, or the date and time can be from the initial email server the message was sent through. These dates and times can possibly determine the sender's general location by time zone if the information comes from their system clock. However, this must be interpreted cautiously, because this depends on the email service used.

Time differences

We mentioned briefly earlier that strict reliance on dates and times stamps should be done at the investigator's peril. Knowing where the time stamp came from is sometimes difficult and should not be totally relied on as coming from the sender. The reason is the investigator will rarely have all the information required to know what email program was used to send the email and the SMTP server settings that passed the email on through the Internet. The sender could employ a "Send Later" feature to throw the receiver off and make them believe the email was written and sent at a time different than when it actually was composed.

Even Microsoft recognizes that differences in time stamps can occur within Outlook. On Office.com, they have the following reference about this fact:

How time stamps appear in messages:

NOTE: You might notice cases where the sent time is after the received time. This delay might be caused by a difference between the system clocks on the sender's computer and on your email server.

Header information translation

Every email header is different and has its own unique identification. In the following tables, we take a look at an email sent from a Yahoo email account to a Google (Gmail) account. We first have to login to and access the receiving Gmail account. Once we open the received email in Gmail, we click on the dropdown arrow on the right side of the email nest to the "reply" arrow. This opens up several options including "Show original". Selecting "Show original" opens the header in another window (Figure 8.5).

Table 8.2 has the complete header we extracted from the email sent to the test Gmail account. Table 8.3 provides a detailed explanation of the header information reflected in Table 8.2. The complete header has several areas of interest to the investigator. We can break the header into five areas of interest:

1. The servers the email passed through
2. Encrypted mail header
3. The traditional To, From, Subject, and Date lines
4. Mail transfer program information
5. Nonstandard information added by servers and email programs

Remember that the email servers stamp the "received" information from the bottom up in the header. In Table 8.4, we break out the raw data in Table 8.2

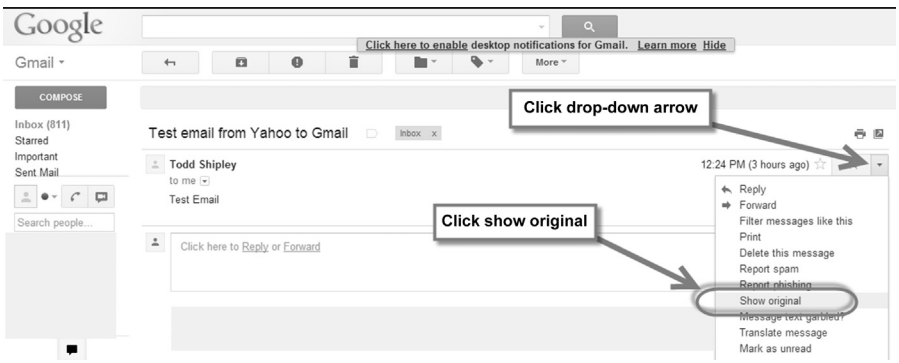

FIGURE 8.5

Gmail account accessing full headers.

Table 8.2 Example Header from Yahoo Email to Gmail

Delivered-To: testgmailaccount@gmail.com

Received: by 10.49.15.197 with SMTP id z5csp55241qec;
Sun, 24 Feb 2013 12:24:27 -0800 (PST)

X-Received: by 10.236.162.197 with SMTP id y45mr16233991yhk.110.1361737467542;
Sun, 24 Feb 2013 12:24:27 -0800 (PST)

Return-Path: <testyahooaccount@yahoo.com>

Received: from nm26.access.bullet.mail.mud.yahoo.com (nm26.access.bullet.mail.mud.yahoo.com. [66.94.237.91])
by mx.google.com with ESMTPS id a27si13288213yhn.132.2013.02.24.12.24.27
(version = TLSv1 cipher = RC4-SHA bits = 128/128);
Sun, 24 Feb 2013 12:24:27 -0800 (PST)

Received-SPF: neutral (google.com: 66.94.237.91 is neither permitted nor denied by best guess record for domain of testyahooaccount@yahoo.com) client-ip = 66.94.237.91;

Authentication-Results: mx.google.com;
spf = neutral (google.com: 66.94.237.91 is neither permitted nor denied by best guess record for domain of testyahooaccount@yahoo.com) smtp.
mail = testyahooaccount@yahoo.com;
dkim = pass header.i = @yahoo.com

Received: from [66.94.237.127] by nm26.access.bullet.mail.mud.yahoo.com with NNFMP; 24 Feb 2013 20:24:26 -0000

Received: from [66.94.237.121] by tm2.access.bullet.mail.mud.yahoo.com with NNFMP; 24 Feb 2013 20:24:26 -0000

Received: from [127.0.0.1] by omp1026.access.mail.mud.yahoo.com with NNFMP; 24 Feb 2013 20:24:26 -0000

X-Yahoo-Newman-Property: ymail-3

X-Yahoo-Newman-Id: 968415.26467.bm@omp1026.access.mail.mud.yahoo.com

Received: (qmail 55713 invoked by uid 60001); 24 Feb 2013 20:24:26 -0000

DKIM-Signature: v = 1; a = rsa-sha256; c = relaxed/relaxed; d = yahoo.com; s = s1024; t = 1361737466; bh = qwi0 + QrpLlhGpEVETzboOXvvDxVGRXmYMTrUSv0peL8 = ; h = X-YMail-OSG:Received:X-Rocket-MIMEInfo:X-Mailer:Message-ID:Date:From:Subject:To:MIME-Version:Content-Type; b = 13CKqrHzBlBA17dE7 + 2T/HS1QEk0sDAHBlO1NQ1FCNluDZYYsVFTktrzyHV/3/QSOeNnk8gLqofZj0 + MBzKzlAG + 4oPUKrYGwqsiF2ufhj/kRLdORZ + hF + j56lnPV + e1uLUnr4i2iS2Ei3ScK + yRtfKJivjbY76jI2hsdL9jLqk =

DomainKey-Signature:a = rsa-sha1; q = dns; c = nofws;
s = s1024; d = yahoo.com; h = X-YMail-OSG:Received:X-Rocket-MIMEInfo:X-Mailer:Message-ID:Date:From:Subject:To:MIME-Version:Content-Type;b = RiLBl0Box/DViNyFivNHcESpQunKLGEYtJUG0vhpW1F18nXcLSc4Y4oNmF/Ko4l0 + oxOnOeOQAHXa2Coz7HNC1RiNSklxkoMmDom6SXg/gKJtKaHrzEwRyyjkxQZmb3do + ePaObBJ4G50aS65j/DytTiotQbcTKnKslteE9HhGk = ;X-YMail-OSG: 7cqc6isVM1kJzx4ley5DeT1ZT.xzbruV5C.MlBV9T28FYZh
mmmqcaH_nyQ_a.QJW4Hom8M35yydPvDNwPXyjHDlRtTzyHepGAV8cBmlN.yX
ZsjUW9jHBTRlAyZBts52CF_RcL9Q_aOabKlQbc3y0jYQzNjexZXuVSdDkWnA
vH8go3GRcXdJM4U2HJaQEqSQbxXFYKHCksZ7uKrB4Gkx57a7LZTBsUkrp4pC

(*Continued*)

Table 8.2 (Continued)

SMWQho3fNlH5RtBbEAmppqMdcQhlJwUofuXGKFdqTaA_07p4.K7lcasK_yo6
93z6qCrlMVvvou6H7_3RW5DV5DGgsdQLpnZavRc.SYWrRbFmc1iW.4MkiREq
5GLkMNaYHxZHuo2FgWiVWMoUk51rf8BDtb2VqAdgLDebVfN.E_KzQBOk5CBK
EVWdq_S0aSmOu5.xJUQ15n4Uu.lD7A7Wywxg5ihR7Ejqrgau_zzJhMg--Received: from [209.78.21.148] by web180903.mail.ne1.yahoo.com via HTTP; Sun, 24 Feb 2013 12:24:26 PST

X-Rocket-MIMEInfo: 001.001,VGVzdCBFbWFpbAEwAQEBAQ--

X-Mailer: YahooMailClassic/15.1.2 YahooMailWebService/0.8.134.513

Message-ID: <1361737466.90408.YahooMailClassic@web180903.mail.ne1.yahoo.com>

Date: Sun, 24 Feb 2013 12:24:26 -0800 (PST)

From: Todd Shipley <testyahooaccount@yahoo.com>

Subject: Test email from Yahoo to Gmail

To: testgmailaccount@gmail.com

MIME-Version: 1.0

Content-Type: multipart/alternative; boundary = "-1576899772-1434694979-1361737466 = :90408"

and provide the path the message took through various SMTP servers (Table 8.5). One can see that the first documented record of our email example moving through an email server is by a Yahoo server in line #1. Of particular note is that the sender's IP address 209.78.21.148 in line #1 is correctly identified and belongs to the ISP used by the sender to log into their online email account. Escalating through the hops the email paths shown in numbers 2–5, Yahoo hands off the message amongst its own servers and in hop #6 passes the email off to Google. In the last hop #7, Google passes the email off to the user's account. Looking at the time stamps this all occurs in a matter of seconds. In that short period of time, seven servers touched the email, passing it on to the recipient. Note that the Yahoo servers are using UTC time (old Greenwich Mean Time) to stamp the email; however, Google translates the time into the local Pacific Standard Time. When the user looks at the email at the receiving or sending end, their email program translates the time into the local time zone. Table 8.3 breaks down the additional elements found in the header.

Another email header

If we look at another email header, this time one sent through Yahoo to Gmail, but via the user's desktop application Microsoft Outlook, we see similar actions through the Mail Transfer Agents (MTAs) (Table 8.6).

Table 8.3 Email Header Explanation from Yahoo to Gmail

Header Name	Header Value	Explanation
Delivered-To	testgmailaccount@gmail.com	Account email sent to
X-Received	by 10.236.162.197 with SMTP id y45mr16233991yhk.110.1361737467542; Sun, 24 Feb 2013 12:24:27 -0800 (PST)	Server in Google Mail system that received the email
Return-Path	<testyahooaccount@yahoo.com>	Email address of sender
Received-SPF	neutral (google.com: 66.94.237.91 is neither permitted nor denied by best guess record for domain of testyahooaccount@yahoo.com) client-ip = 66.94.237.91;	Refers to Sender Policy Framework (SPF), an email validation system to prevent spam by attempting to verify sender IP (Table 8.4)
Authentication-Results	mx.google.com; spf = neutral (google.com: 66.94.237.91 is neither permitted nor denied by best guess record for domain of testyahooaccount@yahoo.com) smtp.mail = testyahooaccount@yahoo.com; dkim = pass header.i = @yahoo.com	Email server checked DKIM header and correctly identified sender's email service as valid
X-Yahoo-Newman-Property	ymail-3	Yahoo mail server version
X-Yahoo-Newman-Id	968415.26467.bm@omp1026.access.mail.mud.yahoo.com	Yahoo mail assigned ID number for this email
DKIM-Signature	v = 1; a = rsa-sha256; c = relaxed/relaxed; d = yahoo.com; s = s1024; t = 1361737466; bh = qwi0 + QrpLlhGpEVETzboOXvvDxVGRXm YMTrUSv0peL8 = ; h = X-YMail-OSG:Received: X-Rocket-MIMEInfo:X-Mailer:MessageID:Date:From: Subject:To: MIME-Version:ContentType;b = 13CKqrHzBlBA17dE7 + 2T/HS1QEk0sDAHBlO1NQ1FCNluDZYYsVFTktrzyHV/3/ QSOeNnk8gLqofZj0 + MBzKzlAG + 4oPUKrYGwqsiF2ufhj/ kRLdORZ + hF + j56lnPV + e1uLUnr4i2iS2Ei3ScK + yRtfKJivjbY76jl2hsdL9jLqk =	Encrypted DKIM header
X-YMail-OSG	7cqc6isVM1kJzx4ley5DeT1ZT.xzbruV5C.MlBV9T28FYZh mmmqcaH_nyQ_a. QJW4Hom8M35yydPvDNwPXyjHDlRtTzyHepGAV8cBmlN. yXZsjUW9jHBTRlAyZBts52CF_RcL9Q_aOabKlQbc	Unidentified Yahoo YMail function

(*Continued*)

Table 8.3 (Continued)

Header Name	Header Value	Explanation
	3y0jYQzNjexZXuVSdDkWnAvH8go3GRcXdJM4U2HJaQEqSQbxXFYKHCksZ7uKr B4Gkx57a7LZTBsUkrp4pCSMWQho3fNlH5RtBbEAmppqMdcQhlJwUofuXGKFdq TaA_07p4.K7IcasK_yo693z6qCrlMVvvou6H7_3RW5DV5DGgsdQLpnZavRc. SYWrRbFmc1iW.4MkiREq5GLkMNaYHxZHuo2FgWiVWMoUk51rf 8BDtb2VqAdgLDebVfN.E_KzQBOk5CBKEVWdq_S0aSmOu5.xJUQ15n4Uu. lD7A7Wywxg5ihR7Ejqrgau_zzJhMg--	
X-Rocket-MIMEInfo	001.001,VGVzdCBFbWFpbAEwAQEBAQ--	Explanation Unknown
X-Mailer	YahooMailClassic/15.1.2 YahooMailWebService/0.8.134.513	Email program used to send email; in this case, Yahoo's classic mail service
Message-ID	<1361737466.90408.YahooMailClassic@web180903.mail.ne1.yahoo.com>	Message-ID added by Yahoo
Date	Sun, 24 Feb 2013 12:24:26 -0800 (PST)	Date of the email
From	Todd Shipley <testyahooaccount@yahoo.com>	Sender's email address
Subject	Test email from Yahoo to Gmail	Subject line of the email
To	testgmailaccount@gmail.com	Recipient's email address
MIME-Version	1.0	Multipurpose Internet Mail Extensions (MIME) version
Content-Type	multipart/alternative; boundary = "-1576899772-1434694979-1361737466 = :90408"	Content type of email which is used by the email program to know how to understand and display the email

Table 8.4 Path Email Took Through Various SMTP Servers

Hop	From	Through Which Server	With What Protocol	Time in UTC
7		10.49.15.197	SMTP	2/24/2013 12:24:27 -0800 (PST)
6	nm26.access.bullet.mail.mud.yahoo.com 66.94.237.91	mx.google.com	ESMTPS[a]	2/24/2013 12:24:27 -0800 (PST)
5	66.94.237.127	nm26.access.bullet.mail.mud.yahoo.com	NNFMP[b]	2/24/2013 20:24:26 -0000
4	66.94.237.121	tm2.access.bullet.mail.mud.yahoo.com	NNFMP	2/24/2013 20:24:26 -0000
3	127.0.0.1	omp1026.access.mail.mud.yahoo.com	NNFMP	2/24/2013 20:24:26 -0000
2		qmail 55713 invoked by uid 60001		2/24/2013 20:24:26 -0000
1	209.78.21.148	web180903.mail.ne1.yahoo.com		2/24/2013 12:24:26 PST

[a]ESMTPS refers to the encryption layers used in the email. See RFC 3848:ESMTP and LMTP Transmission Types http://rfc-ref.org/RFC-TEXTS/3848/chapter1.html#d4e439556.
[b]NNFMP according to several Internet resources stands for "Newman No-Frills Mail Protocol". However, nothing specific from Yahoo can be found that supports that. Yahoo also does not publish any material on its internal handling of email.

Table 8.5 Received-SPF Header Explanation

Received-SPF: pass	A permitted sender
Received-SPF: fail	Is not designated as permitted sender
Received-SPF: softfail	Is not designated as permitted sender
Received-SPF: neutral	Is neither permitted nor denied
Received-SPF: none	Not designate permitted sender
Received-SPF: permerror -extension:foo	Uses mechanism not recognized by this client
Received-SPF: temperror	Error in processing during lookup

Table 8.6 Example Header from Yahoo Email to Gmail Using Outlook

Delivered-To: testgmailaccount@gmail.com

Received: by 10.49.15.197 with SMTP id z5csp127114qec;
Mon, 18 Feb 2013 18:50:36 -0800 (PST)

X-Received: by 10.66.52.79 with SMTP id r15mr41491157pao.46.1361242236401;
Mon, 18 Feb 2013 18:50:36 -0800 (PST)

Return-Path: <testyahooaccount@yahoo.com>

Received: from nm6.access.bullet.mail.sp2.yahoo.com (nm6.access.bullet.mail.sp2.yahoo.com. [98.139.44.133])
by mx.google.com with ESMTPS id o3si22639630paz.263.2013.02.18.18.50.35
(version = TLSv1 cipher = RC4-SHA bits = 128/128);
Mon, 18 Feb 2013 18:50:36 -0800 (PST)

Received-SPF: neutral (google.com: 98.139.44.133 is neither permitted nor denied by best guess record for domain of testyahooaccount@yahoo.com) client-ip = 98.139.44.133;Authentication-Results: mx.google.com;
spf = neutral (google.com: 98.139.44.133 is neither permitted nor denied by best guess record for domain of testyahooaccount@yahoo.com) smtp.mail = testyahooaccount@yahoo.com;
dkim = pass header.i = @att.net

Received: from [98.139.44.96] by nm6.access.bullet.mail.sp2.yahoo.com with NNFMP; 19 Feb 2013 02:50:35 -0000

Received: from [67.195.22.118] by tm1.access.bullet.mail.sp2.yahoo.com with NNFMP; 19 Feb 2013 02:50:35 -0000

Received: from [127.0.0.1] by smtp113.sbc.mail.gq1.yahoo.com with NNFMP; 19 Feb 2013 02:50:35 -0000

DKIM-Signature: v = 1; a = rsa-sha256; c = relaxed/relaxed; d = att.net; s = s1024; t = 1361242235; bh = zDR8VzuSnPALPI2Oe0w4idEjFWbQmVNUfwUuop1dpk0 = ; h = X-Yahoo-Newman-Id:X-Yahoo-Newman-Property:X-YMail-OSG:X-Yahoo-SMTP:Received:From:To:Subject:Date:Message-ID:MIME-Version:Content-Type:X-Mailer:Thread-Index:Content-Language; b = zJ6lwoUheNqzLrPKXzAzh25v/6hiSU5MQSoB5MRNBOatvsCJEYRFMegqEEXMM8TxQmhEQp/BvRBTykTjZ + aVgVcZyZBRJ9owG/hsRXmOl9jGlc + 1VOqDP0rQkpk/TruVlkp5i4LQLlXcwMxzm6VD + QDekG3CkS3uk4Jua3LrSHQ =

X-Yahoo-Newman-Id: 739883.27524.bm@smtp113.sbc.mail.gq1.yahoo.com

X-Yahoo-Newman-Property: ymail-3

X-YMail-OSG: JLThjqoVM1lOm4wlt7jk.KDJFl0WnQlXguxMhWNboTRHyEQ
1J8yrK68QHDPUdtpDaJ8rhi_6Lm6RiT8qZmyN5u0LxSobBgQLCmOXpsuG.VW
H05DsSSQTMF6vJmQA5DoPhvKw0oOyUc7h9f18rDo5BESykTCdd2IpRCquoRx
rDX9h16_fggb9okkodkSMhaHpLOTOXgF0t9wQ_FAnA8qXLh3RBRkjVnAvK1r
O0pU_GxpX9tJuaAolBehXj3C2bVVMB0t8sZla08felznFdrmHJiSHq3eWLlp
_jbHWtNnspUThlEdggEnWyz1se6yCfN0hxuDwGjcvx_CeZPAaoacLwBkMmcP
K9qxZPG4xQWWZthxd7RJFfQ2KgjBmtj3LOD4cEhsVi35pnaNOFHAWwmJ5p2R
S.tg0zT3aZZgmMR_DxLki9.oC9FWy9Fhr6A--

X-Yahoo-SMTP: epBFhb6swBDqEduYvn.LxJxG.wQ.d6_TLl6Cmny3

Received: from Laptop testyahooaccount(toddshipley@209.78.21.184 with login)
by smtp113.sbc.mail.gq1.yahoo.com with SMTP; 18 Feb 2013 18:50:35 -0800 PST

(*Continued*)

Table 8.6 (Continued)

From: "ATT" <testyahooaccount@yahoo.com>
To: "Todd Shipley" <testgmailaccount@gmail.com>
Subject: Yahoo to Google Email
Date: Mon, 18 Feb 2013 18:50:38 -0800
Message-ID: <002d01ce0e4b$e6724e70$b356eb50$@att.net>
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary = "---- = _NextPart_000_002E_01CE0E08.D854B3C0"
X-Mailer: Microsoft Outlook 14.0
Thread-Index: Ac4OS9/suTp1w2JJS/Krzk1m1OaP3w = =
Content-Language: en-us
X-Antivirus: avast! (VPS 130218-0, 2/18/2013), Inbound message
X-Antivirus-Status: Clean

INVESTIGATIVE TIPS

Why a Server Hop Matters

When investigating email headers, the investigator identifies various MTAs that handle the email and pass it to the next server. Each of these is a potential source of information and evidence of the email's movement through the Internet. However, the evidence may not reside there long. Additionally, the evidence in the hops indicates something useful for possibly fulfilling the statutory requirements of some crimes. For instance, some crimes, particularly federal statutes, need an interstate nexus. A Threatening Interstate Communications, 18 U.S.C. § 875 violation requires that the communication crossed state lines. Identifying each of the server IP addresses and their associated owners may go a long way to establishing such legal elements.

In Table 8.8, we can see that the first record of anything through our email servers is by Yahoo in line #1. What is different in this example is the sender's IP address is correctly identified as well as the name of the computer sending, which is "Laptop". The name of the computer used to prepare the example as given in Tables 8.6 and 8.7 is verified by the system information page from that computer as shown in Figure 8.6. Looking at Table 8.8, we can escalate through the hops the email paths show in numbers 2–4. It shows Yahoo passing the email amongst its own servers, and in hop #5, Yahoo finally passes the email off to Google. In the last hop #6, Google passes the email off to the user's account. Looking at the time stamps this all occurs in a matter of seconds. In that short period of time, six servers touched the email, passing it on to the recipient. The investigator should be aware that the servers either stamp the times with the local time of the server or use UTC time (old Greenwich Mean Time) as the time used to stamp the

Table 8.7 Email Header Explanation from Yahoo to Gmail Through Outlook

Header Name	Header Value	Explanation
Delivered-To	testgmailaccount@gmail.com	Account email sent to
Received	by 10.49.15.197 with SMTP id z5csp127114qec; Mon, 18 Feb 2013 18:50:36 -0800 (PST)	Google email server passing email
X-Received	by 10.66.52.79 with SMTP id r15mr41491157pao.46.1361242236401; Mon, 18 Feb 2013 18:50:36 -0800 (PST)	Server in Google mail system that received the email
Return-Path	<testyahooaccount@yahoo.com>	Email address of sender
Received	from nm6.access.bullet.mail.sp2.yahoo.com (nm6.access.bullet.mail.sp2.yahoo.com. [98.139.44.133]) by mx.google.com with ESMTPS id o3si22639630paz.263.2013.02.18.18.50.35 (version = TLSv1 cipher = RC4-SHA bits = 128/128); Mon, 18 Feb 2013 18:50:36 -0800 (PST)	Yahoo email server passing email
Received-SPF	neutral (google.com: 98.139.44.133 is neither permitted nor denied by best guess record for domain of testyahooaccount@yahoo.com) client-ip = 98.139.44.133;Authentication-Results: mx.google.com; spf = neutral (google.com: 98.139.44.133 is neither permitted nor denied by best guess record for domain of testyahooaccount@yahoo.com) smtp. mail = testyahooaccount@yahoo.com; dkim = pass header.i = @att.net	Refers to SPF, an email validation system, to prevent spam by attempting to verify sender IP (see Table 8.5)
Received	from [98.139.44.96] by nm6.access.bullet.mail.sp2.yahoo.com with NNFMP; 19 Feb 2013 02:50:35 -0000	Yahoo email server passing email
Received	from [67.195.22.118] by tm1.access.bullet.mail.sp2.yahoo.com with NNFMP; 19 Feb 2013 02:50:35 -0000	Yahoo email server passing email
Received	from [127.0.0.1] by smtp113.sbc.mail.gq1.yahoo.com with NNFMP; 19 Feb 2013 02:50:35 -0000	Yahoo email server passing email
DKIM-Signature		

	v = 1; a = rsa-sha256; c = relaxed/relaxed; d = att.net; s = s1024; t = 1361242235; h = zDR8 VzuSnPALPl2Oe0w4idEjFWb QmVNUfwUuop1dpk0 = ; h = X-Yahoo-Newman-Id:X-Yahoo-Newman-Property:X-YMail-OSG:X-Yahoo- MTP:Received: From:To:Subject:Date: Message-ID:MIME-Version:Content-Type:X-Mailer:Thread-Index:Content-Language; b = zJ6lwoUheNqzLrPKXzAzh25v/6hiSU5MQSoB5MRNBOatvsCJEYRFMe gqEEXMM8TxQmhEQp/BvRBTykTjZ + aVgVcZyZBRJ9owG/hsRXmOl9jGIc + 1VOqDP0rQkpk/TruVlkp5i4LQLIXcwMxzm6VD + QDekG3CkS3uk4Jua3LrSHQ =	Encrypted DKIM header
X-Yahoo-Newman-Id	739883.27524.bm@smtp113.sbc.mail.gq1.yahoo.com	Yahoo mail assigned ID number for this email
X-Yahoo-Newman-Property	ymail-3	Yahoo mail server version
X-YMail-OSG	JLThjqoVM1lOm4wlt7jk.KDJFl0WnQlXguxMhWNboTRHyEQ1J8yrK68QHDPUdtpDaJ8rhi_ 6Lm6RiT8qZmyN5u0LxSobBgQLCmOXpsuG.VWH05DsSSQTMF6vJmQA5DoPhvKw 0oOyUc7h9f18rDo5BESykTCdd2IpRCquoRxrDX9h16_fggb9okkodkSMhaHpLOTOX gF0t9wQ_FAnA8qXLh3RBRkjVnAvK1rO0pU_GxpX9tJuaAolBehXj3C2bVVMB0t8 sZla08felznFdrmHJiSHq3eWLlp_jbHWtNnspUThlEdggEnWyz1se6yCfN0hxuDwGjcvx _CeZPAaoacLwBkMmcPK9qxZPG4xQWWZthxd7RJFfQ2KgjBmtj3LOD 4cEhsVi35pnaNOFHAWwmJ5p2RS.tg0zT3aZZgmMR_DxLki9.oC9FW y9Fhr6A--	Unidentified Yahoo YMail function
X-Yahoo-SMTP	epBFhb6swBDqEduYvn.LxJxG.wQ.d6_TLl6Cmny3	Unidentified Yahoo SMTP function
Received	from Laptop testyahooaccount(toddshipley@209.78.21.184 with login) by smtp113.sbc.mail.gq1.yahoo.com with SMTP; 18 Feb 2013 18:50:35 -0800 PST	Yahoo email server receiving the email from the login IP address of 209.78.21.184 and the device name used to send the email “Laptop”
From	“ATT” <testyahooaccount@yahoo.com>	Sender’s email address
To	“Todd Shipley” <testgmailaccount@gmail.com>	

(*Continued*)

Table 8.7 (Continued)

Header Name	Header Value	Explanation
		Recipient's email address
Subject	Yahoo to Google Email	Subject line of the email
Date	Mon, 18 Feb 2013 18:50:38 -0800	Date of the email
Message-ID	<002d01ce0e4b$e6724e70$b356eb50$@att.net>	Message ID added by AT&T (Yahoo)
MIME-Version	1.0	MIME version
Content-Type	multipart/alternative; boundary = "---- = _NextPart_000_002E_01CE0E08.D854B3C0"	Content type of email which is used by the email program to know how to understand and display the email
X-Mailer	Microsoft Outlook 14.0	Identifies email program used to receive the email at the user's desktop
Thread-Index	Ac4OS9/suTp1w2JJS/Krzk1m1OaP3w = =	Microsoft Outlook Message-ID
Content-Language	en-us	Language used in email
X-Antivirus	avast! (VPS 130218-0, 2/18/2013), Inbound message	Antivirus program Avast used to scan inbound messages
X-Antivirus-Status	Clean	Antivirus program declaration that email is "Clean" of any malware

Table 8.8 Path Email Took Through Various SMTP Servers

Hop	From	Through Which Server	With What Protocol	Time in UTC
6		10.49.15.197	SMTP	2/19/2013 2:50:36 AM
5	nm6.access.bullet.mail.sp2.yahoo.com 98.139.44.133	mx.google.com	ESMTPS	2/19/2013 2:50:36 AM
4	98.139.44.96	nm6.access.bullet.mail.sp2.yahoo.com	NNFMP	2/19/2013 2:50:35 AM
3	67.195.22.118	tm1.access.bullet.mail.sp2.yahoo.com	NNFMP	2/19/2013 2:50:35 AM
2	127.0.0.1	smtp113.sbc.mail.gq1.yahoo.com	NNFMP	2/19/2013 2:50:35 AM
1	Laptop 209.78.21.184	smtp113.sbc.mail.gq1.yahoo.com	Login	2/19/2013 2:50:35 AM

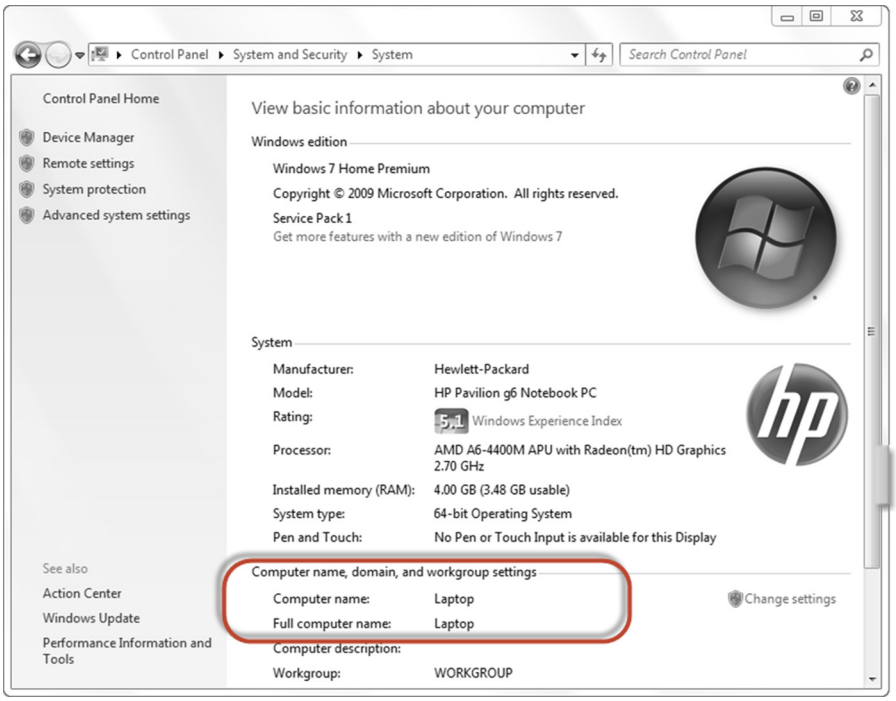

FIGURE 8.6

System page in Windows 7 showing computer name.

Table 8.9 Standard Internal Header Information from an Microsoft Exchange Server

Microsoft Mail Internet Headers Version 2.0

Received: from exchfe02.ad.xxx ([10.10.xxx.xx]) by exch10.ad.xxxi with Microsoft SMTPSVC(6.0.3790.3959);

Fri, 22 Nov 2011 10:29:13 -0800Received: from KMBT59C636.ad.agi ([10.10.x.xx]) by exchfe02.ad.xxx with Microsoft SMTPSVC(6.0.3790.3959);

Fri, 22 Nov 2011 10:29:13 -0800

To:bbxxx@xxxx.com Subject:Message Sender:hxxx@xxxx.com From:hxxx@xxxx.com

Reply- To:hxxx@xxxx.com X-Mailer:KONICA C550 Date: Fri, 22 Nov 2011 10:29:13 -0800Message-Id:<4 7 A3043 8.50C.00206B59C636.hxxx@xxxx.com> MIME-Version: 1.0

Content-Type:multipartlmixed; boundary = "KONICA_MINOLTA_Internet_Fax_Boundary"

Content-Transfer-Encoding:7 bit Return-Path: hxxx@ xxxx.com

email. When the user looks at the email at the receiving or sending end, their email program will generally translate the time into the local time zone, that is, Mon, 18 Feb 2013 18:50:38 -0800 (-0800 is 8 h after UTC or Pacific Standard Time).

A Microsoft Outlook header translation through an exchange server

Not all headers we may need to look at go through the Internet. Email headers are found internally in popular email networks such as Microsoft Exchange servers. If we take a look at the header fields from a common Microsoft Exchange Outlook email, we can identify other interesting information about the email. Table 8.9 reflects a unique situation. The email chain starts from a printer. A document is scanned on the printer that is attached to the systems network (and has an assigned email address on the network), and gets processed by the Microsoft Exchange server. As a result, this email contains a separate header based on the IP from RFC 5322 Internet Message Format. This header was produced by the Konica printer, which sent the email. Table 8.10 lists the definition of the Outlook header information as defined by Microsoft from their website. Ultimately, the message ends up in the user's mailbox that it was addressed to and where it is transferred to the local storage of the user. Our header is found in the Microsoft Outlook Personal Storage File (PST) on the user's computer. Table 8.11 provides a listing of standard header information translation for definitions found in RFC's 5321, 5322, and 2045.

Multipurpose Internet Mail Extensions

We previously discussed the mail transfer program protocol SMTP in Chapter 3. It is the standard protocol for sending email through the Internet. However, it does have limitations. The largest limitations are due to the size of the email that

Table 8.10 Outlook Header Information Translation

Conversation Topic:	The topic of the conversation thread of the Outlook item
Sender Name:	The display name of the sender for the Outlook item
Received By:	The display name of the true recipient for the mail message
Delivery Time:	No definition found
Creation Time:	The creation time for the Outlook item
Modification Time:	A *Date* specifying the date and time that the Outlook item was last modified—Read-only
Submit Time:	No definition found
Importance:	The relative importance level for the Outlook item
Sensitivity:	Indicates the sensitivity for the Outlook item
Flags:	A mail item with a flag marked through the user interface
Size:	Indicates the size (in bytes) of the Outlook item

Table 8.11 Translation of Standard Header Information

Standard Header Information Translation	Field Explanation from RFC 5322 and 2045
Microsoft Mail Internet Headers Version 2.0	This header is added by Microsoft Outlook.
Received: from exchfe02.ad.xxxi ([10.10.xxx.xx]) by exch10.ad.xxxi with Microsoft SMTPSVC(6.0.3790.3959); Fri, 22 Nov 2011 10:29:13 -0800	The "Received:" field contains a (possibly empty) list of tokens followed by a semicolon and a date-time specification. Each token must be a word, angle-addr, addr-spec, or a domain. Further restrictions are applied to the syntax of the trace fields by specifications that provide for their use, such as [RFC5321].
Received: from KMBT59C636.ad.xxx ([10.10.x.xx]) by exchfe02.ad.xxx with Microsoft SMTPSVC(6.0.3790.3959); Fri, 1 Feb 2010 11:40:23 -0800	When the SMTP server accepts a message either for relaying or forfinal delivery, it inserts a trace record (also referred to interchangeably as a "time stamp line" or "Received" line) at the topof the mail data. This trace record indicates the identity of the host that sent the message, the identity of the host that received the message (and is inserting this time stamp), and the date and time the message was received.
To:bbxxxxx@xxxx.com	The "To:" field contains the address(es) of the primary recipient(s)of the message.
Subject:Message	The "Subject:" field is the most common and contains a short string identifying the topic of the message.

(*Continued*)

Table 8.11 (Continued)

Standard Header Information Translation	Field Explanation from RFC 5322 and 2045
Sender:hxxx@xxxx.com	The "Sender:" field specifies the mailbox of the agent responsible for the actual transmission of the message.
From:hxxx@xxxx.com	The "From:" field specifies the author(s) of the message, that is, the mailbox(es) of the person(s) or system(s) responsible for the writing of the message.
Reply-To: hxxx@xxxx.com	When the "Reply-To:" field is present, it indicates the address(es) to which the author of the message suggests that replies be sent.
X-Mailer: KONICA C550	Implementors may, if necessary, define private Content-Transfer-Encoding values, but must use an x-token, which is a name prefixed by "X-", to indicate its nonstandard status, for example, "Content-Transfer-Encoding: x-my-new-encoding".
Date: Fri, 22 Nov 2011 10:29:13 -0800	The origination date specifies the date and time at which the creator of the message indicated that the message was complete and ready to enter the mail delivery system.
Message-Id: <4 7 A3043 8.50C.00206B59C636.hxxx@xxxx.com>	The "Message-ID:" field provides a unique message identifier that refers to a particular version of a particular message. The uniqueness of the message identifier is guaranteed by the host that generates it (see below). This message identifier is intended to be machine readable and not necessarily meaningful to humans. A message identifier pertains to exactly one version of a particular message; subsequent revisions to the message each receive new message identifiers.
MIME-Version: 1.0	A MIME-Version header field, which uses a version number to declare a message to be conformant with MIME and allows mail processing agents to distinguish between such messages and those generated by older or nonconformant software, which are presumed to lack such a field.
Content-Type: multipartlmixed; boundary = "KONICA_MINOLTA_ Internet_Fax_Boundary"	A Content-Type header field, generalized from RFC 1049, which can be used to specify the media type and subtype of data in the body of a message and to fully specify the native representation (canonical form) of such data.

(*Continued*)

Table 8.11 (Continued)

Standard Header Information Translation	Field Explanation from RFC 5322 and 2045
Content-Transfer-Encoding: 7 bit	A Content-Transfer-Encoding header field, which can be used to specify both the encoding transformation that was applied to the body and the domain of the result. Encoding transformations other than the identity transformation are usually applied to data in order to allow it to pass through mail transport mechanisms which may have data or character set limitations.
Return-Path: hxxx@xxxx.com	The "Return-Path:" header field contains a pair of angle brackets that enclose an optional addr-spec.

can be sent and its inability to deal with non-ASCII characters. This has been overcome with an additional set of protocols that describe how to send larger messages and attachments. This protocol is commonly referred to as MIME. MIME stands for Multipurpose Internet Mail Extensions. MIME allows the inclusion of non-ASCII characters and non-English languages, multiple fonts, and of course multimedia objects such as images, audio, and video (Brodkin, 2011).

MIME has become the standard protocol for allowing the addition of media as in pictures and video into an email. How does this occur you might ask? Well, the protocol uses an encoding method known as base64 to convert the nontext items, binary data, such as videos, or pictures into text. This then allows the standard SMTP to more easily transmit the data. Upon receipt, your email program unencodes the base64 data into a file we can understand again. MIME uses the Content-Type field to help it determine if the data needs to be encoded. Table 8.12 provides an explanation for common MIME Content-Types (Figure 8.7).

Looking at little X

We already mentioned that header entries beginning with an X are nonstandard and applied by a user's email program or an email server or MTA that it passes through. The X lines in the header are intended to provide additional information to aid in the sending of the email through various servers. To understand some of the X lines in an email header, we have put together a short list in Table 8.13 of commonly encountered X lines you might see when tracing an email header. Many of these can be found in various RFCs including RFC 2076.

Table 8.12 Content-Type Explanation

Content-Type	Description
application/octet-stream	Used where the message is an unknown type and contains any kind of data as bytes
application/xml	Used for application-specific xml data
x-type	Used for nonstandard content type
image/jpeg	Used for images
multipart/related	Used for multiple related parts in a message
multipart/signed	Used for multiple related parts in a message including signature
multipart/mixed	Used for multiple independent parts in a message

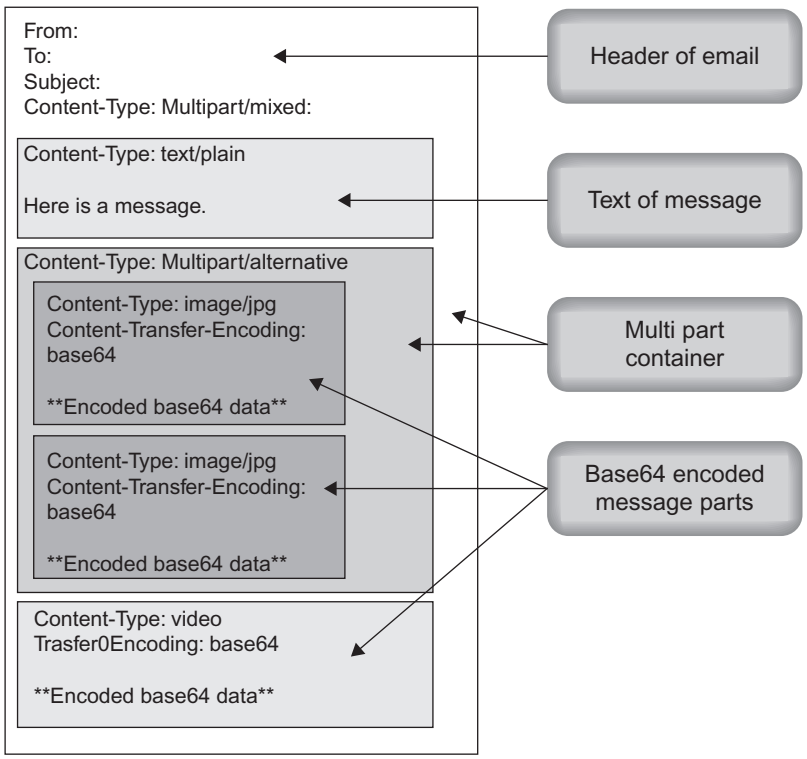

FIGURE 8.7

MIME email analysis.

Table 8.13 Common X Header Explanations

Header	Explanation
X-Apparently-To	Intended receiver of the email
X-Antivirus	Antivirus tool used to check email
X-Antivirus-Status	Status of the email according to the antivirus tool as Clean or Spam
X-Complaints-To	Where to direct your complaints you have about an email you received
X-Confirm-Reading-To	Create an automatic response for read messages
X-Errors-To	The address to send an email to for any errors encountered
X-Ymail-ISG	Yahoo Incoming Spam Guard
X-Mailer	Program used to send the email
X-Notifications	Explanation Unknown
X-Originating-IP	IP address of ISP used by sender
X-PMFLAGS	Additional information used with Pegasus Mail
X-Priority	Priority of email being sent
X-Received	MTA receiving email (does not necessarily mean the last server in the line
X-Sender	Additional information about the sender of the email
X-Spam-zzz	Where zzz is any number of different spam tags relating to the Spam filter on the email server. Some of these include Checker-Version, Level, Report, and Status
X-UIDL	Used with emails distributed over POP
X-Yahoo-Newman-Property	Explanation Unknown
X-Yahoo-Newman-Id	Yahoo internal mail transfer protocol ID
X-Ymail-OSG	Yahoo Outgoing Spam Guard

THINGS TO KNOW

Sender IP information in an email header is often controlled by the MTAs first processing the email. Historically to prevent spam, these MTAs would pass through the sender's IP address. This assisted the receivers of an email trace back the email to the sender. This was commonly added as the header X-Originating-IP. Changes to the way some of the large ISP companies process email have started to appear. Google no longer adds the sender's IP address in their headers. As of mid-December 2012, Microsoft has started adding a new line to its headers titled X-EIP and has removed the X-Originating header. The X-EIP header appears to be an encoded IP address, but to date has not been translated. Controlling spam has become a significant issue and one that has affected the method by which the investigator traces an email.

INVESTIGATIVE TIPS

Email from Other Sources

Email is such a prolific tool that it is available not just on computers but also on cell phones, gaming devices, tablet devices, and social media sites. Headers sent from these devices can also provide the investigator with specific header information about the sender and the location or device sent from. This can provide another potential source of digital evidence for later collection and review by digital forensic investigators.

Android Phone Email:

Email sent from an Android phone can be potentially identified through the email headers through the Content-Type header. The Content-Type header may have "com.andriod.email" in the text. The Message-ID may contain "email.android.com". The first "Received:" line will most likely contain an IP address assigned to the cell phone's service provider.

iPhone Email:

Email sent from an iPhone can be potentially identified through the email headers through the Content-Type header. The Content-Type header may have "text/plain; charset = us-ascii". An "X" header X-Mailer may contain the text "iPhone Mail". The first "Received:" line will most likely contain an IP address assigned to the cell phone's service provider.

Nook Tablet devices:

Email sent from a Nook Tablet can potentially be identified through the email headers Message-ID which may contain "email.android.com".

Facebook email:

Emails sent from a Facebook account may be identified from the account sender which will be the Facebook account followed by @facebook.com. The first received line may also include the text "helo = www.facebook.com" and the DKIM header may have a reference to facebook.com also. There may possibly be an "X-Originating-IP" header containing an IP belonging to facebook.com.

Faking an email and hiding its sender

So we have looked at the real header, but what can be done to hide the real sender of an email. There are several things the sender can do to hide their location from the receiver. A few of those methods include:

1. Anonymous remailers/ open relays: SMTP mail servers on the Internet that allow anyone on the Internet to forward email. These have become increasingly difficult to find because most of them have been closed due to their misuse by spammers.
2. Email on anonymous networks: Anonymous email sent through the Tor or I2P networks. Tor and I2P both offer access to email through their anonymized networks (www.torproject.org and www.i2p2.de).
3. Forging email headers: Sender uses controlled SMTP server to send email with altered email.
4. Anonymous email accounts: Email accounts with no requirement for inputting real identifying information about the sender. Most of the larger email services including Google, Yahoo, and Microsoft Live allow the suspect or the investigator to create fictious accounts.

5. Fake mail generators/disposable and temporary accounts: Web-based services that let the sender input any return email address. Searching the Internet will find numerous sites that provide this service. Most of these advertise they keep no records of the IP addresses connecting with the email server as a way to assure their customer's privacy.

Each of these methods adds to the difficulty the investigator will have in identifying the IP address of the suspect or possibly make it entirely impossible to trace. Identifying the actual IP address may include legal service on multiple IP addresses or undercover contact with the target.

Collecting email from a web-based system

Email collection from a web-based service can be an effective evidence collection technique for the investigator. Both criminal investigators and civil investigators can properly collect the web-based email in support of their investigations. Examples of collection possibilities include documentation of a victim's threatening emails or a civil investigator conducting client collection of emails in response to a litigation hold request. Regardless of the reason given to the proper authority for the investigator to collect the email, such as permission or by court order, the investigator can collect emails stored on a remote server belonging to a web-based email provider.

Collecting email from web-based accounts can be accomplished fairly easily with a proper understanding of the mail protocols used. Email from a web mail account can be done by using a local email client (one installed on the investigator's workstation or laptop) like Outlook from Microsoft or a free client like Zimbra from VMWare. Using one of these local email clients, the investigator can set up his connection to the web-based email service and synch his client with the web-based service. Each of the web-based email services has slightly different connection parameters. The investigator needs to research the connection parameters prior to conducting the collection. This will ensure the collection is conducted without issues. Prior to the collection, the investigator needs to have the proper legal authority established and obtain the login usernames and passwords for the account to be acquired. Logging into the web-based email service, such as Google, may also require compliance with certain security features like their notification of an unrecognized computer. This can require the collection of a text message from the account holder's cell phone.

Mail protocols

SMTP is the protocol used for transmitting email across the Internet. We discussed this protocol in Chapter 3. Along with the SMTP protocol are the protocols for accessing the user's mail transfer servers. These protocols are:

- Post Office Protocol (POP)
- Internet Message Access Protocol (IMAP)

Both POP and IMAP are used for communication between a user's email program and the user's mail transfer server. Each protocol allows the email user to download their email to a local device for later or off-line review. The functions of the protocols are different and require specific setup on the mail transfer server as well as the local device to accept the mail through these processes.

Conducting email collection from web-based services should be done through the use of IMAP and not POP. While POP is an effective tool for personal synchronization of email and access to that email, it does not effectively allow for complete collection of web-based email. IMAP was designed to allow for complete control and synchronization of SMTP email accounts on an email server. While IMAP is the best method for collecting the email, POP may be the only alternative depending on the email service. Yahoo as an example does not allow desktop access through IMAP. We discuss how each method is accomplished below.

Investigator's email collection options

The investigator has several options available to collect email from a MTA. The investigator can provide legal service to the mail hosting company and wait for their response. This may be the only option if access externally from the web is not available. If the investigator has external access to the email account with the appropriate permission and account access information, there are some other options for collecting the email. Each option requires an understanding of the protocol and the requirements of the MTAs (the MTA in these cases usually refers to a web-based accessible email service, that is, Gmail, Yahoo mail, or Live mail). We are going to discuss two of the easiest options for the investigator to access the mail account externally or from the user point of view. The first is a free method, Zimbra by VMware, and the other uses a reasonably common email program, Outlook by Microsoft. Both of these tools provide the investigator the ability to collect email from mail transfer services. Both programs are desktop tools that give the user the ability to collect the emails from a specific account that the investigator has access to. The access requires that the investigator has the legal authority and the username and password to the account.

To accurately collect the email from the MTA, the investigator in most cases will have to login to the account and set up the account to allow for the transfer of the mail using either POP access or IMAP. Depending on the accessed email service, additional features may need to be invoked to allow for the collection of all folders. In Gmail, additional steps are required to collect the chats saved in the account. The investigator needs to change the setting to have the chat viewable in the mailbox. Also in Gmail, contacts and calendar events require a separate export of those items as they are not in the mailbox which has an IMAP access connection. The investigator can document the settings of the account and any changes he makes by taking screen shots of the access process, using the tools noted in Chapter 5. Each of the Internet email programs have different settings and should

be researched prior to conducting the email collections. Common with any of the collection methods is that they are using the Internet and any latency it may have as well as the email servers containing the data to be collected. What this means to the investigator is that when the synchronization of the account begins between the method selected and the email account, the time involved in the collection can be a few minutes with small amounts of data to hours for accounts with large numbers of emails.

INVESTIGATIVE TIPS

Always there are exceptions to every rule. In the case of downloading email from web-based services, it is Yahoo. Yahoo mail collection can be a little different depending on the service being provided by Yahoo. Yahoo has free access accounts and paid email accounts. The free services are generally only accessible by the POP3 protocol. The pay accounts have the option of accessing the account through IMAP. Some reports by Yahoo users on the Internet have related they have accessed their free accounts by IMAP access, but Yahoo states they do not support that protocol for free accounts. There are third party utilities that purport to connect through the IMAP protocol, but validation by the investigator should occur prior to implementing any utility during an investigation.

Zimbra Desktop email collections

Zimbra Desktop is an email program from VMWare, the makers of virtual machine technology. Zimbra Desktop is part of a suite of email service programs provided as Open Source and pay for products. The Zimbra family of products includes server-based programs as well as the desktop program we are going to discuss here. Zimbra Desktop is a simple to use and install program that allows the investigator to easily capture email from an online mail service. Here are the steps:

Zimbra Desktop installation:

1. Download Zimbra Desktop from the Zimbra website www.zimbra.com.
2. Install Zimbra Desktop on local machine.
3. The first screen will ask for the investigator to add an email account. Select the type of email to collect.
4. Under Add New Account add the account name, email address, and password. Select “Check Messages:” to “manually” and check “Sychronize all calendars” and “Synchronize all contacts and groups”.
5. Click “Validate and Save”.

Some additional notes for setting up specific accounts:

a. Setting up a Yahoo account may require additional validation processes.
b. Gmail accounts require you to change the Gmail account settings to accept IMAP connections. In addition, the folders within the Gmail account need to be made visible to the IMAP function. Under the “Label” tab in the settings function select the “Show in IMAP” for each folder to collect and select

FIGURE 8.8

Adding new account to Zimbra.

"show". This makes the folders visible in the folder tree on the left side of the screen and downloadable.

Setting up new accounts in Zimbra Desktop: (Figure 8.8).

The Add New Accounts function in Zimbra Desktop allows you to easily add new accounts. The selections include:

- Yahoo! Mail: You can set up Yahoo! Mail, Yahoo! Mail Plus, Yahoo! Small Business, Ymail, or Rocketmail accounts.
- Gmail: Your Gmail account must be set up to allow IMAP access. You must log into the target Gmail account and enable IMAP in the "Labels" tab under the settings. Check all the items to "Show" and check the box for each item to "Show in IMAP".
- Other POP/IMAP accounts: You must have complete settings information in order to set up POP/IMAP access. You can obtain such information from the target's service provider or research it on the Internet.

Once the account is added select the account and right click to select "Send/Receive".

Once the synchronization is complete, the investigator can verify that the email was collected by comparing the number of emails in the online account to the number held in the synchronized account in Zimbra. The investigator can then use the Zimbra email client to export the messages out in a compressed file as an evidence container. In Zimbra click on the "Preferences" tab and an option under the targeted user account will appear called "Import/Export". Click this and a new field will appear on the right. Under "Export" select "Advanced Settings"

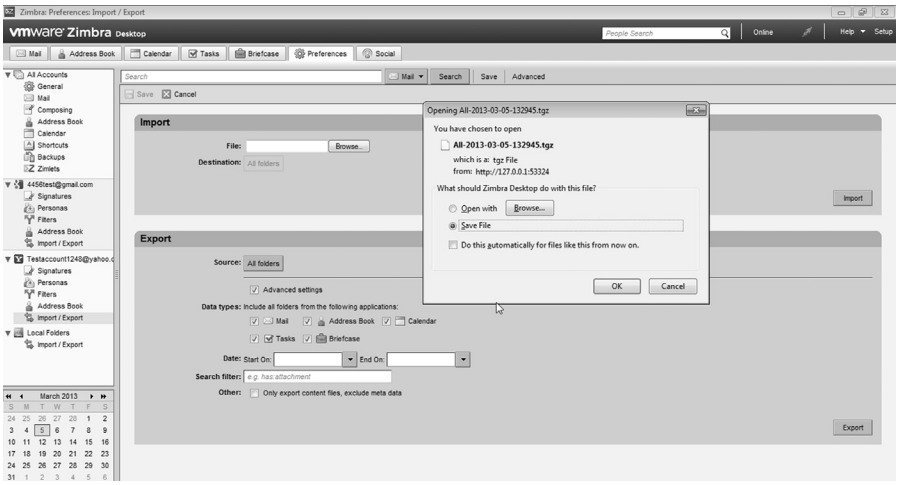

FIGURE 8.9

Zimbra Desktop saving email from online account.

and include all the data types required. Set the data range and leave the "other" box blank. Click the "Export" button and a box to save the data will appear. Zimbra saves the data in a compressed .tgz file to the location you select. This evidence container can then be hashed to provide a unique identifier for the file. After email collection is completed, the investigator needs to access the account and return the settings to their original state. The investigator can use Zimbra to review the email after the emails are saved separately as an evidence item (Figure 8.9).

Using Outlook for email collections

Using Microsoft Outlook for web-based email collections requires setting up Outlook to access the email account. The investigator needs to research online the exact account access settings prior to conducting the collection. Simply doing a Google or Bing search on the email server and "IMAP Account Settings" will provide the setting information needed. The following steps can be used in Outlook to set up a new account for collection:

1. Create a new email account by clicking on "Tools", then "E-mail Accounts".
2. Add a new email account and click "Next".
3. Select IMAP and click "Next".
4. This window asks for specific connection information. The investigator should have already researched the specific connection requirements for the email service to be accessed including:
   a. Your name: This is the user's account to be accessed.
   b. Email address: The user account's complete email address.

   c. Incoming mail server: The incoming mail server for the email service.
   d. Outgoing mail server: The outgoing mail server for the email service.
   e. Username: The user's account username.
   f. Password: The user's password.
5. At this point, don't click on the "Next" button; click on the "More Settings" button to compete the proper setup of the account to allow for the collection.
6. Under the "More Settings" box, there are specific options unique to the web-based email service from which the investigator will be collecting email. The prior research should indicate what exactly will be required for the particular email service you are collecting from. As an example, under the "Outgoing Server" tab the box titled "My outgoing server (SMTP) requires authentication" may be required to be checked. Additionally, under the "Advanced" tab, the setting for the "incoming server" and the "outgoing server" ports may need to be changed to meet the service access requirements.
7. Once the settings are correctly input, the investigator can click "OK" and Outlook will test the connection. If the connection is good two green check marks will appear, if not an error notice will appear advising the investigator to correct the settings.
8. Outlook will connect to the email service with the input account information and settings and begin to download the folder structure and then the emails. This however is not the end of the setup process for the collections using Outlook. Because the services are online and the email is accessible through the Internet Outlook does not automatically download complete files and their attachments. Depending on the version of Outlook, the investigator is using the investigator needs to go to "Send/Receive Groups" and go to the account and select "Edit".
9. In the "All Accounts" window, each folder option needs to be changed. The investigator needs to be selected and the "Download complete item including attachments" radio button selected individually for the folders to be collected. Select "OK" when completed. This will allow all the email to be saved into the Outlook account previously setup by the investigator.
10. Once the downloading of the account information is complete (this can take several hours even for small accounts), the investigator can go to the Outlook storage location for the version used during the collection and copy the Outlook PST file into evidence.

Once the synchronization is complete, the investigator can verify that the email was collected by comparing the number of emails in the online account to the number held in the synchronized account in Outlook. The investigator can then use the Outlook email client to export the messages out in a Microsoft Windows PST file as an evidence container. The PST file is the common storage file for email in Outlook. This PST can then be hashed to provide a unique identifier for the file.

After the email collection is completed, the investigator needs to access the account and return the settings to their original state. The investigator can use Outlook to review the email after the PST is saved separately as an evidence item.

INVESTIGATIVE TIPS

Other Investigative Techniques for Identifying Targets on the Internet

Identifying the target of an investigation through IP addresses is a standard tool of the Internet investigator. But, if one can't get the correct IP address, or identify the target's ISP, what can the investigator do? Well the investigation doesn't end just because the target has hidden himself. Granted it makes it much more difficult, but finding them can occur. Remember, the more often the suspect(s) engages or interacts with their victim(s) or repeats their illegal conduct the more likely you as the investigator will be given additional clues that will lead to their identification and apprehension. In later chapters, we will discuss proactive investigations and specific things the investigator can employee to identify targets. IP addresses are still the corner stone of any of these processes.

Relevant RFCs related to IP tracing

The following Request for Comments (RFCs) reflects the standard protocols that guide the formation, sending, movement through the Internet, and receiving of emails. Each of the references provide the investigator with a variety of information that is unique to emails and the use. Becoming familiar with the underlying email protocols will provide the investigator with a solid foundation of how the email system works. It will also enable the investigator to easily identify and parse through an email's header to identify where and when it was produced. To locate the RFCs, the investigator can go the Internet Engineering Task Force (IETF) website at http://www.ietf.org/rfc.html and using the search function can find the listed RFC.

Message Format

- RFC 2822 Internet Message Format
- RFC 3464 Extensible Message Format for Delivery Status Notifications

SMTP—Simple Mail Transfer Protocol

- RFC 821
- RFC 1652 SMTP Service Extension for 8 bit-MIMEtransport
- RFC 1869 SMTP Service Extensions
- RFC 1870 SMTP Service Extension for Message Size Declaration
- RFC 1985 SMTP Service Extension for Remote Message Queue Starting
- RFC 2034 SMTP Service Extension for Returning Enhanced Error Codes
- RFC 2476 Message Submission
- RFC 2554 SMTP Service Extension for Authentication
- RFC 2821 Simple Mail Transfer Protocol

- RFC 2920 SMTP Service Extension for Command Pipelining
- RFC 3030 SMTP Service Extensions for Transmission of Large and Binary MIME Messages
- RFC 2645 ON-DEMAND MAIL RELAY (ODMR) SMTP with Dynamic IP Addresses
- RFC 2852 Deliver By SMTP Service Extension

MIME

- RFC 822 Standard for the Format of ARPA Internet Text Messages
- RFC 2045 Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies
- RFC 046 Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types
- RFC 2047 Multipurpose Internet Mail Extensions (MIME) Part Three: Message Header Extensions for Non-ASCII Text
- RFC 2048 Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures
- RFC 2049 Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples

POP3—Post Office Protocol, Version 3

- RFC 1939 Post Office Protocol—Version 3

IMAP4—Internet Message Access Protocol, Version 4

- RFC 2683 IMAP4 Implementation Recommendations
- RFC 3501 Internet Message Access Protocol—Version 4rev1

CONCLUSIONS

This chapter provided methods by which one can trace an IP address and emails. Tracing an IP address is a basic function of the Internet investigator. Understanding the process required to locate the IP address and determine its origin is fundamental to the successful completion of an investigation. We have attempted to cover the basic skills necessary to accomplish these basic processes. Familiarity with the information in this chapter will give the investigator a solid foundation for investigating crimes committed on the Internet, particularly in how to identify those responsible for their commission.

Further reading

AFRINIC (n.d.). *African network information centre*. Retrieved from <http://www.afrinic.net/>.

APNIC—Home. (n.d.). Asia-Pacific Network Information Centre (APNIC). Retrieved from <http://www.apnic.net/>.

ARIN. (n.d.). American Registry for Internet Numbers (ARIN). Retrieved from <https://www.arin.net/>.

Brodkin, J. (n.d.). The MIME guys: How two internet gurus changed e-mail forever. *Network World—Network World*. Retrieved from <http://www.networkworld.com/news/2011/020111-mime-internet-email.html?page=1>.

Common Internet Message Header Fields. (n.d.). *People.dsv.su.se*. Retrieved from <http://people.dsv.su.se/~jpalme/ietf/mail-headers/mail-headers.html/>.

DNSstuff. (n.d.). *DNS tools, manage monitor analyze, DNSstuff*. Retrieved from <http://www.dnsstuff.com/tools/tools/>.

FortÃ©. (n.d.). Internet message headers—quick reference. *Tieto- ja sÃ¤hkÃ¶tekniikka Tampereen Teknillinen Yliopisto*. Retrieved from <http://www.cs.tut.fi/~jkorpela/headers.html/>.

Free Online Network tools—Traceroute, Nslookup, Dig, Whois lookup, Ping—IPv6. (n.d.). *Free online network tools*. Retrieved from <http://centralops.net/co/>.

How Base64 Encoding Works—About Email. *About email—find free email, email program support, spam help and tips*. Retrieved from <http://email.about.com/cs/standards/a/base64_encoding.htm/>.

Internet Assigned Numbers Authority. (n.d.). Internet Assigned Numbers Authority. Retrieved from <http://www.iana.org/>.

IP Address Geolocation to Identify Website Visitor's Geographical Location. (n.d.). *IP address geolocation*. Retrieved from <http://IP2Location.com/>.

LACNIC. (n.d.). Latin America and Caribbean Network Information Centre (LACNIC). Retrieved from <http://www.lacnic.net/en/web/lacnic/inicio/>.

MaxMind—IP Geolocation and Online Fraud Prevention. (n.d.). *MaxMind—IP geolocation and online fraud prevention*. Retrieved from <http://www.maxmind.com/>.

Reno, J. (n.d.). *BrainyQuote.com*. Retrieved from <http://www.brainyquote.com/quotes/quotes/j/janetreno315534.html/>.

Request for Comments (RFC) Pages. (n.d.). *Request for comments (RFC) Pages*. Retrieved from <www.ietf.org/rfc.html/>.

RIPE Network Coordination Centre. (n.d.). Réseaux IP Européens Network Coordination Centre. Retrieved from <http://www.ripe.net/>.

Setting Up POP/IMAP Accounts. (n.d.). *Zimbra*. Retrieved from <http://www.zimbra.com/desktop/help/en_US/Zdesktop/z-Setting_up_POP_IMAP_accounts.htm/>.

SPF: RFC 4408 (n.d.). *SPF: Project overview*. Retrieved from <http://www.openspf.org/RFC_4408#header-field/>.

Traceroute, Ping, Domain Name Server (DNS) Lookup, WHOIS. (n.d.). *Traceroute*. Retrieved from <http://network-tools.com/>.

Understanding the Information Contained in an E-mail Header. (n.d.). *Computer hope's free computer help*. Retrieved from <http://www.computerhope.com/issues/ch000918.htm/>.

This page intentionally left blank