SPECIAL TOPICS SERIES

APRI

American
Prosecutors
Research Institute

Understanding E-mail:

A Primer for Local Prosecutors

BJA Bureau of Justice Assistance

American Prosecutors Research Institute
99 Canal Center Plaza, Suite 510
Alexandria, VA 22314
www.ndaa-apri.org

Thomas J. Charron
President

Roger Floren
Chief of Staff

Jason Scott
Senior Attorney, White Collar Crime Program

Debra Whitcomb
Director, Grant Programs and Development

George Ross
Director, Grants Management

This document was produced under Grant No. 98LS-VX-0002 from the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice. This information is offered for educational purposes only and is not legal advice. Points of view or opinions expressed in this document are those of the authors and do not necessarily represent the official position of the United States Department of Justice, the National District Attorneys Association, or the American Prosecutors Research Institute.

The American Prosecutors Research Institute is the nonprofit research, training and technical assistance affiliate of the National District Attorneys Association.

Understanding E-mail:

A Primer for Local Prosecutors

August 2005

Jason Scott, Senior Attorney
White Collar Crime Program
American Prosecutors Research Institute

TABLE OF CONTENTS

INTRODUCTION

The universe of crimes involving digital evidence is expanding exponentially. Many types of cases involve at least one component having to do with retrieving digital evidence. Online fraud, identity theft, child pornography (stored images), hacking, computer intrusion, drug offenses (pagers, cell phone memory), vehicular homicide (data recorders) and many other crimes have a "computer" element. Many times, these pieces of evidence are relayed electronically using e-mail via the Internet to move the data from one place to another. E-mailing information today is as commonplace as making a regular telephone call. E-mail accounts are free and easily acquired by anyone with access to the Internet. The increasing ease of access to the Internet and e-mail is creating unique problems for law enforcement trying to investigate and prosecute these crimes.

From a prosecutor's perspective, e-mails are digital evidence stored on media devices. This monograph will discuss the basic "tech" terminology a prosecutor is likely to encounter and needs to be familiar with when prosecuting high-tech crimes involving e-mail.[1] It will review how e-mail works, how it moves through the Internet, where an investigator might find it in a home or business, what prosecutors should look for when examining it, and the paths e-mail takes to reach its final destination. The monograph also will dispel the myth that a degree in computer science or electrical engineering is necessary to understand the technology. The challenges of tracing e-mails, reading e-mail headers and recovering electronic evidence are similar to challenges that arise in other criminal investigations, except in the context of a newer and perhaps less familiar medium. To illustrate what concepts are central to grasp in these types of cases, this report will continually ask the question, "Why is this important to my case?"

[1] The legal process relating to obtaining e-mail and e-mail account information is discussed in a companion monograph entitled *The ECPA, ISPs & Obtaining E-mail: A Primer for Local Prosecutors.*

THE INTERNET

Before learning about tracing e-mails and reading e-mail headers, prosecutors need to understand the structure and organization of the Internet, and the network through which e-mail travels.

Structure

The Internet is essentially a "network of networks" that are interconnected, capable of communicating and sharing data with each other, and able to act together as a single network. A network is two or more devices connected to each other that are capable of exchanging data via a common protocol that exists between the two devices. A protocol is an agreed-upon format, or language, for transmitting data between two devices. This common language allows the machines to communicate. Machines on one network can communicate with machines on other networks and can send data, files, and other information back and forth.[2] Machines in a network can be connected to each other by means of a cable or wireless device allowing the transfer of data (information) from one machine to the other and vice-versa.

Every computer logged into the Internet has an Internet Protocol (IP) address at a given point in time. An IP address is an identifier for a computer or a device on a Transfer Call Protocol / Internet Protocol (TCP/IP) network. Networks using the TCP/IP protocol route messages based on the IP address of the destination.[3] The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. For example, 65.248.124.50 is the IP address for www.ndaa-apri.org. Connecting a private network to the Internet requires the use of registered IP addresses. Every computer that communicates over the Internet is assigned an IP address that uniquely identifies the device and distinguishes it from other computers connected to the Internet during that same time. The sender's address is the IP address assigned to that particular computer at the specific time it was connected to the Internet. This

[2] www.webopedia.com

[3] www.webopedia.com/TERM/I/IP_address.html

IP address stays with the e-mail as it travels along its intended path. Each server[4] the e-mail passes through adds its identifying IP address to the e-mail header.

Typically, IP addresses are either static or dynamic. A static IP address is semi-permanent in that the user and the Internet service provider (ISP) have contracted for that IP address to be regularly available for the user to connect to the Internet. Each time that customer connects to the Internet, the connection uses the same IP address. Cable modems, digital subscriber lines (DSL), T1, T3 and other "broadband" connections are normally assigned a static IP address.[5] A dynamic IP address changes each time the customer accesses the Internet. Telephonic dial-up users are connecting to the Internet through dynamic IP addresses. Whenever the customer dials into the Internet via an ISP, the IP address assigned to the connection is different. The dynamic IP address identifies that computer connected to the Internet through that specific ISP only for the duration of that one-time connection. A dynamic address is more difficult for an investigator to trace. The ISP may not maintain the records as long as those for static IP addresses, requiring the investigator to establish a time frame when the suspect's computer was connected to the Internet.

Large ISPs will have a range of available IP addresses to assign to individuals who dial in to the Internet. Smaller ISPs and businesses frequently lease IP addresses from the large ISPs. The Internet Corporation for Assigned Names and Numbers (ICANN) assigns ranges of IP addresses to ISPs. ISPs may use those addresses or "sub-let" them. Whether users are connecting via dial-up modem or high-speed modem, their access point to the Internet will have an IP address assigned and the connection can be tracked (with certain exceptions to be covered later).

[4] A server is a computer or device on a network that manages network resources. For example, a *file server* is a computer and storage device dedicated to storing files. (www.webopedia.com/TERM/s/server.html)

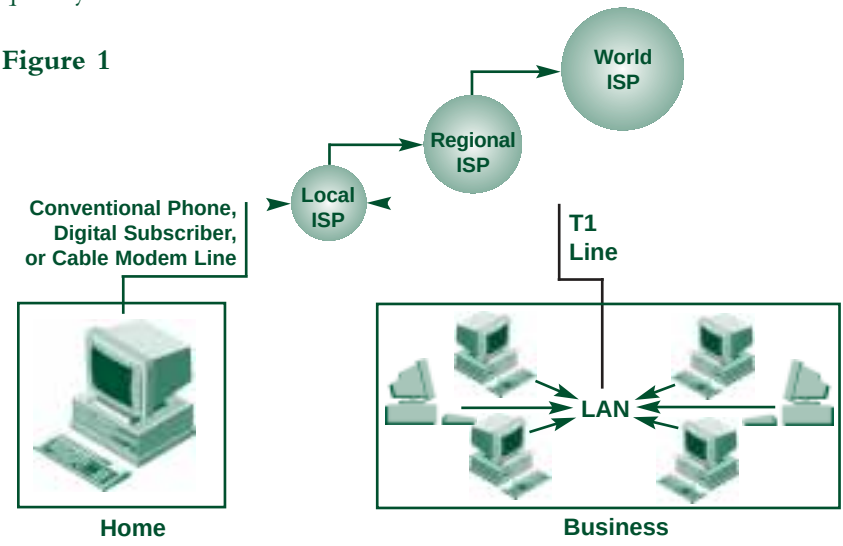
[5] Static IP addresses assigned to a customer can sometimes change. An ISP will lease a block of IP addresses and assign one to a customer for a specified period of time. When the lease expires, a new static IP address can be assigned.

Networks

Several computers connected together at one location, e.g., a prosecutor's office, are called a local area network (LAN). Several LANs connected together over a wide geographic area, e.g., a county's computer systems, are called a wide area network (WAN). A WAN usually consists of several large or small LANs. The one machine tasked with controlling the traffic on the LAN is called a server. A server can be an ordinary personal computer (PC) that has the necessary software and hardware that allow it to act as the gatekeeper for information moving within or into and out of the network. A LAN can have one server for handling traffic within the LAN and another for handling e-mails coming into and out of the LAN or network. The server that handles e-mail and access to the Internet is typically called a communications server. A server that handles intra-network traffic is typically called a network server.

Figure 1 below depicts how a PC of an individual user or a business network consisting of a LAN connects to the Internet. A "T1 Line" is a fast connection to the Internet, i.e. capable of moving large amounts of data quickly.[6]

Figure 1



[6] T-1 lines are a popular leased line option for businesses connecting to the Internet and for Internet Service Providers (ISPs) connecting to the Internet backbone. T-1 lines are sometimes referred to as *DS1* lines. (www.webopedia.com/TERM/T/T_1_carrier.html)

The home PC or business LAN connects to the Internet using a modem transmitting data (e-mail, picture, file, etc.) on a conventional phone line, DSL or a cable modem coaxial cable line. The first connection is to the local ISP. The user or business will have a contract with the ISP to provide access to the Internet for a fee. The local ISP is networked to a regional ISP, which in turn is connected to the world ISP or the "backbone" of the Internet.[7]

[7] The backbone of the Internet is a term used to describe the main network connections composing the Internet. (www.webopedia.com/TERM/B/backbone.html)

E-MAIL

E-mail is short for electronic mail, which is the transmission of messages or data over communications networks. E-mails can have files embedded in them and/or attached to them. The embedded or attached files can be pictures, text, images, charts or many other types of files. E-mail traveling across the Internet is normally not encrypted[8] and can be read in much the same way as the back of a postcard in the post. E-mail can be found on Web-based or host-based systems. Web-based e-mail, like Hotmail or Yahoo mail, stores the e-mail at a remote location accessible via the Internet. Web-based e-mail can leave traces of the e-mail on the computer used to view it. Host-based e-mail, e-mail that is retrieved and stored on a computer in a business or home for viewing, will remain there depending on user settings.

E-mail can be stored in one of at least four places: the sender's computer, the mail server at the sender's ISP, the mail server at the recipient's ISP, and the recipient's computer. There are variations to the path that e-mail can take and the places along that path where a copy of the e-mail might temporarily be stored before reaching its final destination. The communications server in a LAN or a WAN will temporarily store the e-mail until the network user retrieves it.

Sending E-mail

Generally, when you send an e-mail you are typing a note or attaching a file that your PC or network will send through the Internet to be received at an electronic mailbox where you have addressed the e-mail. The recipient's mailbox can be on the Internet, at a local ISP, on a work computer or on a home PC. Typically, the e-mail waits on the recipient's computer or mail server until the recipient claims it.

E-mail that is transferred through the local, regional and world ISPs is then delivered via the backbone ISP to another regional, then local ISP.

[8] Encrypted e-mail prevents e-mail from being read as it travels through and across the Internet.

The e-mail is broken into data packets (small units of data). The data packets are reassembled at the electronic mailbox of the intended recipient, who also has an agreement with a local ISP that provides access to the Internet. Data can travel along several indirect "hops" (pathways) before reaching its destination. Not all data travels neatly bundled in one package, like a letter in an envelope. A useful analogy is that the e-mail and any attachments are broken into several envelopes that arrive nearly simultaneously and are reassembled for delivery at the intended recipient's ISP.

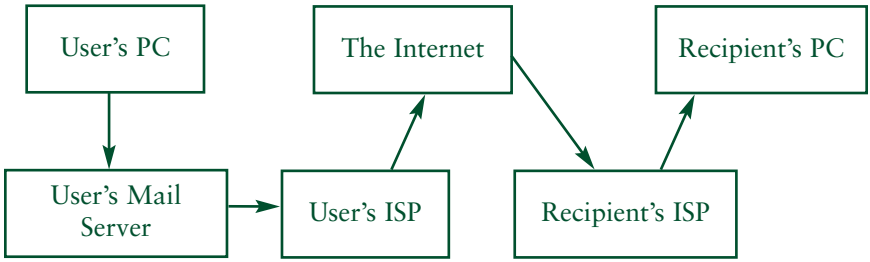
The e-mail is broken apart and reassembled by an e-mail client. An e-mail client is a computer program that acts as a post office where the user can collect mail that has arrived from the Internet. Outlook, Lotus Notes and Eudora are common e-mail client programs. The e-mail client uses a computer language called a "protocol."

Information travels over the Internet via a variety of languages known as protocols. A computer or device must support the right protocols before it can communicate with other computers. Some examples of common e-mail protocols are: SMTP – simple mail transfer protocol (server to server); POP3 – post office protocol 3; IMAP – Internet mail access protocol; and LDAP – lightweight directory access protocol (see glossary for detailed explanations).

Using the protocol, the user's machine:
- connects to the Internet through its ISP server;
- contacts the mail server for the intended recipient's computer;
- has an electronic conversation confirming destination, end user information and availability to receive e-mail; and
- transfers the e-mail, broken into smaller packets, to an electronic mailbox for the intended recipient.

This process happens without the user's knowledge. Figure 2 depicts the typical path an e-mail takes when sent from one user to another. The sender is using a PC on a LAN, and the intended recipient is using a stand-alone PC connected to an ISP.

Figure 2



Reading E-mail Headers

E-mail headers, commonly referred to as the "TO" and "FROM" lines, are added by the e-mail client to an e-mail as it travels from the user's PC to its final destination. Each leg of the e-mail's journey across the Internet involves passing through a mail server[9] (large computer or switching device), often called a "hop." As the message passes through, each server "stamps" the message with an Internet protocol address (IP address), a date, a time generated by that server, and additional information. All of this information is in the full header at the beginning of every e-mail.

Headers are normally added to the message three times: (1) when the message is composed, by the e-mail program the sender is using; (2) when that e-mail program transfers control to the sender's mail server; and (3) when the sender's mail server transfers control to the ISP. The process is analogous to an envelope that is postmarked with the date and time as it passes through the hands of several postal carriers and post offices before arriving at its final destination. This analogy includes a confirmation of delivery. An e-mail header is your best friend when trying to identify the sender of an e-mail. Without the header information, it is impossible to see where the e-mail is coming from and when it was sent.

Most e-mail clients hide the header information for aesthetic reasons. Users can reveal full header information within their mail programs to

[9] A "mail server" is simply a computer whose sole purpose is to act as a gatekeeper for e-mail traffic (e-mail server) or a message manager and "traffic cop" for network traffic (network server). There are other types of servers as well.

see the details of where the e-mail has traveled.[10] These programs reside on the user's computer and/or on the company mail server and are a temporary way station until an e-mail is opened and read. E-mail client programs allow the user to view the original header information for e-mail that is retrieved. However, the servers that the e-mail passes through may not have the correct time and dates and may be in different time zones. These factors have to be accounted for when piecing together the timeline of an e-mail.[11] Be aware that an e-mail address can easily be manipulated, using the e-mail client, to show an address other than the actual sender's address or recipient's address.[12] In addition, some mail servers have message forwarding. Message forwarding simply includes another way station in the header information and path of the e-mail. Note the locations in the headers where mail is being forwarded from and forwarded to.

Figure 3 is a simplified graphic of the path the e-mail in Figure 4 travels.

Figure 3

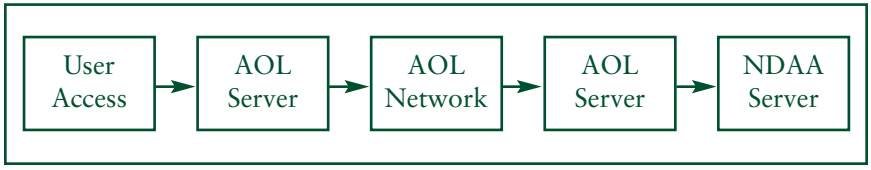


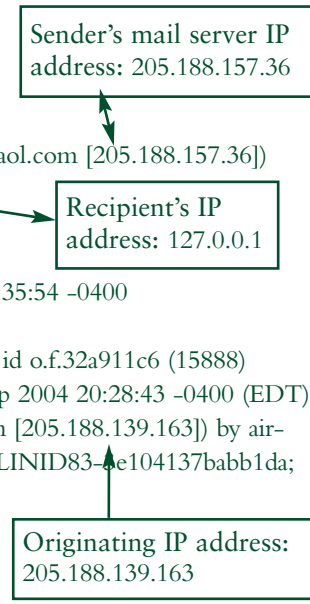
Figure 4 is a sample e-mail header, which will be used to "walk" readers through the available information in the text that follows. To track an e-mail chronologically, header information is read from the bottom to the top. The "to" and "from" fields contain the e-mail addresses for the recipient and the sender.

[10] How this is done will depend upon the user's e-mail software. For example, in Outlook, with an e-mail open, click on "View" and then on "Options" to display the Internet headers.

[11] Some Web sites and software programs offer to remove or "strip" the headers from an e-mail to protect the sender's identity, location or both. Investigations involving "stripped" e-mail headers are complex and beyond the scope of this monograph.

[12] This is not to be confused with the IP address, which generally cannot be altered and may only be done with great difficulty and expertise.

Figure 4
Sample E-mail Header



Return-path: <Julian123@aol.com>
Received: from imo-d04.mx.aol.com (imo-d04.mx.aol.com [205.188.157.36])
by ndaa.org (ndaa.org [127.0.0.1])
(MDaemon.PRO.v7.1.2.R)
with ESMTP id md50000285249.msg
for <Joshua@ndaa.org>; Thu, 02 Sep 2004 20:35:54 -0400
Received: from Julian123@aol.com
by imo-d04.mx.aol.com (mail_out_v37_r3.4.) id o.f.32a911c6 (15888)
for <joshua.smith@ndaa-apri.org>; Thu, 2 Sep 2004 20:28:43 -0400 (EDT)
Received: from aol.com (mow-d22.webmail.aol.com [205.188.139.163]) by air-id08.mx.aol.com (v101_r1.4) with ESMTP id MAILINID83-de104137babb1da; Thu, 02 Sep 2004 20:28:43 -0400
Date: Thu, 02 Sep 2004 20:28:43 -0400
From: Julian123@aol.com
To: Joshua.smith@ndaa-apri.org
Subject: APRI Trainings
MIME-Version: 1.0
Message-ID: <274EF33D.17A03C1A.0017949A@aol.com>
X-Mailer: Atlas Mailer 2.0
X-AOL-IP: 209.144.140.2
X-AOL-Language: english
Content-Type: text/plain; charset=iso-8859-1
Content-Transfer-Encoding: 8bit
X-MDRcpt-To: Joshua.smith@ndaa-apri.org
X-Rcpt-To: Joshua.smith@ndaa-apri.org
X-MDRemoteIP: 205.188.157.36
X-Return-Path: Julian123@aol.com
X-MDaemon-Deliver-To: joshua@ndaa.org
X-Spam-Checker-Version: SpamAssassin 2.63 (2004-01-11) on InterShield
X-Spam-Status: No, hits=1.2 required=5.0
tests=FROM_ENDS_IN_NUMS,NO_REAL_NAME
autolearn=no version=2.63
X-Spam-Level: *
X-Spam-Processed: ndaa.org, Thu, 02 Sep 2004 20:35:57 -0400
X-MDAV-Processed: ndaa.org, Thu, 02 Sep 2004 20:35:57 -0400

Following is a line-by-line analysis of the e-mail header in Figure 4, starting from the bottom of the header.

Step 1

X-Spam-Checker-Version: SpamAssassin 2.63 (2004-01-11) on InterShield
X-Spam-Status: No, hits=1.2 required=5.0
tests=FROM_ENDS_IN_NUMS,NO_REAL_NAME
autolearn=no version=2.63
X-Spam-Level: *
X-Spam-Processed: ndaa.org, Thu, 02 Sep 2004 20:35:57 -0400
X-MDAV-Processed: ndaa.org, Thu, 02 Sep 2004 20:35:57 -0400
These are programs that scan the e-mail and its attachments for spam[13] and viruses.[14]

Step 2

X-MDaemon-Deliver-To: joshua@ndaa.org
This is a command to deliver the e-mail to the address joshua@ndaa.org.

Step 3

Return-Path: Julian123@aol.com
This is the e-mail address for the recipient to send e-mail back to the original sender.

Step 4

X-Mailer: Atlas Mailer 2.0
X-AOL-IP: 209.144.140.2
X-AOL-Language: english
Content-Type: text/plain; charset=iso-8859-1
Content-Transfer-Encoding: 8bit
This describes the content and format of the e-mail as well as the client used to send the e-mail.

Step 5

Message-ID: <274EF33D.17A03C1A.0017949A@aol.com>
This is the message ID attached to the e-mail. It helps administrators locate the e-mail in a log.

13 Spam is electronic junk mail or junk newsgroup postings.

14 Viruses are programs or pieces of code that are loaded onto a computer without the user's knowledge and run against the user's wishes.

Step 6
From: Julian123@aol.com
To: Joshua.smith@ndaa-apri.org
Subject: APRI Trainings
The subject line is input by the sender. The "to" line is the e-mail address where the sender intended to send the e-mail.

Step 7
Date: Thu, 02 Sep 2004 20:35:54 –0400
The e-mail transfer happened on Thursday, September 2, 2004 at 8:35 p.m. Eastern Standard Time (which is –4 hours behind Greenwich Mean Time).

Step 8
with ESMTP id md50000285249.msg
The receiving machine assigned the ID number md50000285249. This information helps the network administrator search for the message in the machine's log file.

Step 9
Received: from aol.com (mow-d22.webmail.aol.com [205.188.139.163]) by air-id08.mx.aol.com (v101_r1.4) with ESMTP id MAILINID83-3e104137babb1da; Thu, 02 Sep 2004 20:28:43 -0400
This is the third "received from" address with a time and date stamp from that communication server.

Step 10
Received: from Julian123@aol.com
by imo-d04.mx.aol.com (mail_out_v37_r3.4.) id o.f.32a911c6 (15888)
for <Joshua.smith@ndaa-apri.org>; Thu, 2 Sep 2004 20:28:43 -0400 (EDT)
This is the second "received from" address, time and date stamp.

Step 11
for <joshua@ndaa.org>;
The message was addressed to joshua@ndaa.org…

Step 12
(MDaemon.PRO.v7.1.2.R)
…running a program called Mdaemon.Pro.

Step 13

by ndaa.org (ndaa.org [127.0.0.1])

This is the machine that received the message…

Step 14

(imo-d04.mx.aol.com [205.188.157.36])

*…which is really named **imo-d04.mx.aol.com** and has the IP address 205.188.157.36. This is the sender's IP address.*

Step 15

Received: from imo-d04.mx.aol.com (imo-d04.mx.aol.com [205.188.157.36])
by ndaa.org (ndaa.org [127.0.0.1])
(MDaemon.PRO.v7.1.2.R)
with ESMTP id md50000285249.msg
for <joshua@ndaa.org>; Thu, 02 Sep 2004 20:35:54 -0400

*This piece of mail was received from a machine calling itself **imo-d04.mx.aol.com.***

Identifying the Sender or Recipient of E-mail

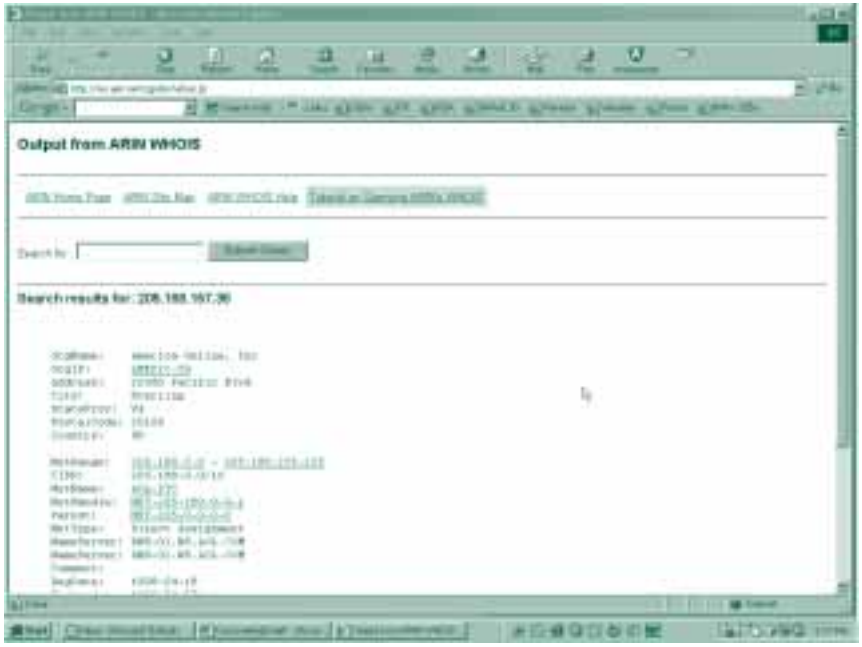
Once the first sending or "originating" IP address for the e-mail is obtained from the header information (see Step 14) your investigator can go to one of several Web sites to track the registration information for that IP address.[15] Below is a screen capture of the Web site for the American Registry for Internet Numbers (www.ARIN.net).

Figure 5

The sender's IP address in the e-mail example (Figure 4, Step 14) is "205.188.157.36." Type the IP address into the "search whois" box and hit "enter" for registration information. The folling screen shot (Figure 6) reveals that the e-mail sent to NDAA originated from America Online (AOL).

[15] Other online tools to identify the users of IP addresses are: www.samspade.org, www.arin.net, www.ipindex.net, www.allwhois.com, www.whois.net.

Figure 6



Typically, the IP address from ARIN.net (or similar registration information Web sites) will be from an ISP. The output from the ARIN WHOIS screen also gives an address for AOL, a range (net range) of IP addresses that this ISP uses, an e-mail and phone address for the technical assistance contact and various other information.

In our AOL e-mail example, the message was traced to an ISP where an individual had a single user account. However, the AOL subscriber accessed his account through the Internet, which is why the sender's mail server IP address [205.188.157.36] and the originating IP address both resolve to "Americ-59," a server at America Online, Inc (see Figure 4, Step 15). This detailed information is in the call-out screen capture shown in Figure 7.

Figure 7

```
OrgName:    America Online, Inc
OrgID:      AMERIC-59
Address:    22080 Pacific Blvd
City:       Sterling
StateProv:  VA
PostalCode: 20166
Country:    US

NetRange:   205.188.0.0 - 205.188.255.255
CIDR:       205.188.0.0/16
NetName:    AOL-DTC
NetHandle:  NET-205-188-0-0-1
Parent:     NET-205-0-0-0-0
NetType:    Direct Assignment
NameServer: DNS-01.NS.AOL.COM
NameServer: DNS-02.NS.AOL.COM
Comment:
RegDate:    1998-04-16
Updated:    1998-04-27

TechHandle: AOL-NOC-ARIN
TechName:   America Online, Inc.
TechPhone:  +1-703-265-4670
TechEmail:  domains@aol.net

# ARIN WHOIS database, last updated 2004-10-21 19:10
# Enter ? for additional hints on searching ARIN's WHOIS database.
```

Using the appropriate legal process (at the state level, a grand jury or search warrant), the investigator can now contact the "Techhandle" at the ISP to obtain information on the specific user who was accessing AOL at the time and date stamped on the e-mail. The tech person at AOL can determine which user account sent the e-mail by referencing the message ID (284EF33D.17A03C1A.0017949A@aol.com) contained within the e-mail header at Step 5. If the registering information is based in the United States, and better yet, within your jurisdiction, you are ready to proceed. Although the registering information may be false, the payment information will be accurate. Generally, an ISP that provides the sending e-mail account will "capture" the sender's IP address at the time the account was created.

At this point, the investigator has traced the e-mail back through the Internet to the originating ISP. The originating ISP, using the message ID, has determined which account holder generated the e-mail that was sent out through the ISP's server to the recipient. Additional investigative work may be necessary to identify the person sitting behind the keyboard, using this account and sending this e-mail, at this specific date and

time (e.g., staking out a location, employing a ruse to determine who is in the house or business or on the computer while the account is simultaneously being watched elsewhere).

A network administrator can be a valuable source for retrieving e-mails from a company's e-mail servers. As their title suggests, network administrators are responsible for tending to their networks and performing maintenance and upgrades as necessary. A network administrator might be instrumental in identifying the sender, particularly when trying to recover an e-mail that came from a business with a LAN. In a business setting, each node or workstation on the network has a particular address identifying it to the network servers. Network servers have the capability to log or record which users are accessing which portions of the network or communications server (e-mail and the Internet) at what times, on what dates and for how long. A review of the network server log (if it is turned on) will reveal which workstations on the network accessed the Internet at specific dates and times. Some LAN administrators do not track which workstations are sending e-mail to the network communication server. Maintaining all this information requires large amounts of storage, and some ISPs may not retain logs of user access activity for any length of time because of the excessive storage requirements. There are no mandated minimum retention periods for ISPs. Similarly, network administrators may not log any usage information, even simple network traffic and/or access to the Internet through the business's communication server. Most ISPs have a department that assists law enforcement in procuring these records via correct legal process. This process actually might be easier than identifying an individual user in the home setting, as users in a business setting typically are the only ones (besides the network administrator) to have access to their workstations via a password. Reminder: The times and dates attached to e-mail headers reflect the settings of the clock in that particular server on that particular hop.

Hiding the Sender's Identity

High tech criminals are adept at manipulating and exploiting new technologies to attempt to mask their identity and location. Unfortunately, there are several ways for e-mail senders to hide their identity.

- *Unauthorized Network Access* via wireless computing (wi-fi) enables the e-mail sender to be almost anywhere there is a wireless fidelity signal to connect to the Internet. With a laptop, wi-fi access to the Internet and an e-mail account, an individual can perpetrate many types of high-tech crimes. By gaining unauthorized access to a wi-fi network, perpetrators can disguise their identity.

- *Relaying* is another method used by e-mail senders trying to hide their identity. An e-mail is relayed if it is sent through another e-mail server hacked into by the sender. A correctly configured e-mail server will only process e-mail from within its network of users. An e-mail server that is not configured correctly becomes vulnerable to a great variety of programs that provide remote access to unauthorized senders. An investigation could lead to the e-mail server where mail is being relayed from another source. In this type of investigation, it is crucial to determine whether the network administrator of the relaying e-mail server is logging the IP addresses of the sender's e-mails.

- *Anonymizers*, or re-mailers, are Web sites that operate under the guise of protecting a user's privacy. They intentionally strip headers from e-mails and do not maintain server logs or records of any kind. After stripping the IP tracking information, the anonymizers forward the e-mails to their intended recipients. An e-mail that travels through an anonymizer site may prevent your investigator from locating the original source of the e-mail. Many (if not most) of the servers and businesses that sell this service are located outside the United States.

- *Spoofing* is an attempt by the sender to conceal the source of an e-mail message by placing false information in the e-mail header. Senders can manipulate their address via the software they use to generate e-mails and connect to the Internet (e.g. Outlook, Eudora, Lotus Notes). The e-mail the recipient receives will display a false e-mail address in the "From" field at the top of the e-mail. In fact, software is available on the Internet that allows senders to remove an IP address and potentially replace it with someone else's address. However, the first machine to receive the spoofed message records the real IP address of the machine sending the message, even though the faked identification is in the

header. This is a low-tech approach to committing crimes involving e-mail and reveals the criminal's relative lack of sophistication.

CONCLUSION

Computing technology is continually advancing. Whenever an investigator enters a domicile or work place and discovers a stand-alone computer, PDA,[16] Blackberry, laptop computer or even a cellular phone, there will likely be a connection to the Internet and electronic evidence that is stored in the device. The Internet connection includes an e-mail account for the owner, which in turn might be a source for evidence (this potential repository of evidence might be in the form of pictures or word documents, but it also might involve e-mails that are sent to and from the media device).

This monograph has discussed the basic technical terms and processes involved in investigating and prosecuting a high-tech case involving e-mail. More thorough and technical manuals exist for prosecutors seeking even greater detail on the technical workings of e-mail, ISPs, networks and servers. Some of these resources are listed in Appendix A.

Successful high-tech investigations can best be achieved when a prosecutor and investigator work together as early in the investigation as possible. Legal process and investigative choices when searching and seizing the computer or storage device will impact how the case will be charged and tried.[17] Coordination between the prosecutor and investigator can ensure that e-mail evidence is obtained in a legal and timely manner.

This monograph is only a starting point for prosecutors to accumulate a base of knowledge. Armed with an understanding of what e-mail is, how it is generated, how it travels across the Internet and where to find it, prosecutors can begin to more fervently prosecute these types of cases.

16 A PDA is a personal digital assistant, a handheld device that combines computing, telephone/fax, Internet and networking features. www.webopedia.com/TERM/P/PDA.html.

17 These issues are discussed in APRI's companion monograph entitled *The ECPA, ISPs & Obtaining E-mail: A Primer for Local Prosecutors*.

APPENDIX A: ADDITIONAL RESOURCES

Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Computer Crime and Intellectual Property Section (CCIPS), Criminal Division, United States Department of Justice, July, 2002. www.cybercrime.gov

High Tech Crime Investigators Association (HTCIA) www.htcia.org

California High-Technology Crime Prosecutor Resource CDROM, Sacramento Valley Hi-Tech Crimes Task Force, Lt. Michael Tsuchida, Project Director, Sacramento County Sheriff's Office. Phone: 916-874-3002, e-mail: hitech@sacsheriff.com, Web site: www.sachitechcops.org.

GLOSSARY

The original author and copyright holder of this glossary is Matisse Enzer and the current version of the glossary is available at www.matisse.net/files/glossary.html.

ARP
The protocol that translates Internet Protocol, or IP, addresses (for example, 128.10.3.42) into physical network addresses. One of the many members of the TCP/IP protocol suite, ARP is a key player in the process that allows a packet of data addressed to a particular Internet host to find its destination.

ARPANet
(Advanced Research Projects Agency Network) — The precursor to the Internet. Developed in the late 60s and early 70s by the US Department of Defense as an experiment in wide-area-networking that would survive a nuclear war. See Also: Internet

Backbone
A high-speed line or series of connections that forms a major pathway within a network. The term is relative as a backbone in a small network will likely be much smaller than many non-backbone lines in a large network. See Also: Network

Bandwidth
The amount of info you can send through a connection. Usually measured in bits-per-second. A full page of English text is about 16,000 bits. A fast modem can move about 15,000 bits in one second. Full-motion full-screen video would require roughly 10,000,000 bits-per-second, depending on compression. See Also: T-1

Browser
A Client program (software) that is used to look at various kinds of Internet resources. See Also: Client, URL, WWW

Client
A software program that is used to contact and obtain data from a server software program on another computer, often across a great distance. Each Client program is designed to work with one or more specific kinds of Server programs, and each Server requires a specific kind of Client. A Web Browser is a specific kind of Client. See Also: Browser, Server

DSL
(Digital Subscriber Line) — A method for moving data over regular phone lines. A DSL circuit is much faster than a regular phone connection, and the wires coming into the subscriber's premises are the same copper wires used for regular phone service. A DSL circuit must be configured to connect two specific locations, similar to a leased line.

A commonly discussed configuration of DSL allows downloads at speeds of up to 1.544 megabits (not megabytes) per second, and uploads at speeds of 128 kilobits per second. This arrangement is called ADSL: "Asymmetric" Digital Subscriber Link. Another common configuration is symmetrical: 384 Kilobits per second in both directions.

In theory, ADSL allows download speeds of up to nine megabits per second and upload speeds of up to 640 kilobits per second.

Domain Name
The unique name that identifies an Internet site. Domain Names always have two or more parts, separated by dots. The part on the left is the most specific, and the part on the right is the most general. A given machine may have more than one Domain Name but a given Domain Name points to only one machine. For example, the domain names:

ndaa-apri.org
mail.ndaa-apri.org
workshop.ndaa-apri.org

can all refer to the same machine, but each domain name can refer to no more than one machine.

Usually, all of the machines on a given Network will have the same thing as the right-hand portion of their Domain Names (ndaa-apri.org in the examples above). It is also possible for a Domain Name to exist but not be connected to an actual machine. This is often done so that a group or business can have an Internet e-mail address without having to establish a real Internet site. In these cases, some real Internet machine must handle the mail on behalf of the listed Domain Name. See Also: IP Number

E-mail
(Electronic Mail) — Messages, usually text, sent from one person to another via computer. E-mail can also be sent automatically to a large number of addresses (Mailing List).

Fire Wall
A combination of hardware and software that separates a LAN into two or more parts for security purposes. See Also: Network, LAN

Host
Any computer on a network that is a repository for services available to other computers on the network. It is quite common to have one host machine provide several services, such as WWW and USENET. See Also: Network

HTML
(HyperText Markup Language) — The coding language used to create Hypertext documents for use on the World Wide Web. HTML looks a lot like old-fashioned typesetting code, where you surround a block of text with codes that indicate how it should appear. Additionally, in HTML you can specify that a block of text, or a word, is linked to another file on the Internet. HTML files are meant to be viewed using a World Wide Web Client Program.

HTTP
(HyperText Transfer Protocol) — The protocol for moving hypertext files across the Internet. Requires a HTTP client program on one end and an HTTP server program on the other end. HTTP is the most important protocol used in the World Wide Web (WWW). See Also:

Client, Server, WWW

Internet
The vast collection of inter-connected networks that all use the TCP/IP protocols and that evolved from the ARPANET of the late 60s and early 70s.

IP Number
(Internet Protocol Number) — Sometimes called a dotted quad. A unique number consisting of four parts separated by dots, e.g.

165.113.245.2

Every machine that is on the Internet has a unique IP number — if a machine does not have an IP number, it is not really on the Internet. Most machines also have one or more Domain Names that are easier for people to remember. See Also: Domain Name, Internet, TCP/IP

ISP
(Internet Service Provider) — An institution that provides access to the Internet in some form, usually for money. See Also: Internet

LAN
(Local Area Network) — A computer network limited to the immediate area, usually the same building or floor of a building. See Also: Ethernet

Modem
(MOdulator, DEModulator) — A device that you connect to your computer and to a phone line, that allows the computer to talk to other computers through the phone system. Basically, modems do for computers what a telephone does for humans.

Network
Any time you connect two or more computers together so that they can share resources, you have a computer network.

Node
Any single computer connected to a network. See Also: Network, Internet.

Packet Switching
The method used to move data around on the Internet. In packet switching, all the data coming out of a machine is broken up into chunks. Each chunk has the address of where it came from and where it is going. This enables chunks of data from many different sources to co-mingle on the same lines, and be sorted and directed to different routes by special machines along the way. This way many people can use the same lines at the same time.

Router
A special-purpose computer (or software package) that handles the connection between two or more networks. Routers spend all their time looking at the destination addresses of the packets passing through them and deciding which route to send them on. See Also: Network, Packet Switching.

Server
A computer, or a software package, that provides a specific kind of service to client software running on other computers. The term can refer to a particular piece of software, such as a WWW server, or to the machine on which the software is running, e.g. "our mail server is down today, that's why e-mail isn't getting out." A single server machine could have several different server software packages running on it, thus providing many different servers to clients on the network. See Also: Client, Network.

SMTP
(Simple Mail Transfer Protocol) — The main protocol used to send electronic mail on the Internet. SMTP consists of a set of rules for how a program sending mail and a program receiving mail should interact. Almost all Internet e-mail is sent and received by clients and servers using SMTP, thus if one wanted to set up an e-mail server on the Internet, one would look for e-mail server software that supports SMTP. See Also: Client, Server.

T-1
A leased-line connection capable of carrying data at 1,544,000 bits-per-second. At maximum theoretical capacity, a T-1 line could move a megabyte in less than 10 seconds. That is still not fast enough for full-screen, full-motion video, for which you need at least 10,000,000 bits-per-second. T-1 is the fastest speed commonly used to connect networks to the Internet. See Also: T-3

T-3
A leased-line connection capable of carrying data at 44,736,000 bits-per-second. This is more than enough to do full-screen, full-motion video. See Also: T-1

TCP/IP
(Transmission Control Protocol/Internet Protocol) — This is the suite of protocols that defines the Internet. Originally designed for the UNIX operating system, TCP/IP software is now available for every major kind of computer operating system. To be truly on the Internet, your computer must have TCP/IP software. See Also: IP Number, Internet.

WAN
(Wide Area Network) — Any network that covers an area larger than a single building or campus. See Also: LAN, Network.

WWW
(World Wide Web) — Frequently used (incorrectly) when referring to "The Internet," WWW has two major meanings. First, loosely used: the whole constellation of resources that can be accessed using Gopher, FTP, HTTP, telnet, USENET, WAIS and some other tools. Second, the universe of hypertext servers (HTTP servers), which are the servers that allow text, graphics, sound files, etc. to be mixed together.

American Prosecutors Research Institute
99 Canal Center Plaza, Suite 510
Alexandria, Virginia 22314
Phone: (703) 549-4253
Fax: (703) 836-3195
http://www.ndaa-apri.org

APRI