

By Andrew Donofrio

Identifying the sender of an e-mail

Recently a woman entered police headquarters complaining that she believed she was being harassed and threatened by her ex-husband. The woman further explained that the threats were coming in the form of e-mails. She was receiving these electronic threats at her home and work e-mail accounts almost daily and feared for her life. As a detective assigned to investigate this case, you know that the author of these e-mails needs to -- and probably can -- be uncovered. But you are perhaps unsure how to begin this process and what's involved in a computer communication -- specifically e-mail. Understanding Internet protocol (IP) addresses and using eMailTrackerPro and VisualRoute, programs from Visualware, a Turlock, California-based software company, can benefit you.

Understanding Internet protocol addresses

In order to communicate on the Internet, a person generally needs an IP address. In the case of an alleged crime, discerning the suspect's IP address can be a bit confusing for investigators not frequently involved in technology-related cases.

It is helpful to think of an IP address as an identification number for your computer while on the Internet network. An IP address is a 32-bit numeric address, which is written as four numbers separated by periods. A typical IP address might resemble this: 172.20.105.69. Each number can range anywhere from 0 to 255. The technical end of this is of less concern to most general case detectives. However, if a case is tried in court, the technical aspects of this need to be explained by a knowledgeable computer investigator.

Therefore, what is important for the investigator to realize is that each IP address for each computer on the Internet -- at any given time -- needs to be unique. So, you

might ask, with the above numeric configuration, is it mathematically possible to give each user his or her own IP address? The answer: No. While some users of the Internet are assigned a static IP address (meaning it never changes for the life of the computer on the network), most are handed a dynamic IP address from their Internet service provider (ISP) each time they sign on.

To illustrate this scenario let's use the ever-popular ISP, America Online (AOL). An

tor needs to do is determine the IP address used at the time the e-mail was sent, figure out which Internet service provider issued the IP address, and subpoena that ISP to find out who the user was that had that IP address on the date and time the e-mail was sent. It is important to note that the results should make sense in the context of the investigation. So, for example, if the results point to an administrative computer in a monastery and your victim hasn't had any recent disagree-

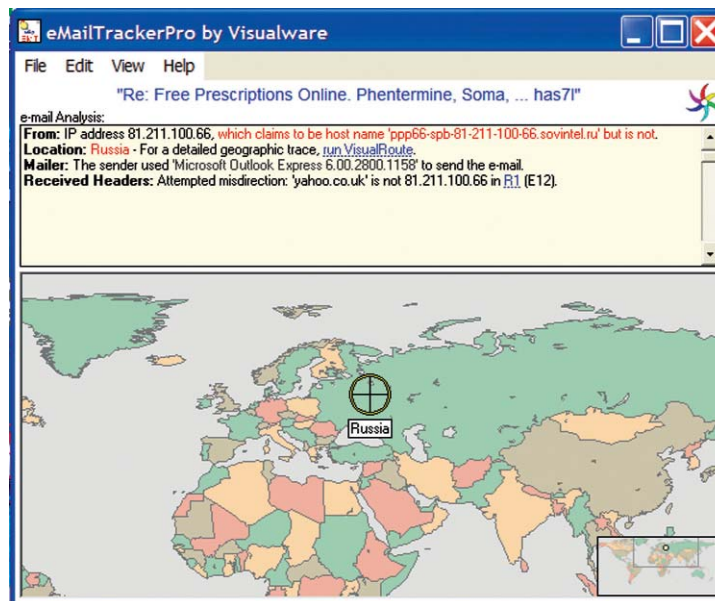
ments with a monk, you might want to give the case a second look before executing the arrest and search warrants. Granted there are other issues that come into play, but this is generally how e-mail and all Internet communications are traced.

Now the issue becomes: How do we find the IP address in the e-mail? Every sent e-mail is packaged with headers, which are data that contain the originating IP address. Each e-mail client (AOL mail, Outlook, etc.) varies slightly on how to get the header information, but generally speaking headers are attainable. Even with this information though, it is important to remember that e-mail makes several stops (known as hops) along its path and is stamped with an IP address at every turn. The headers

must therefore be read and interpreted to determine which is the originating IP address. For experienced computer investigators, this becomes second nature and they will know exactly which utilities to run to get the information they seek. However, for the vast majority of the law enforcement population this is a more difficult proposition. This is where eMailTrackerPro and VisualRoute can help.

Using eMailTrackerPro

eMailTrackerPro enables an investigator to track the route of an e-mail from its point of origin to its final destination -- and everywhere in between. The software makes tracing IP addresses easy and understandable.



eMailTrackerPro analyzes e-mail headers and identifies the IP address geographical region of the sender.

AOL subscriber would dial into the AOL network to venture out on the Internet and be assigned an IP address from the pool of IP addresses available to AOL. Once that IP address is assigned to the user, it comes out of the pool for the life of the session. If the user disconnects and then reconnects a short time later, chances are he will be assigned a different address. The key for investigators is that most IP address assignments are logged by the Internet service provider and kept for a limited period of time. Although the length of time varies from ISP to ISP -- some keep this information for days, others for months. Investigators need to act quickly.

In most instances though, all an investiga-

You simply cut and paste an entire e-mail header and the software will do the rest. The software will determine the IP address of the system from which an e-mail originated, and the source location will be displayed graphically on a world map.

When used with VisualRoute, an optional integration product, eMailTrackerPro can provide enough information to file a subpoena and ultimately identify a user. Although a separate program, VisualRoute integrates almost seamlessly with eMailTrackerPro. By using VisualRoute, a user can quickly and easily access the information for the ISP from which the e-mail originated. Those familiar with computer technology will recognize the integration of several popular tools into VisualRoute. The program combines the "ping," "whois," "traceroute" and "reverse DNS" utilities into one package.

"Ping" is a utility used to determine if a specific IP address is available and accessible. It works by transmitting a packet of data across the network (in this case the Internet) to a specified IP address or domain name and then waits for a reply. It assures that the address is up and running.

In understanding the "reverse DNS" it is important to realize that domain names, such as "microsoft.com" or "nytimes.com," are actually IP addresses (numbers) but are translated into names by a utility known as "domain name server" (DNS). Having to remember the domain name is much easier than having to remember the IP address for a particular Web site or e-mail address, hence the need for translation. When investigating the origin of an e-mail, the reverse needs to happen: An IP address needs to be translated into a domain name. The "reverse DNS" utility accomplishes this task. However, having the domain name alone is not enough.

The "whois" utility is then used to get registration information about an IP address or a domain name. It will provide the name, address and contact information of the domain's owner. From an investigative standpoint, it usually provides the location to send the subpoena.

In the past, investigators typically ran each utility separately and then combined the results to determine the sender of an e-mail. Now VisualRoute has brought it all together into one neat package that is easy to understand and follow.

In understanding the "reverse DNS" it is important to realize that domain names, such as "microsoft.com" or "nytimes.com," are actually IP addresses.

Sgt. George Welch of the Jefferson County Sheriff's Department in Kansas used eMailTrackerPro to help locate a missing girl. On June 5 the Jefferson County Sheriff's Department received a report from a worried mother who explained that her daughter had run away. Although the runaway 15-year-old girl left several notes outlining a plan to start a new life in Texas with an older boyfriend, both family and investigators lacked specifics. They essentially had no idea where she had gone. Interviews with the girl's friends also revealed her plans to go to Texas, but again lacked specifics. In essence, investigators were without a lead. Then on June 10, five days after the girl's disappearance, her mother received an e-mail from an unfamiliar Yahoo address. This is when Welch got involved.

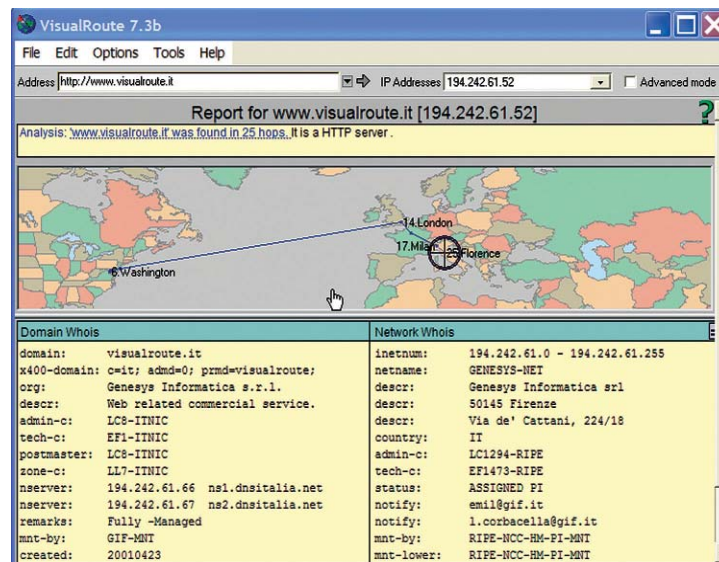
Welch, a 15-year veteran of the Jefferson County Sheriff's Department, serves as one of

Safety. Rose responded to the job service center and was happy to report that users of the Internet there were required to register. A quick check of the center's database revealed a name and address of the sender. Shortly thereafter, the runaway girl was in the custody of law enforcement and ultimately returned to the safety of her family.

Welch is quick to point out that he was not the hero in this case. Rather, he explained, it was the combined effort of many talented police officers. "A whole lot of people did what was right and acted quickly here, and that's why we got her back," states Welch. He also gives credit to the help he received from eMailTrackerPro and VisualRoute. "Using these programs certainly got this done quickly," Welch says.

Of course no one utility or software program is the panacea for conducting computer investigations, but Visualware's programs can make investigations easier. Combined with good police work and verification of the results, eMailTrackerPro and VisualRoute can save an investigator both time and effort. Detectives don't have to rely on computer specialists in the early stages of an investigation. Because of the ability to hide or "spoof" IP addresses, detectives should always verify their results with an expert but they can begin their inquiry into the origin of an e-mail and get just short of a full identification quickly.

Lastly, eMailTrackerPro and VisualRoute can also aid in the prosecution of the case. A presentation utilizing the software can be presented to the attorney prosecuting the case to aid understanding. The attorney in turn can present it to the jury to get them to understand -- and hopefully convict.



VisualRoute traces IP addresses to their city and country location, and identifies the network providing Internet access for the IP.

the agency's computer crime specialists. He utilized both eMailTrackerPro and VisualRoute to track the origin of the e-mail. Within a very short time, the e-mail was pinpointed as being sent from a job service center in Utah. Welch then coordinated with Det. David Rose of the Utah Department of Public

Andrew Donofrio is a detective sergeant, serving as a general case investigator for a municipal police department in Bergen County New Jersey. He serves on countywide task forces for computer crime and arson. He is schooled in many areas of forensic science. He can be reached at drewdonofrio@optonline.net.