Chapter 8
Investigations on the Web:
Examining Online Investigations and Sting Operations

Chapter Outline

I. Introduction
   A. Some technology-assisted crimes require little, if any, physical contact with the victim.
      1. Victimization occurs via the Internet.
      2. Locating and tracking an offender can sometimes be extremely difficult.
      3. Law enforcement will begin its search of these types of crimes on the Internet.

II. Locating a Suspect on the Internet
   A. How the Internet is accessed
      1. Individuals are not actually connecting directly into the Internet, nor are they connecting directly into the World Wide Web.
      2. They are connecting into their Internet Service Provider (ISP), the company that provides Internet and e-mail services for a monthly fee.
      3. When a person dials into or connects to the system, the ISP provides the customer access to the Internet and the World Wide Web.
      4. In order to confirm that the customer does not exceed their allotted monthly usage and to maintain records for billing purposes, each customer is assigned a temporary Internet address—known as an Internet Protocol (IP) address—that allows the ISP to locate the customer while he or she is online.
   B. Internet Protocol (IP) Addresses
      1. The IP address is the principle means by which later discussions on tracking a suspect will focus.
      2. Multiple persons can use the same IP address.
      3. Although each computer is provided a unique IP address by their ISP, this does not mean that the customer keeps that IP address throughout their contract with the provider; this is due to the limited number of IP addresses available for use.
      4. When a customer connects to their ISP, they are assigned an IP address that may or may not be one they have used in the past.
         a. The process of constantly reassigning IP addresses upon each connection by the customer is known as dynamic IP addressing.
      5. Each time the IP address is assigned to a customer, the ISP's computers monitor which customer has been granted the IP address, how long they maintain the address, and from where they have accessed the ISP's service.
         b. These records can be used by law enforcement investigators to locate a subject.
      6. Not all IP addresses are dynamic in nature.
         a. Some companies and universities have purchased blocks of IP addresses that they use on a regular basis.
         b. Computers on the network may keep the same IP address to simplify networking
         c. IP addresses that do not change each time they are accessed are referred to as static IP addresses.

7. There is a third form of IP address that is used today; it is referred to as sticky IP, which is a mix of dynamic and static, and is most commonly encountered by individuals who use cable modems.

a. May remain the same until the user or the provider (cable company, etc.) resets the connection or disconnects the connection for a period of time.

C. Finding who "owns" a given IP address at a given time

1. Locate the IP address.

a. The IP address normally appears in the following format and is referred to as IPv4: ###.##.##.##.

i. There is a new IP address format referred to as IPv6 (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, with each x representing a hexadecimal value) being used because the availability of IPv4 IP addresses is slowly coming to an end.

b. Depending upon the operating system that a person is using, a computer's IP address can be located using a series of keystrokes, or by clicking on an icon associated with the computer's network settings.

c. Even if an investigator does not have direct access to a machine that has been used in a criminal act, it is still possible to locate a computer's IP address.

2. Determine who owns the IP address.

a. To prevent two separate companies from attempting to license out the same IP address, each IP address in use must be registered by a company or individual.

3. Conduct a query.

a. There are several international registration agencies and the database detailing available addresses is linked together.

b. An Internet registry aids in determining who owns an IP address so that the actual user can be identified through the ISP's computer records.

c. There are several ways of accessing an Internet registry, but two of the more common methods involve the use of websites (www.arin.net and www.samspade.org) that allow you to query the IP address involved in an incident.

III. Locating Information from E-mails

A. The process of identifying an e-mail's owner is similar to that of identifying a user on the Internet; one must locate the sender's IP address and then conduct a query.

B. Locate the IP address within an e-mail.

1. When a person addresses an e-mail, the recipient's e-mail address is inserted into the "to" line on the form.

a. Address: screenname@ISP.com

2. When the sender clicks the send button, the e-mail message is routed to the ISP designated after the "@" sign.

a. Message does not move directly to the intended recipient's ISP

b. It is delivered to multiple computers on its way to the intended recipient.

c. Each computer that receives a copy of the message retains a copy of the e-mail to ensure that the message will reach its intended recipient.

d. If the original message is lost during transmission, then the last computer to handle the e-mail will communicate with the next computer and resend the e-mail message if necessary.

i. This process benefits law enforcement in tracing electronic communications because investigators can reverse track the message through other computers if the final computer cannot be located or does not have a copy of the message.

3. Tracing an electronic message

a. Every e-mail message has a header section that contains information relating to the path the e-mail took on its route to the intended recipient.

i. Initially this header was included in the text portion of the e-mail, but today, it has been removed.

ii. With the header no longer prominently displayed in the text, it is not uncommon for a victim to bring in a copy of a harassing e-mail without this header information, which hinders the investigation due to lack of evidence.

iii. The header is removed by default, but can normally be easily revealed to a user because web-based programs provide various methods for users to see the full e-mail message.

iv. It is important that investigators practice locating the header information in several different e-mail utilities and to understand that many victims might not know how to locate this information.

b. Examining an e-mail header

i. When some people first examine an e-mail header, they lose hope because it appears to be a collection of computer gibberish meant to be read only by a computer.

ii. Three sections of an e-mail header

1. Section A—Return Path Information

a. Tells who the e-mail was originally sent from, or at least who the e-mail server thought the e-mail was from.

2. Section B—Routing Information

a. Listing of every computer that the e-mail message has passed through on its way to its intended recipient.

b. Can be used to get IP address and once the IP address is obtained, then the investigator can begin the process of applying for a subpoena, a court order, or a search warrant to obtain information on the user who sent the message.

3. Section C—Identification Information

a. Provides the date and time the message was sent from the suspect computer.

b. Also contains the message ID.

V. Online Investigations: Proactive versus Reactive

A. The level of narcotics distribution via the Internet is relatively small when compared to crimes such as identity theft, digital child pornography, and cyberstalking.

B. Cyberstalking and identity theft are almost always handled in a reactive manner because a victim's complaint is necessary in order to begin an investigation.

C. Digital child pornography has become such a widespread problem that many agencies have begun employing proactive investigations in attempts to control the problems that develop from this activity.

1. Federal law enforcement, small municipal and state law enforcement agencies, and private organizations may attempt to locate individuals collecting and distributing child pornography by spending time on the Internet under the guise of being a child or potential victim for the pedophile offender.

2. A screen profile is generated for the officer that indicates he or she is a child of anywhere from six to 14 years of age.

3. The decoy spends time chatting and interacting with others in the chat room in hopes of luring out a potential groomer.

4. The officer will continuously chat with various other chat room members until the potential offender (who creates his or her own profile that appeals to young children) initializes contact.

5. The officer will then continue talking with the potential groomer, a term given to one who prepares children for physical sexual relationships, until a case has been established against the individual.

6. Once sufficient evidence has been collected, then an arrest warrant is issued for the offender.

7. Discovering offender's ID

a. During conversations the offender's name may be revealed

i. This is rare because individuals who solicit children are often not willing to reveal their true identities to anyone out of fear of being caught.

b. An actual face-to-face meeting is between offender and undercover officer is arranged by the offender

i. Upon arrival, the offender is arrested and charged.

ii. Method is commonly employed by agencies and requires the least amount of technological skill.

c. Identifying an offender—tracking an IP address

i. If there is an exchange of e-mails and instant messages, these communications may be used to locate a suspect's IP address, leading to identification of the offender and an eventual arrest.

ii. This method is the most technologically challenging, but it may be used in cases where the offender suspects something is wrong and breaks off contact.

8. Problems with these investigations

a. Training and technological skill

i. Use of computer or Internet

ii. Online investigations

iii. Culture of online world (language and mannerisms)

iv. Legal considerations and the proper methods of preserving evidence

b. Legal issues associated with conducting an online undercover investigation

i. Major issue is that of avoiding a scenario in which a suspect could argue that he or she was entrapped.

ii. *Sorrells v. United States* (1932)—for entrapment to be claimed, there must proof that the law enforcement officer encouraged the individual to commit the crime and that absent the officer's urgings the defendant would not have been predisposed to commit the crime.

iii. There are software programs today that can help an agency that desires to record its online investigation activity.

9. The "Dateline" Phenomenon

a. In 2004, Chris Hansen, a correspondent for NBC television, partnered with a volunteer organization called Perverted Justice to develop and film a "Dateline" special called "To Catch a Predator."

b. Perverted Justice's volunteers used the Internet to find men who sought to engage in sexual relationships with minors. Then, along with NBC and Hansen, a meeting was set up. When the individual arrived at the meeting, Hansen would be there asking them questions about their behavior. Earlier episodes also involved the presence of police.

c. The show was cancelled in 2007 after an incident in Texas in late 2006 led to Louis Conradt, a district attorney from a nearby town, committing suicide when the "Dateline" camera crew went with police to the suspect's residence to execute an arrest warrant.

i. Conradt's family later filed a lawsuit against NBC claiming that the show caused them extreme emotional distress and was negligent in the activities that led to Conradt shooting himself.

ii. "Dateline," NBC, and Perverted Justice all denied any negligence, but the lawsuit was settled out of court and the "Dateline" specials were halted.

d. The "Dateline phenomenon" is important to consider, however, as it brought sting operations to the forefront of Internet safety discussions and made more people aware of the dangers of pedophiles online.

Key Terms

Dynamic IP addressing: Process of constantly reassigning IP addresses upon each connection by the customer.

E-mail header: Section of the e-mail message that contains information relating to the path the message took on its route to the intended recipient.

Internet networking: The connection of computers from around the world.

Internet Protocol (IP) address: A temporary Internet address that allows the ISP to locate customers while they are online.

Internet Service Provider (ISP): The company that provides Internet and e-mail services, usually for a monthly fee.

Intranet networking: The connection of computers within the same organization.

Message ID: The identification information generated by the mail server when the message is sent.

Static IP address: An IP address that does not change each time it is accessed.

Sticky IP: An address that remains the same until the user or the provider resets the connection or disconnects the connections for a period of time.