Chapter 8

Conducting Cyber Investigations

Solutions in the chapter:

- **Demystifying Computer/Cyber Crime**
- **Understanding IP Addresses**
- **The Explosion of Networking**
- **The Explosion of Wireless Networks**
- **Interpersonal Communication**

- ☑ **Summary**
- ☑ **Solutions Fast Track**
- ☑ **Frequently Asked Questions**

Introduction

We often fear most what we don't understand. That could be said about computers and the investigation of computer crimes. Many investigators cringe at the mention of a computer and seek to offload any computer-related crime to the "computer crime guy" in their office. Although computers have been around for a few decades, they've finally reached levels where it is feasible to expect that everyone has access to a computer. The computer is no longer a "nice to have," it is a "must have." Those who don't own their own computers can walk into a public library or cyber cafe to gain access to a computer. Similarly, access to the Internet is becoming ubiquitous through connections provided by libraries, coffee shops, computer stores, and even fast food restaurants. This explosion of computer technology and acceptance has opened up a whole new world of opportunity to the criminal element that constantly looks for new ways to exploit people through time proven scams and tactics. As computers become more deeply integrated within society, it is likely that a computer or similar type device will play a role in criminal activity. A basic understanding of computers is all that investigators will need to learn that *computer crime* is just plain old crime packaged up in a shiny new wrapper.

Demystifying Computer/Cyber Crime

Computers start to play a role in crime in situations where the capabilities of the computer allow a person to commit that crime or store information related to the crime. An e-mail phishing scam is a common example where the bad guy generates a fictitious e-mail for the sole purpose of enticing people to a spoofed site where they are conned into entering sensitive personal information. That sensitive information is then available to the bad guy in order to perpetrate an Identity Theft. In another example, a suspect might use the computer to scan and generate fake bank checks, or create fake identification. In both of these cases the crime required the inherent capabilities of the computer for its commission.

WARNING

The mere presence of a computer does not make a crime a computer crime. We must be careful not to hastily label a crime a "computer crime" just because a computer was involved. What if the new laptop I purchased was stolen from my vehicle while I was in the convenience store getting milk? This would not be a computer crime just because a computer was involved, but a theft. How about an office fight where an employee strikes another with the keyboard of their computer—should we call out the Forensic team? Absolutely not (well, maybe, if the assault resulted in a homicide). The computer in and of itself is not important, it is just merely an object like many others in our lives.

Since computers are so pervasive, it is an absolute necessity that investigators learn how to investigate crimes that involve a computer. The basic design of computers—including vast amounts of storage and meticulous file time-tamping—can make them a wealth of evidence as traces of the crime can often be retrieved by an experienced investigator. This does not mean that every investigator needs to become an expert in computer technology, but there are basic concepts and methods that must be learned in order to develop old school leads. *The key is to gain at least some basic computer knowledge and skills to put you ahead of the average computer user*; *skills that allow you to apply traditional policing skills and procedures to the case.*

The crimes that are being committed haven't changed, just the manner in which they're being committed. Think about it. Back before the Internet, the telephone, the telegraph, and the Pony Express, if a person wanted to threaten to kill someone, it was likely they would have to physically place themselves in proximity to the person and speak that threat. As services and technologies developed, new ways emerged through which a person could commit that same threatening act. They could send a letter, a telegram, or even better, make a phone call. Now we can send an e-mail or instant message (IM). Same crime; same underlying elements and facts to be proven. The only change is the manner of delivery. The key to a successful investigation of a computer crime is the development and follow-up of case leads. Although many leads will dead end, it is the one that continues to develop into further leads that can end up solving your case. Many believe that investigations involving com-

puters are above their capabilities, but that is often not the case. By learning and adapting some basic computer knowledge and skills, today's investigator can react to new technologies and still develop workable old school leads.

NOTE

IM stands for instant message. Instant messaging is another way for people to communicate with each other by computer in real time. A chat session is established between two or more computers using compatible applications through which written messages and files can be transmitted back and forth. The unique challenge of instant messages is that their content is not often recorded by service providers or the applications facilitating the chat. Once the IM session closes, the contents tend to be lost. This is not always the case as users can turn on chat logging, but by default most chat applications do not record sessions.

Throughout this chapter, critical skills will be discussed that prepare an investigator to deal with computer crime investigations. By developing a basic understanding of key concepts and learning to apply basic computer skills, an investigator can learn how to proceed with computer crime cases much in the same way as traditional cases. Issues such as IP Addresses, Networks, Wireless Devices, and Interpersonal Communication will be discussed with the sole purpose of providing the investigator with a basic understanding of each topic area and the skills that can be employed to yield workable physical leads. Many of these skills will build the foundation of computer crime investigations not only today, but well into the future as these technologies expand and become more complex.

Notes from the Underground…

"Application Stupid"

Even though computers have been in our society for quite some time, it is still arguable that many within the population are not highly skilled with them. With the prevalence of computers today, it becomes increasingly important for computer and software companies to develop systems and applications that are "user friendly." These user friendly devices and systems are intended to make people's lives easier. People, being creatures of habit, are often quick to embrace any solution that will allow them to work less. This has facilitated the rapid acceptance and integration of complicated systems into everyday life.

In the quest to make applications and operating systems easier for the end user, programmers have had to develop very advanced and complicated programs. There is a direct correlation between the ease of use by the end user compared to the complexity of the underlying code that is required for the application to run. Many operating systems today are so advanced compared to their earlier versions that little interaction is required of the end user to install new programs or add peripherals. The system itself is able to identify new devices or programs, load the necessary supporting drivers, and set parameters to make the new device or program function. All this is done for the benefit of the end user, who is no longer required to have a fundamental understanding about how the computer and/or its software functions.

A large majority of people are what I call "application stupid"; the process of using a computer or application is so simplified that the user is not required to possess any enhanced level of computer skill or knowledge. The user is able to operate the computer, sometimes at a fairly high level, without having any understanding about what is going on in the background. Application stupidity can provide an opportunity to the investigator to obtain traces of information or evidence that has been left behind as a result of the complexity of the application or operating system versus the rudimentary skill of the user. For example, a suspect creates a file on their computer that is incriminating in nature, they delete it, and then they empty their recycle bin. They believe that the file no longer exists—which is not the case. Their

Continued

limited knowledge about how operating systems handle deleted files has created an opportunity for the investigator to retrieve the deleted file.

The simpler the program is to the end user, the more complex the coding; the more complex the coding, the more likely that fragments of information will be left behind. The theory of application stupidity is likely to become more pervasive as the complexity of operating systems and programs increase to keep pace with a growing user base that demands simplicity.

Understanding IP Addresses

All law enforcement investigators need to understand the basics of IP addressing in order to trace users of the Internet to a physical location. Just as a phone number that shows up on a caller id box from a threatening phone call can provide investigators with a specific starting location for their investigations, an IP address can provide that same type of lead. By understanding what IP addresses are, how they're assigned, and who has control over them, an investigator can develop workable case leads.

IP addresses provide a connection point through which communication can occur between two computers. Without getting into too much detail about them, it is important that you understand how to identify an IP address when you see one. These addresses are made up of four 8-bit numbers divided by a ".", much like this one: 155.212.56.73. Currently the Internet operates under the IPv4 (Internet Protocol Version 4) standard. In IPv4 there are approximately 4 billion IP addresses available for use over the Internet. That number will be expanding in the near future to about 16 billion times that number when transition is made to IPv6.

During the birth and initial development of today's Internet, IP addresses primarily were assigned to computers in order for them to pass network traffic over the Internet. Computers were physically very large, extremely expensive, and pretty much limited to the organizations that controlled the primary networks that were part of the primordial Internet. During this time, an IP address most likely could be traced back to a specific computer. There are a limited number of large organizations that own and control most of the

IP Addresses available with IPv4. Therefore, if an investigator has been able to ascertain the IP address of an illegal communication, they will also be able to determine which organization owns the network space within which that address is contained. That information in and of itself will often not be enough since many of these organizations sublease blocks of the IP Addresses they own to smaller companies, such as Internet Service Providers (ISP). It will be the investigative follow-up with the ISP that is likely to provide the best results. Using an analogy, we can think about IP addresses much like phone numbers, where the major corporations are states and ISPs are towns or calling districts. If an investigator was following up on a case involving a phone number, the area code would narrow the search down only to a particular state, and the remaining numbers would identify a particular account.

Remember that for Internet traffic to occur, an external IP address must be available to the device. Access to an external IP address is provided by an ISP. ISPs sublease blocks of IP addresses from one or more of the larger corporations that control address space and in return they will in essence sublease one of those addresses to the individual customer. This connection to the Internet is most often done through a modem. Modems came in varying configurations such as dial up, cable, and DSL. Depending on at what point in time you began using the Internet, you may already be familiar with these devices. The older of the three listed is the dial-up modem that required the use of a telephone line. When users wanted to connect to the Internet, they would plug the modem installed in their computer to their phone line and then dial one of the access numbers provided by the ISP. The dial-up modem is the slowest of the available devices that can make the transfer of large files a painful process. Therefore when dealing with cases that require large file transfers such as child pornography, it is less likely that a dial-up connection would be used. A distinct advantage of the dial-up modem, though, is the portability since the connection can be made on any phone line by dialing an appropriate access number and providing valid account information.

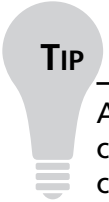
More common today is Internet service provided through TV cable or through DSL (Digital Subscriber Line); both of these services provide higher connection speeds making the transfer of large files relatively easy. When a consumer contacts an ISP about Internet access, typically they are assigned an installation date when a technician comes to the residence to connect the

necessary wiring to the home through either their cable provider (cable modem) or phone provider (DSL). With the appropriate wiring in place, an external modem is connected to the line provided through which the computer in the home will connect. The modem provides the interface through which the home computer can be physically connected to the Internet.

When the home user is connected to the ISP's physical connection to the Internet, the ISP must still assign the home user's computer an IP address in order for the computer to communicate over the Internet. IP addresses are assigned two ways, statically and dynamically. If static addressing was to be used, the install technician would configure the computer's network interface card (NIC) with the specific IP address during install. Static assignment by an ISP would limit the total number of customers an ISP could have by the total number of external addresses they control. Let's say that XYZ ISP had subleased a block of IP addresses from a large corporation in the amount of 1,000 unique valid addresses. If that ISP statically assigned addresses to their customers, then the total number of customers they could have on the Internet would be limited to 1,000. Leasing blocks of external IP addresses is very expensive as the demand is high compared to availability. ISPs realize that it is unlikely that all their customers will be on the Internet at the same time, so in order get the largest return on their investment, they use an addressing scheme called dynamic addressing, which allows for computers that are actively connected to the Internet to be assigned an unused IP address.

Here's how dynamic addressing works. XYZ ISP has 1,000 addresses available to their customers. They set up a server, referred to as DHCP server, which maintains a list of the available addresses. At installation, the technician sets the consumer's computer NIC to get an address assignment through DHCP. When the consumer's computer is turned on and connected to the network, the NIC puts out a broadcast requesting an IP address assignment. The DHCP server responsible for the assignment responds to the request by providing an IP address from the pool of available addresses to the computer's NIC. The length of time that the computer will use that assigned address is based upon the "lease" time set by the DHCP server. Remember that the ISP wants to have the maximum number of customers using the smallest number of addresses, so the ISP wants to ensure that any unused addresses are made available to other computers. The lease time determines how long that address

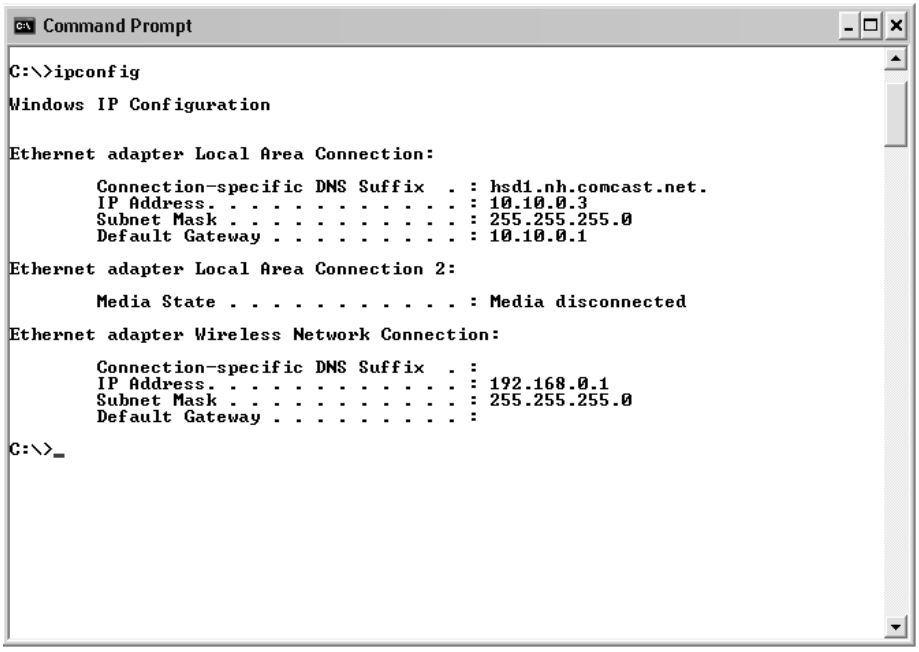
will used before the NIC will be required to send out another broadcast for an IP address. The IP address returned after the reassignment could be the same address used previously or an entirely new address, depending on what's available in the server pool.



TIP

A number of details about the configuration of a computer's NIC(s) can be determined in Windows by using the `ipconfig` command at the computers command prompt—most importantly the computer's IP Address (see Figure 8.1).

Figure 8.1 *ipconfig* Command



Note that this example provides details on three different NICs; two physical Ethernet ports identified by the Local Area Connection designation and one wireless network connection. Each NIC can possess a different IP address. IP addresses are important because each device that communicates

over the Internet must have an address. In a computer crime investigation involving the Internet, it is very likely that the investigator will need to track an IP address to a location—preferably a person. As discussed earlier, ISPs control the assignment of IP addresses, and ISPs can provide the link between the IP address and the account holder. Understanding the distinction between static and dynamic IP assignment is very important because the investigator must record the date/time that IP address was captured. If the ISP uses DHCP, the IP address assignments can change—investigators need to be sure that the account holder identified by the ISP was actually assigned the IP address in question when the illicit activity occurred.

Let's take a moment and think about this. You're investigating an e-mail-based criminal threatening case where you were able to determine the originating IP address of the illegal communication. You were able to determine which ISP controls the address space that includes the IP address in question. If ISPs use dynamic addressing, how are you going to be able to determine which subscriber account used that address if any of a thousand or more could have been assigned to the suspect's computer? In this case, it would be extremely important for you to also record and note the date and time of the originating communication. The date/time stamp can be matched against the logs for the DHCP server to determine which subscriber account was assigned the IP address in question at that time.

The Explosion of Networking

Much like ISPs use dynamic addressing to maximize the number of customers they could have using a limited number of addresses, customers began using routers to increase the number of computers they could use in their homes that could share that IP address provided by the ISP. The router passes network traffic back and forth between the Internet and all the home computers in the residence connected to that network router. All the network traffic sent from the home computers through the router to the Internet will be seen as coming from a single IP address. The investigator who traces an IP address back to a router will need to do more case follow-up at the location to determine if there is more than one possible computer involved. Analysis of the router configuration and/or logs may provide more information about the

computer requesting and receiving the illegal traffic as information, such as the computer's hostname, internal IP address, or MAC address.

Networks have become common place today as the cost and implementation of computer systems has dropped dramatically. Years ago, computer systems were very large (room size) and extremely expensive. This limited the organizations that could afford to use computers in any meaningful way. Today, computers are much more powerful and affordable. This has allowed both companies and individuals to purchase and use numerous computer systems to accomplish specific needs. The concept of networks, much like the Internet, allows multiple computers to become interconnected to each other in order to share files and resources. The computers on the network will still need to be assigned IP addresses in order to communicate with other computers on the network—but the addresses assigned within a network behind a router, *or gateway*, will fall into the category of internal IP addresses. Unlike the external address assignments required to send and received information on the Internet, internal IP addresses allow computers within a network to communicate with one another. In order for computers on these private networks to access the Internet, there is likely to be an established gateway that has been assigned a single external IP address to be used by all computers on the network.

NOTE

Internal IP addresses can also be used to set up more than one computer into a network environment. When computers are placed within a network, they will be able to see the existence of each other on the network and can be used to pass communications and share files. This is completely independent and not reliant upon having access to the Internet. However, without some type of Internet access, the communications transmitted over that internal network (most often referred to as a private network) would remain within that network and would not be accessible to other computers not physically included in its scheme. Private networks are very common in corporate environments where large numbers of employees need to access or share files with other employees, but for security purposes, no Internet connection is included in order to stop possible unauthorized access from outside the network.

Gateways become a transfer agent for computer traffic between computers on the network and the Internet. This means that the network owner is only required to assign a single external IP address to the gateway in order for one or hundreds of the computers on the network to access the Internet. This provides a challenge to investigators who have been able to trace back that IP address to the gateway owner. The IP address no longer identifies a specific computer directly, but merely identifies the gateway that handed the traffic on to the Internet on behalf of all the computers on the private network. More follow-up must be performed in order to establish the identity of the system that sent the request to the gateway initially.

A benefit of investigating a traditional wired network is that the number of devices connected often is limited to the location at hand and physical limitations of transmission over wired lines. Being able to trace an IP address back to a particular location and network greatly helps reduce the total overall number of suspects. If other identifying information such as the internal IP address, hostname, and MAC address has been determined, then the ability to narrow the suspect down to a single device is greatly increased. If the device is found, then traditional investigatory techniques can be used.

Hostname

Hostnames are the system names assigned to a computer by the system user or owner. These names are used to identify a computer in a network in a format that is easiest to understand by people. If there are multiple computers in the network, each could be given unique identifying names making them more easily recognizable, such as Receptionist PC or Dave's Laptop. The naming choice selected might help to identify the likely location or user of that system. If for example you were investigating a threatening e-mail that had originated from a computer within a network named "Jedi," you might look for people who have access to the network who are also fans of the *Star Wars* series. Keeping in mind that the names can be changed by the user at any time, the matching or nonmatching of a hostname to a suspicious communication or activity is by no means conclusive in itself.

MAC Address

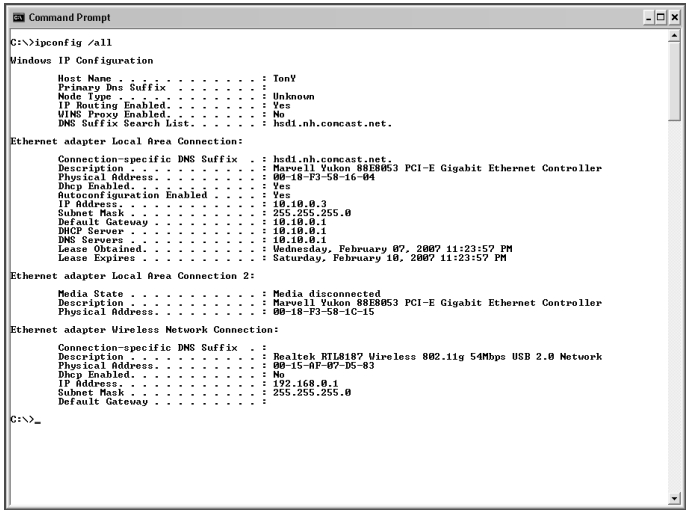
MAC addresses are the identifying number assignment given to NICs that provide network connectivity. That connectivity can be wired or wireless depending on the type of NIC present. MAC addresses are unique to every NIC and would be most equivalent to a serial number. This means that if an investigator is able to determine the MAC address of the device used in the crime, then the device containing the NIC could be identified specifically. However, just like a hostname can be changed, MAC addresses can also be changed through a process called MAC spoofing. Whether or not a MAC address matches a particular communication is not in itself conclusive evidence that the computer containing the NIC was or was not responsible.

TIP

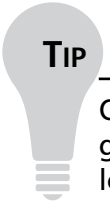
In the previous Tip we learned that the *ipconfig* command can provide some details about a computer's network interface card configuration. There is a switch that can be added to the *ipconfig* command that provides more detail about the NIC configuration. At the command prompt, *ipconfig /all* is used (see Figure 8.2).

You will notice that other details have been provided that are not seen in the *ipconfig* command, including the computer's hostname, and each of the NIC's MAC addresses.

Figure 8.2 *ipconfig/all* Command



Being able to determine the computer's MAC address is a useful skill for investigators. At one organization, network security had set alerts in their system to notify the system administrator when MAC addresses of stolen equipment appeared on the network. The systems administrator notified law enforcement that a stolen laptop had just connected to one of the organization's wireless access points, and they were able to direct the officer to the general area in range of the given access point. The officer was able to make a directed patrol of the area looking for anyone using a laptop that matched the general description of the stolen laptop. Unfortunately the officer was not aware of the `ipconfig/all` command. Knowing that command would have allowed the officer to conduct field interviews and request consented permission to check the MAC address of any of the suspected laptops against the recorded MAC address of the stolen laptop.



TIP

Once investigators have narrowed the scope of their network investigation down to one computer, they may want to consider the following lines of questioning:

- Who has access to the device?
- Did they have access on the date and time in question?
- Did they have motive?
- Is there evidence still on the device that can be retrieved?
- What information does the suspect provide?

The Explosion of Wireless Networks

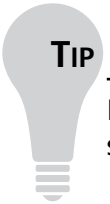
In the not too distant past, networks were isolated to corporate and government entities using large computer clusters and a wired infrastructure. It was less common to find homes with a computer; much less a network. All of that changed with the advent of wireless technology. Many homes and consumer establishments contain private and/or open networks providing access to the Internet, network devices, or offline storage. Cellular companies also compete within the wireless space and offer numerous Internet-enabled devices that allow consumers to stay connected. This proliferation of interconnected and

overlapping wireless networks allows criminals to be more portable, creating a heightened challenge to law enforcement to first locate the origin of the action or communication.

Hotspots

Hotspots refer to locations where wireless Internet services are readily available to any user. Some are fee-based and others are offered as a free service to attract customers. In the fee-based system, the person connecting to the network is required to submit valid payment information prior to being granted access. As a service to attract customers into their establishments, many businesses now offer free Internet. This means that anybody entering the establishment, or within range of their wireless signal, can utilize their network to gain access to the Internet. These free hotspots can pose a significant problem for law enforcement since an IP address traced back to any establishment that is set up as a free network is likely to leave the investigator with a large suspect pool—basically anyone within range of the network.

In these situations, the timestamp of the illegal or suspicious activity continues to be critical to the investigation. Knowing the date and time of the alleged incident would allow you to narrow down the pool of possible suspects. A pattern of illegal activity from the address might help build a profile of the offender sufficient enough to jog the memory of employees about a "regular" who visits the location during those time frames. Of course, be careful not to exclude employees in the pool of possibilities unless they can be eliminated based on work assignments and schedule. Tracing back the IP address will provide only a lead toward where the investigator should look further. It will be traditional investigative skills that will help yield a possible suspect. Understanding IP addresses, hostnames, and MAC address assignments will be crucial to matching your suspect's device to the router configuration and/or traffic logs.



TIP

Investigators working cases involving wireless networks should consider the following lines of inquiry:

Do the employees remember anything unusual during those time periods?

Is the establishment equipped with video cameras and is there footage of the time period in question?

Does the investigator have a possible suspect photo, sketch, or other information that might help in the follow-up?

Does the router providing the service maintain activity logs? If so, what was the computer name and MAC address of the device that perpetrated the activity in question?

Wardriving

As people learn to appreciate and utilize new technologies, they can inadvertently open themselves up to an opportunist who prays on that innocent lack of understanding. Wireless technology is a perfect example. People have longed for the day when they wouldn't be forced to sit at the same desk or location in their home or office to use a computer, but could move about freely without the constraint of wires. Laptop devices have evolved to the point that they are lighter, more portable than, and just as efficient as full-size desktop computers. Most now come equipped with a wireless card as a standard device, which means that the only new device needed to achieve true portability at home or office is the installation of a wireless router.

Wireless routers are so inexpensive and easy to set up that many homes and offices are now wireless enabled. Many wireless routers come with installation CDs that automate the entire process using default settings that will work with most devices. This means that within a few quick steps of returning home with this device, the average person can have a fully functional wireless network established that will communicate with the wireless-enabled laptop they already own. Using the old adage "if it works don't fix it." many will make no attempt to secure that network from outside intrusion. They will not be aware that they have just created an open wireless network that is available to anyone within the wireless signal range.

There are those that drive through neighborhoods looking for the presence of open, unsecured wireless networks. This process is referred to as *wardriving*, and requires no special equipment other than a wireless-enabled device that is capable of detecting wireless signals. Some will record the location of these networks for their own personal use, still others might post the locations on the Internet as part of a greater hotspot map for anyone to utilize. The types of crimes that can be perpetrated using one of these locations varies. First, the intruder may use the network only as free access to the Internet with no illegal intent other than nonpermissible use of that network and Internet account.

Some people may use this opportunity to scan the network, looking for devices within the network that have known vulnerabilities that they might be able to exploit in order get account and password information. This network could be used to send threatening e-mails, launch viruses, or transfer child pornography. An investigator who has been able to trace the IP address back to the home owner account would need to use some traditional policing skills, which might include interviewing residents, consented or warranted searches of Internet-enabled devices, and review of the wireless router's configuration and log files. Computer skills will lead the investigator to the location, but traditional police work will tie everything together.

Security Alert...

Investigating Wireless Networks

There are situations where a homeowner may contact an investigator about unauthorized access of his or her wireless network. Since most routers have the ability for logging and e-mail alerts about certain activity, an investigator with consent of the network owner could set the configuration of the system to generate log files and e-mail the investigator when suspicious activity is occurring. Remember that in order for a person to use the network, he or she would have to be within range of the signal. If an investigator knew the activity was occurring in real-time, he or she might be able to locate a suspect based

Continued

on activity in the neighborhood. What other houses appear to have activity?

Are there any suspicious people or vehicles in the area?

Since the range of the signal is typically a setting within the administrative function of the router, it would also be possible to lower the signal power, reducing the overall range of the network. This in turn may pull the suspect into closer proximity to the location, making them easier to locate. Recently, I recall an investigation where a neighborhood child was suspect of stealing a laptop from a residence. The network had been secured and would allow access only to that specific laptop, so logging was enabled with e-mail alerts to notify the investigator should any activity be initiated by that laptop. That type of activity alert would notify the investigator that the stolen laptop was in range of the network, which might yield a suspect with evidence in hand.

Wireless Storage Devices

In order to keep up with demand for wireless, many manufacturers now offer remote wireless storage devices, which could pose a significant challenge to investigators trying to locate illegal material. Within the range of a wireless network, a suspect could potentially hide a storage device in an area of their residence that is not readily accessible or apparent. This poses a significant challenge to investigators during consent and search warrant execution. Investigators must always be thinking about the possibility of a remote storage device, especially if it is determined that a wireless network is in use.

Certain limitations with these remote devices can be useful in determining their existence, ultimately helping to determine their location. Even with their portability, these devices will need some type of power source and persistent connectivity to the network. This can limit their proximity to the signal area of the device they typically associate with as well as power availability. When powered, these devices will connect wirelessly to the network they're configured to associate with. This means that if an investigator is able to gain access to the gateway device establishing the network, they might very easily identify that there is another associating wireless device that they have not accounted for. The real challenge comes when these devices are not powered. Without power these devices are off and will not associate with the

wireless devices, making them invisible to the entire network. Their discovery would have to come through physical observation at this point, rather then through their virtual presence.

If an investigator had the skills to recognize that a wireless network was in use within the suspect's residence, he or she might be more inclined to ask probing questions about that network, possibly getting the suspect to disclose the existence of a remote device. Physical searches of the residence could also be potentially more productive if the investigator has keyed in on the fact that there might be remote devices involved, requiring a more thorough and educated search.

Interpersonal Communication

As people look to stay connected with friends, family, and coworkers, they are likely to use one or more methods of communication, including e-mail, chat, and blogging—all of which are easily supported on today's computers and portable devices such as laptops, PDAs, and cellular phones. Investigators must be familiar with how these various systems work and how one might be able to retrieve critical case information from stored communications or fragments of previous exchanges. What makes the area of interpersonal communication so important to the investigator is that people are inherently very social; people routinely discuss their daily lives with friends and may even brag about crimes to others. Being able to capture, decipher, and trace back communications to their origin is a critical law enforcement skill.

E-mail

E-mail communication was present at the start of the Internet, and has exploded over the last decade, making it more likely that people today use e-mail in some form or another. E-mail provides another conduit through which people can communicate 24 hours a day, 7 days a week. Unlike a phone conversation that needs the recipient to answer, an active e-mail discussion can be carried out through multiple e-mails spread over time. Messages are sent and are held in a waiting inbox at the convenience of the recipient, who will choose when to read the message and how best to respond. Once an e-mail is read, it is usually up to the receiver to decide and

make the conscious choice to delete or discard that communication. This provides a unique opportunity to law enforcement investigating crimes involving e-mails, since undeleted e-mails will be viewable and previously deleted e-mails might be recovered through various forensic methods.

There are countless e-mail addresses and accounts in use today. They fall into two major category types. The first are e-mails generated with e-mail programs that reside on the local user's machine. One of the most common is Outlook or Outlook Express (a Microsoft product), which runs on the user's machine and can be set up with relative ease assuming the account holder has an active Internet connection. E-mails sent and received through this type of account will be stored locally on the user's machine. If this type of e-mail program is used to generate and send illegal communications, it is likely that evidence of those communications might be recovered from the machine used.

The other popular e-mail service is free Internet-based e-mail such as Microsoft's Hotmail and Google's Gmail. These services don't require users to have any special programs in order for them to send and retrieve e-mail in their account. They are able to access mail that is stored on servers provided by the provider they use by signing into a previously created account. These services are extremely portable since they can be accessed from any computer with Internet access and a web browser. With an Internet-based account, an e-mail might be traced back to the originating ISP and it may also be possible to determine the IP address of the machine that connected when the account was created. This is, of course, all dependent on whether the service provider maintained those records for any specific period of time. Even with this type of account, remnants of Web-based e-mail may be recoverable as HTML documents in temporary Internet files or drive space that hasn't been overwritten by newer files.

With all e-mail cases, it is critical that the investigator follows up on the e-mail address associated with the active case he or she is working. Since there are countless e-mail addresses in use on the Internet, it is not uncommon to have hundreds, if not thousands of variations for the same or similar address. John_Smith@domain is entirely different than JohnSmith@domain. Be sure to match all instances of your suspected e-mail communications exactly.

Chat/Instant Messaging

Chat and instant messaging is another extremely popular method of communication. Unlike e-mail, which ends up being loaded on an e-mail server or downloaded onto the receiver computer's local e-mail program, chats and instant messages are made through direct communication between the two devices. The devices involved exchange communications back and forth in real-time for as long as that "window" is open. Conversations held in chat are not saved by the applications typically used to facilitate this method of communication. This means that for the most part, chat and instant messaging conversations are lost once that session ends.

Service providers do not log chat and instant message traffic, which can be challenging to the investigator investigating a case where chat or instant messaging might have been used. Just like with e-mails, it is extremely important that investigators trace or follow up on the correct screen name or chat id being used by the suspect(s). There are still cases where an investigator might be able to retrieve chat history, as it is possible that one or all of the parties involved may have turn on logging within the application they use. Remnants of chats might also reside on drive space that has not been overwritten by new files. This is where forensic examination can come in very handy if a suspect computer has been seized.

Social Networking and Blogging

Social networking sites, such as Myspace and Facebook, and blogging technologies allow people a conduit through which they can post their thoughts, ideas, and self-expression onto the Internet instantly. For example, within Myspace, users can create an account for themselves along with a personal Web page through which they can express themselves in any manner in which they see fit, be it through music, video, or written expression. These pages become part of a larger online community with similarly minded individuals being able to link together into what is referred to as a *friends network*. Since the information entered at account creation has no true factual verification, it is possible for people to create fictitious identities in order to pass themselves off as someone they're not. The name an investigator might obtain from a Myspace created page might not be the actual identity of the person

who created and uses that space. However, it might still be possible to obtain information from the organization responsible for Myspace, such as an account holder's IP address information used during the original account creation or the IP addresses the account holder used to access the account—that type of IP information might be traced back to a suspected user account.

Even though there are no guarantees that information on Myspace pages will be completely factual, this type of online community provides a very powerful and unique service to law enforcement. If an investigator is able to positively identify an online identity as belonging to a specific suspect, the investigator might also be able to develop further leads about conspirators based on other identities contained in their friends network. It is critical to investigators that they monitor the activity of potential suspects that they identify by keeping up with the suspect's social networking and blog-related activity.

Media and Storage

Media exists in numerous configurations with varying storage capacities. Most people today are very familiar with the floppy disk, CD-ROM, and DVD—all of which can store and contain files of evidential value. DVDs started reaching capacity sizes in excess of 8 gigabytes, which meant that suspects could save illegal files that would have filled up an entire computer hard drive just years ago on one silver disk. Finding just the right DVD during a search of a suspect or residence could provide numerous evidentiary files. A smaller segment is likely to be familiar with hard drives and understand their role within the computer.

The trend now within media is that of portability. As if trying to find a CD or DVD wasn't hard enough, further technology advances have brought about flash drives and mini smart cards. Many flash drives are smaller than a pack of gum and some mini smart cards are the size of a postage stamp (only thicker) and are capable of holding gigabytes of information. Investigators must be aware of the different types of digital media that exist and be able to identify the media in the field. The variety, and more importantly the size, of media must be taken into consideration when applying for search warrants where digital evidence is suspected; the hiding places for this type of storage are countless.

Summary

What makes computer crime so fearful to some and intriguing to others is the unknown. As investigators learn to deal with and investigate crime involving computers, many are quick to label any crime with a computer presence as a computer/cyber crime. Many of these investigators, and prosecutors, believe that computer crimes are really new crimes; but criminals and "crime" have shown the ability time and time again to be able to adapt to new technologies. It is reasonable to question whether computer crime is just a generational phenomenon caused by a gap in computer understanding and acceptance by many older Americans that did not have the same opportunities to use and learn on computers as the younger generations. Is it likely that this problem will correct itself over time? In the future, computer crime, as it is viewed today, will become nonexistent—not because crime won't exist in the future, but because computer-related crimes will be viewed for what they really are, *crime*.

Solutions Fast Track

Demystifying Computer Crime

- ☑ The explosion of computer technology and acceptance has opened up a whole new world of opportunity to the criminal element that constantly looks for new ways to exploit people through time-proven scams and tactics.
- ☑ The key for investigators is to gain at least some basic computer knowledge and skills to put you ahead of the average computer user, skills that allow you to apply traditional policing skills and procedures to the case.
- ☑ There is a direct correlation between the ease of use by the end user compared to the complexity of the underlying code that is required for the application to run. The simpler the program is to the end user, the more complex the coding; the more complex the coding,

the more likely that fragments of information will be left behind. These fragments can be located by law enforcement during investigations.

Understanding IP Addresses

- ☑ All law enforcement investigators need to understand the basics of IP addressing in order to trace users of the Internet to a physical location.
- ☑ In a computer crime investigation involving the Internet, it is very likely that the investigator will need to track an IP address to a location—preferably a person.
- ☑ Investigators need to record the date and time that an IP address was captured to ensure the captured IP was actually assigned to the suspect identified—dynamic addressing can cause the assigned IP addresses to change.

The Explosion of Networking

- ☑ The investigator who traces an IP address back to a network will need to do more case follow-up at the location to determine if there is more than one possible computer involved.
- ☑ Hostnames and MAC addresses can be used as investigative tools to help identify a computer on a network.

The Explosion of Wireless Networks

- ☑ The proliferation of interconnected and overlapping wireless networks allows criminals to be more portable.
- ☑ The anonymity provided by free WiFi access in hotspots and stolen WiFi, that is, wardriving, highlights the importance of good police work to mitigate the impact of the technology on the investigation.

- ☑ Investigators need to consider that wireless storage devices will be used by suspects, and a plan to detect and find these devices must be part of the overall search planning.

Interpersonal Communication

- ☑ People are inherently social and routinely discuss their daily lives with friends and may even brag about crimes to others. Being able to capture, decipher and trace back communications to their origin is a critical law enforcement skill.

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form.

Q: I'm new to cyber crime, but I really want to get involved. Should I jump right into doing forensics?

A: Although there is plethora of training available in the field of digital forensics, you may want to consider getting acclimated to crimes with a cyber component before jumping in with both feet into forensics. Much of what is discussed in this chapter reflects the belief that most cyber crime is just plain ol' crime. Where we may hold this belief to help those that dislike technology realize that they can still work computer crime cases without having a thorough knowledge of computers, we may suggest the same train of thought to you; there is plenty of crime to investigate that has a cyber component that does not require a forensic examination. Tracing e-mail harassments, responding to threats over chat, and investigating sexual solicitations over IM are but a few of the types of crimes that can be investigated without immediately requiring a forensic exam. My recommendation is to find a training course that focuses on the investigation of Internet-related crime—the skills you learn in class such

as this won't be wasted if you choose to go the forensics route in the future. By the way, by focusing on crimes that you can investigate without requiring a forensic examination will make your chief a lot happier than your request to purchase $20,000 of software equipment to start processing forensics cases.

Q: I want to get involved with catching predators online. I've seen the TV shows and there doesn't appear to be anything to it. Why should I bother to learn all the technology junk if I don't need to?

A: This is a very popular question. Unfortunately, the fact that it gets asked shows that many people do not know what they do not know, and goes squarely to the heart of *application stupidity*. Agreed, there is little technical knowledge required to "chat" with a potential suspect, and if everything goes according to plan, they show up at your door and you take them into custody. But what happens when things don't go according to plan? Are you aware of the underlying software or process that makes the chatting possible? Is your machine configured correctly and appropriately protected—naming the computer DetectiveDesk22 may show up during a scan of your computer and may blow your cover. Are you knowledgeable about how the particular chatting software works? Does it use a proxy? Will it provide you a direct connection during a file transfer or webcam stream—and if yes, do you have the skills to capture the bad-guy's IP address during that exact moment of transfer? Do you have the skills to properly set up an online identity and protect it from discovery? Although the initial setup of the identity may be trivial, the long-term maintenance and believability of the profile may affect your investigations.

In principle, it sounds like a good idea to get a screen name together to begin enticing predators into the stationhouse, but obtaining basic computer investigative skills will go a long way toward conducting more successful and productive investigations. Further, these skills may prove critical one day when a predator shoots you a webcam image of a child held hostage—that exact moment is not the time to begin learning about the underlying technology—these skills need to be acquired and practiced before employed in active operations.