chapter 3

# If He Had Just Paid the Rent

*"The prisoners will not be harmed, until they are found guilty."*
*—Q, in "Encounter at Farpoint," from the television series,*
Star Trek: The Next Generation

## Introduction

The problem with many criminals is that they get addicted to illegal behavior. The excitement that comes from committing the first crime has its roots in the fear of getting caught. If

they don't get caught, they are encouraged to do it again and possibly again. As they get away with more crimes and infractions, they begin to feel untouchable. Eventually, they feel like they can commit any crime and get away with it.

Fortunately for us, that becomes their fatal flaw. All of these little crimes eventually catch up with them. This is why police training teaches cops to investigate small crimes, because they can lead to the discovery of much larger ones. Of course, you can never tell when a small incident will turn out to be nothing or become a pretty big deal, so it is important to examine them all.

Take the case of our new friend, Wesley. He was renting an apartment in New York City (NYC) for about $2,000 a month. NYC is a tenant-friendly city, so it is difficult to evict a deadbeat occupant. It did not take much for Wesley to figure this out, and soon he stopped paying the rent on his apartment—which went on for months. As you might imagine, his landlord William didn't like this at all.

William was getting weary of trying to chase him down to collect the rent. He would get evasive answers and empty promises of payment, but no money. After six months of fighting for some attention, he had enough and decided to proceed with legal action. It was time to evict Wesley. It was not an easy route, but the way he saw it, he simply had no alternative.

## The Eviction

William hired a lawyer and filled out the necessary paperwork to start the eviction process. In NYC, this can be very tricky, and trying to do it without a lawyer is often a

mistake. The process requires a final, formal demand for the rent. Once this is done, and after a few more steps, the case can go to court. Only through a trial can the landlord get the legal authority to forcibly evict the tenant. When he gets the judgment in his favor, he gets a Warrant of Eviction, which empowers the government to physically remove a person from his rented home.

In this case, Wesley went without paying the rent for six months before the Warrant of Eviction was finalized and assigned to Sheriff Yar to execute. Expulsion can be either difficult, or more difficult. Difficult is when the tenant is in the place at the time of the eviction. The Sheriff lets the tenant take his personal belongings and escorts him out of the apartment. The more difficult option is when the tenant is not there. The Sheriff then needs to forcibly enter the apartment and remove the personal property that is inside, usually putting it on the street. Either way, once the process has been completed, the apartment is turned over to the landlord.

Tenants can usually sense that they are about to be kicked out of their residence, especially when they haven't been paying rent for a while. By that time, they have usually vacated the apartment, taking away anything of value. Wesley wasn't this bright.

There was no one home when Yar arrived, and it was beginning to seem as if Wesley had skipped town. Because William was there as well, he was more than happy to open the apartment for Yar. Upon entry, it was obvious that Wesley had not cleared his apartment out, as there were quite a few televisions and other strange electrical equipment. This seemed very odd, and Yar immediately suspected that the apartment was being used to store stolen goods.

Because the equipment might have been considered evidence of a crime, leaving it on the street was not an option. He needed help and wanted to contact the NYPD to have them check it out, but what was he going to do with the apartment in the mean time? Unfortunately, since this was not an emergency, he could not call and wait for them. Instead, he would need to set up a time when they could come by and in the meantime secure the site to prevent Wesley from coming back in. He could not let William have his place back—not yet. Oh great, William thought, he would have to wait even longer before he could rent out the apartment again.

So Sheriff Yar padlocked the door, put some yellow tape across its opening, and posted a notice that an eviction warrant was being served. He wanted to make sure Wesley was not going to be able to remove or destroy any of the evidence. Now he could go contact the NYPD.

Wesley arrived to his "apartment" later in the day to find out he was being evicted and could not get in. Panicked, he called William and was informed that he was being expelled because he failed to pay rent for six months, owing $12,000. Wesley profusely apologized and asked to meet with him to take care of his debt. William told him that he would only take cash, no checks, because he knew it was his only chance to get the money he was owed.

Somehow, in a matter of minutes, Wesley got the money together to pay his overdue rent. It was hard to believe this was the same guy that was hard to find and unwilling to pay just a couple of days before. William could not believe his eyes and eagerly took the cash. Wesley, after taking a deep breath of relief, asked to be let into his apartment. William told him that now he would need to speak to Sheriff Yar, because that's who now had control over the apartment.

Wesley got really upset and tried to argue to get his money back, but William, being a true New Yorker, knew better than to give him the cash back. Getting the back rent paid was a nice surprise for William, but since Sheriff Yar had the apartment, he still did not have an apartment to rent.

The NYPD cops arrived quickly to inspect the apartment. They immediately determined that the "TVs" in the room were actually computer monitors. The "other electrical stuff" was computer and networking equipment. With that mystery solved, a new one arose. What were all of these devices being used for? This was a residential apartment, not an office, so this equipment seemed very out of place. The cops were unsure as to how the equipment was being utilized and decided to play it safe. They posted a couple of officers to guard the place and left.

They decided to leave the apartment and find a law enforcement agency that specialized in computer cases. In New York City, Supervisory Special Agent Robert Weaver of the New York Field Office (NYFO) of the United States Secret Service (USSS) had just recently started an experimental multi-jurisdiction, multi-discipline task force known as the New York Electronic Crimes Task Force (NYECTF). It is comprised of agents from the Secret Service, the FBI, the NYPD, and the State Police, along with representatives from the high-tech industry that specialize in computer crime investigations and computer forensics. The NYECTF, with its diverse makeup and expertise, was designed to handle cases just like this.

The NYECTF agents accepted the case but were not able to come down to inspect the location immediately because they needed to get a search warrant. As we are well aware, those can take a couple of days to get completed. So in the mean time, members of the NYECTF were able to get some

cops from the NYPD to continue guarding the apartment while the paperwork was completed, ensuring that the potential evidence inside the apartment was not compromised.

## A Simple Twist

Wesley's panic grew. Not only could he not get into his apartment, but also the police were either looking through his stuff or were about to look through it. He was scared and desperate, so he decided that he needed to do something. Calling upon his fantastic criminal mind, he set about a course of action. He broke into his own apartment (which was under surveillance) through a window and came out quickly, running off with a laptop computer. The police officers that were guarding the place were caught by surprise. Who would have expected that a tenant who had been evicted from his apartment would want to break back in? It seems very funny today, but a few years ago, law enforcement did not think that high-tech crimes would inspire such amazingly bold acts. At that time, no one would have expected it.

Sadly, when the police finally realized what was going on, Wesley was already gone. Apparently there was something very valuable to him in that computer. Of course, the cops felt really embarrassed that they allowed this to happen. Their sergeant, a bit frustrated, replaced them with different officers who were more careful.

## NYECTF

I got involved in this case together with one of my friends, Hugh, because we were part of this new task force. We were pleased to be able to offer our computer and telephone expertise to help the NYECTF. Hugh was a seasoned telecommunications security professional, having worked for companies such as New York Telephone and NYNEX for many years. He was very knowledgeable and easy to work with.

Some members of the organization, who asked to meet with us in New York City, called us in. They had an assignment coming up and wanted to discuss some options, so we got together with them at their office in 7 World Trade Center (WTC) early in the evening. From there, we went down to the parking garage of 1 WTC (the north tower). Because of the bombing of the WTC garage by fanatics in 1993, additional security had been put into place. You needed official permission and a special pass to gain access. The guys on the task force definitely had the pull to escort us in.

The Secret Service had a section of the garage reserved for them. Here, they stored their government vehicles, affectionately known as G-rides, and parked their personal cars. We met there to discuss the upcoming search and to help load the van with the equipment that would be needed. One of the things that Hugh noticed right away was a "NYNEX" vehicle that just did not look right. He turned to Bob, pointed to the van, and politely asked, "What the hell is that?" With a smirk, Bob told him that it was one of their undercover vans. Hugh responded that it made sense, because it wasn't a real NYNEX truck. To this day, none of us could tell how Hugh knew!

Tip

If you ever plan to make an undercover vehicle, like a replica telephone van, be sure to have some of the security personnel look it over. They might be able to save you some potential embarrassment.

After a little while, it started to sink in to Hugh and me where we were. The garage walls were painted green in some sections, yellow and red in others—not a usual color scheme, to be sure. We were told that the red paint signified the area where the bomb had been set off three years prior, at level B-2. We finally understood we were near the location where the truck bomb was set off back in February of 1993. This was a very somber moment for us.

As we stood in the building's foundation, I remember marveling at the immensity of the structure, thinking that it would be nearly impossible to significantly damage these massive buildings that were reaching nearly a quarter mile into the sky. Sadly, recent history has proven me wrong.

The rest of the night was spent preparing the computer forensic equipment for the search, which was scheduled for the next day. We were assembling cartons, power cords, any disk duplicators that we could find and items of the like. This was just some basic preparation that needed to be done.

## Time to Collect the Stuff

It was time for the search, and entering the apartment was pretty stress-free. After all, Wesley had been evicted, and it would have been highly unlikely to find him there.

Tip

When confronted with a seemingly overwhelming task, step back and break it up into manageable sub-tasks. Then it is easier to ask for help where you need it.

In the apartment, we found a couple of powerful computers that were networked together. This setup was further connected to a device that had wires coming out of it. How is that for a description? Well, that is how it appears to you when you enter an unfamiliar place and have no idea what you are going to find. That was the situation, and it seemed a bit overwhelming at first.

This was a case in which being methodical and patient paid off. The first step was to photograph the equipment and the interconnections before any computers or wires were touched. This can be extremely valuable, in case any questions arise during subsequent forensic examination. It was a fine option in this particular scenario, because there was no element of surprise. Usually, what should follow is to find the primary network connection and disconnect it, but that wasn't necessary here. If Wesley had wanted to change anything, he certainly had the time and the advance warning to do so.

After photographing the systems, our first setback arose. No one knew how to do a field forensic examination of the systems using the equipment we had with us in the apartment. That meant that the computers would need to be seized as evidence, and the examination would be done later. Given that was the case, it was time to shut down the computers and label and disconnect the cables. One of the members of the team was kind enough to draw a network diagram, displaying how the computers were connected.

This took care of the computers, but what about the device with the wires coming out of it? Good thing that Hugh was there, because he quickly recognized the piece of equipment as a Channel Service Unit/Data Service Unit (CSU/DSU). A CSU/DSU converts signals from a Local Area Network (LAN) to those of a T-1 data circuit. These are high-speed circuits rated at 1.544 MBs. Back in 1996, it was very unusual to see this kind of sophisticated apparatus in a residence, especially considering the service cost about $3,000 a month. This type of equipment was something we would have expected to see at an Internet Service Provider. To make matters even more exciting, a little later we found two more active CSU/DSU units. Wesley apparently had three T-1 circuits. Wow! No wonder he had no money left over to pay the rent.

Because a CSU/DSU unit does not store any data, it really has no forensic value. This meant that we did not need to seize or even disconnect them. That was helpful, as it reduced the amount of wires that needed to be labeled.

Hugh discovered something very interesting. Someone had physically tapped into the telephone lines that were running through the building. Apparently, Wesley's apartment was located right at the core access for the telephone service of the complex. He literally drilled a hole in the wall and tapped into the phone cables serving the residents. This allowed him to gain access to just about anyone's telephone lines in the edifice. With this type of access, he could easily eavesdrop on other people's conversations. This was something that none of us expected to see. You never know what you might find in a search until you actually get there.

In the end, only the computers and the disk drives were seized as potential evidence. The operating assumption at the time was that the equipment might have been stolen, and we could check the hardware's serial numbers back at the lab.

The computers were state-of-the-art Sun SPARC stations, which cost about $15,000 each. There were enough reasons to suspect that they were "liberated" from their rightful owner(s). The equipment was packed up and brought to 7 WTC as evidence—where we could start our investigation.

## The Initial Examination

Our primary goal during the initial evidence examination was to determine whether the computers were stolen or rightfully owned by Wesley. Our first approach was to contact Sun, the computer manufacturer. We had the model and serial numbers, so we hoped they had a registry of their sales and would be able to tell us who had bought them. Even if they couldn't give us an exact name, the name of a company would help. Of course, this would take some time.

Next, we wanted to see if there was any data on the computer system that might point to the original owner. Perhaps some of the configuration information on the computer system would lead the way. This was a long shot, to be sure, but it could work.

Of course, we did not have the root password or any other passwords for this system. We needed access to the data in order to prove our theory, and we wanted to avoid password guessing or any other activity that might disrupt the system. Our goal was to find a way to read the data off the disk drives without upsetting them. Because these computers were Suns, they had industry standard SCSI disk drives and a SCSI access port in the back. We decided to connect another PC to the Sun's SCSI port and read the data right off the disk drive. This technique would allow us to get to the data without having to guess any passwords.

Tip

While passwords are a standard security measure, they are not capable of protecting data against physical access. Barring encrypted files, if a person can get to the physical disk drive, he can usually get to the data.

Now that we had access to the data, we were able to do a simple check of the configuration files for the system. While nothing in this examination helped us determine if the equipment was previously owned, we did learn something: the computer was a server for an Internet Service Provider named borg.net. That was quite a surprise, and it certainly explained why the T-1 circuits were in the apartment. Apparently, Wesley was running an ISP out of his home. There is nothing apparently illegal about this, short of his not paying business taxes, running a business in an area zoned residential, or some other infraction. It was just an unexpected discovery.

## The Previous Owner

The leads from Sun began to pay off. We discovered that they had sold the computer to a university in New York City. They were even able to give us a contact name there. It looked like Sun kept computerized records very efficiently. Clearly it was time for one of the agents to follow up on this. One question that we wanted to ask was, "How did the computer get from the university to Wesley?"

After a short conversation with the contact at the university, we got our answer. It turned out that the computer had

been stolen about a year before we had seized it. Well, this appeared to be the first confirmed crime we had for Wesley. It seemed he did an inside job, because he had worked at the University for a short time. Our best guess was that he left work one day with the computer and never went back.

While interviewing people at the university, the agents uncovered other pieces of information. First, one of the employees had been receiving anonymous harassing email messages that were coming from borg.net (ring a bell?). The employee assumed it was Wesley, because they had known each other for a while, and Wesley had a history of doing this to him. The second thing reported was the suspicion that someone had broken into the university computer network. They had been experiencing unexplained computer changes and file deletions. After searching for an explanation, they were able to trace them back to borg.net.

Based on this information, the agents asked a judge to issue a warrant so they could search the disk data and try to find the source of the harassing email and any evidence of hacking against the university. Once they got it, the search of the data could finally begin.

One of the very first findings of the data search turned out to be interesting: borg.net had approximately 10 users. This seemed very odd, as 10 is a very small number of customers and certainly would not justify the three T-1 circuits that were in place. To understand the implications of this information, consider that a typical ISP might have a T-1 circuit for every 50 to 100 customers; in this case, borg.net had a ratio of one for every three.

The second interesting finding was that Wesley had password files from several universities, including the university in question as well as some local businesses. We concluded, based on some other files we found, that he was cracking the

password files to hack in. Whether he was a student or an employee at the University, there was absolutely no valid reason for him to have the password files on his computer. What made matters even worse was that he was storing these very critical security files at an ISP where others might also be able to download them and break into the victims' networks.

All the evidence collected up to this point was enough to create a nightmare for Wesley—and it only got worse. While reviewing the data, we discovered that the third and most distressing finding was not so much the vast amount of pornography found on the servers, but the amount of underage pornography. This discovery in itself was disturbing enough, but combined with the fact that he was running an ISP made the situation really unsettling. It strongly suggested that he was either trafficking with or at the very least facilitating the distribution of these materials. He was on very shaky ground, and the future did not seem too bright for him.

In summary, after our preliminary review of the equipment and connections found at Wesley's residence, we had come up with enough evidence to prosecute him for three crimes. First on the list was the possession of the stolen computer system. Second was the possession of more than 50 password-userid combinations (a potential violation of 18 USC 1029 as discussed previously in Chapter 1, "An Attack on the Telephone Network." These devices would allow him to gain access to quite a few different universities and businesses in the area. With these compromised accounts, Wesley, or any of his few cronies at the ISP, could gain access to sensitive records. Third was the underage pornograph;. not only for possession of it, but for trafficking or at least facilitating its distribution. Nothing good here!

## The Prosecution

Because Wesley had never been arrested before, he hired a lawyer in an attempt to keep his record clean. Taking a fine bargaining position, his attorney demanded the immediate return of his equipment, even though things were looking pretty bad for him. From the government's point of view, there was enough evidence to indict him and bring the case to trial. As expected, the agents in charge not only denied his request, but also decided to press charges against him. Our dear Wesley was booked. At least the defense had made the case so that he could be let out on bail.

At that point, there was nothing left for me to do. I had written my notes of the forensic examination and set them aside in case they needed me to testify at the trial. Now it was just a matter of waiting for the case to wind its way through the court system, which can take a very long time. So, as far as I was concerned, I was done for the time being.

A year went by, and the case was finally set to go to trial. To no one's surprise, Wesley did not show for his court date. He skipped, meaning that he missed a required date and was likely to forfeit his bail. As is usual with these events, the judge entered a warrant for his arrest. Wesley was now a wanted man. He certainly knew how to disappear, because the police were unable to locate him around the area.

As you can imagine, this wasn't the first time that an event like this had happened. Sadly, it happens often enough that law enforcement has procedures for handling these events. All of the evidence, notes for the case, and pertinent information concerning his wrongdoings were stored in the evidence locker at 7 World Trade Center. Sometimes this is how cases end, so we decided to forget about him and move on.

## Why Speeding Is Not Such a Good Idea

In late 2000, I received a call from one of the agents at the task force. He left me a voice message that simply said, "Remember Wesley? He's back." Ah yes, memories!

Wesley had been arrested on an outstanding warrant and was on his way back to NYC. He had been stopped for speeding somewhere in the southwestern United States. Have you ever wondered what happens between the time you get stopped by a cop and the time he gets to your car? To most of us it seems like an eternity, but for the cop it goes pretty fast. As a routine precaution, he runs a check on the license plate to make sure the car is not stolen and to get any other pertinent information. This lets him know a little more about what he is walking towards before he approaches the car. When he gets to your car, he asks for your registration and license, which he takes back to his vehicle to run a standard wants and warrants check. That is exactly what happened in Wesley's case.

While the car checked out OK, Wesley did not. The warrant from New York City caught up to him, so he was arrested on the spot and set for transport back to The Big Apple, where he had been terribly missed by all of us. After all this time, he was finally shipped back to face the charges he had run away from. Score one for the good guys.

To say he was shipped back is not far from the truth. Capturing fugitives happens very often. When the transport goes across U.S. state lines, the Marshall Service gets the task of returning them to the jurisdictions where they are wanted. Clearly, Marshals are interested in spending the tax

dollars they receive as frugally as possible, so they do not spend a lot of money on transportation. For a typical case like this one, they generally prefer to transport prisoners via bus, sending them from one jail to another over a series of days before they reach their final destinations. Wesley was able to enjoy nearly seven days of government frugality, since they focus on safe, cost-effective transportation and literally spare every expense on luxuries.

Tip

If you are a fugitive and you are going to partake in activities where you might get caught, consider doing so close to the jurisdiction where you are wanted. This will make for a more pleasurable transport by the Marshall Service…. Perhaps you might consider driving in comfort to the jurisdiction and turning yourself in.

## Fugitive Lessons

There was plenty of time to debrief Wesley on his "ride" back to the East Coast. The agents were able to learn some details of our fugitive's life on the run. After the indictment, he left the U.S. and returned to his native homeland, China. That was a great choice for him, considering the U.S. doesn't have very good extradition treaties with them. Even if the U.S. authorities had known where he had been, which they hadn't, there was basically zero chance that they could convince the Chinese to arrest him and send him back to be tried. There was not enough trust yet on the country-to-country level to allow this to happen.

He stayed in his home country for a few years, but could not resist the temptation to come back. We don't know why, but criminals often desire to return to the scene of the crime. Maybe it is either the excitement of possibly getting caught, the feeling of infallibility while fooling the police, or perhaps a belief that the authorities will just forget about everything. No matter the motivation, the desire is often there. Cops know this, and as long as they remain patient and persistent, they usually get their suspect.

Even though there had been a warrant for his arrest in NYC, he was somehow able to re-enter the U.S. The old Immigration and Naturalization Service (INS) did not stop him and certainly did not notify any other law enforcement agency. Remember, this was prior to the events of 9/11.

**Note**

In a world where people can travel the globe easily, it is very important for law enforcement agencies to work closely with border control and immigration services. Passport and visa issuing agencies need to be included as well. They are becoming an important resource for trans-country law enforcement.

Once in the U.S., Wesley thought it would be best to settle down in the Southwest, figuring it was far enough from NYC that no one would know about his previous activities. He was avoiding the charges and living a life on the run…until that one little speeding ticket caused the whole ball of carefully wound yarn to unravel.

Such is the life of a fugitive. One minute you are driving your car thinking that you have beaten the system, and the next minute you find yourself in handcuffs on a slow bus back to the "scene of the crime."

## The Fugitive's Choice

Usually, guys like Wesley do not accept their guilt right away. They commonly plead "not guilty" and get a lawyer, because they really don't have much to lose by doing this. Because he skipped, it was clear he wasn't going to be released on bail again and was going to sit in jail until the case was closed. If found guilty, he would most likely get credit for time served against his sentence. However, if he was found "not guilty," he would just be released. Consider it the fugitive's choice. Its foundation is based on the premise that, having already skipped bail, the defendant is not going to get another chance to be released on bail; he is going to spend time in jail whether he pleads guilty or innocent. Unlike the prisoner's dilemma, the fugitive's choice encourages only one decision: a plea of innocence in all circumstances.

*Prisoner's Dilemma*

The prisoner's dilemma was originally formulated by mathematician Albert W. Tucker and goes a little something like this: Monica and Lorena are picked up on suspicion of having robbed a bank. The police do not have a strong case on evidence alone, because the surveillance cameras were not working on the day of the robbery. However, they do have two suspects and would like to have at least one of the suspects rat out the other. But how? The two suspects are taken into separate rooms so that they cannot communicate with each other. Both Monica and Lorena are told the following:

*continues*

- If you confess to the crime and testify against your friend, you will go free, and she will get 4 years.
- If you don't, but your friend does, you will get 10 years.
- But, if neither of you confesses, there is enough evidence so that you'll both get 2 years.

Their options are summarized in table 3-1.

**Table 3-1** Prisoner's Dilemma Payoff Matrix

| | **Monica confesses** | **Monica keeps silent** |
|---|---|---|
| Lorena confesses | Monica gets 5 years<br>Lorena gets 5 years | Monica gets 10 years<br>Lorena goes free |
| Lorena keeps silent | Monica goes free<br>Lorena gets 10 years | Monica gets 2 years<br>Lorena gets 2 years |

Given that each must make this decision without knowing what the other is deciding, they are facing a dilemma. Clearly the best thing for both to do is keep quiet. However, the penalty for either one should they be the only one that doesn't confess is quite high. Even though it would be better for both to keep quiet, both usually confess.

As you will notice in Table 3-2, there are only two potential outcomes in this choice: that the defendant is ultimately found guilty or innocent (represented on the left-hand side). Defendants like Wesley have only two options: to plead innocent or to plead guilty (represented as the two columns on the right).

In each table entry, the consequences associated with each action are associated with a favorable (+) or unfavorable (-) value. The options that are least favorable are pleading guilty when you are innocent and pleading innocent when you are innocent. The truly guiltless are not in a very good position once they have skipped bail, now are they?

**Tip:** Even if you are innocent, do not skip bail unless you are ready to leave the country and never return!

As you can see, the best move in both cases is to plead innocent. This leaves the option open that a jury might actually find a guilty defendant innocent or that a problem with the prosecution might show up during the trial. Even when culpable, the defendant will get credit for time served in jail while awaiting trial.

**Table 3-2** Payoff Matrix #1

| | **Pleads guilty** | **Pleads innocent** |
|---|---|---|
| Is found guilty | (+)Starts serving time immediately, meaning he will eventually get out earlier | (+) Time spent in jail awaiting trial credited to prison sentence |
| | (-)No chance to get out of charges | (+) Trial gives defendant a chance to beat the charges |
| Is found innocent | (-)Serves time for no good reason<br>(-)Longer potential prison sentence | (-) Thanked for the time served |

*continues*

With this being the case, why do people ultimately choose to plead guilty? Because the prosecution sometimes will adjust the payoff matrix to encourage the defendant—commonly done by offering a reduced prison sentence in exchange for a guilty plea. This offer is usually proposed only when the defendant gets the sense that he or she is going to lose the trial. Until then, he or she has no incentive to plead guilty.

## Wesley's Moves

Wesley was fortunate enough to come from a wealthy family that could not believe their child should have to face the criminal justice system. So they hired Deanna, a defense attorney with an impeccable record, to defend their baby. She proved to be good immediately by challenging the evidence. She claimed that in order to defend her client in an adequate manner, she needed to see all of the information against him. This would allow her to test whether the cops had correctly done their job of preserving the evidence—she knew that without evidence, the case would fall apart.

Five years is a long time for a disk drive to be sitting in a storage closet, and retrieving data when they have been sitting so long might not be possible. Perhaps a magnet might have erased part of the data over the years. Maybe the physical disk drive spindles lost their lubrication with age and would fail on the first restart. It was a gamble where she had nothing to lose—and a lot to win.

I was asked by the task force agents to assist in generating a copy of the evidence for the defense. This, I was told, was not going to be easy, because it appeared that some of the hardware had failed during the years it was in storage. Further, none of the agents remembered how to operate such an ancient computer. The standard evidence storage technique back in 1996 was to keep the original disk drive as evidence. When we first processed this case, we did not have the ability to copy the data off of the disk drives and put it on a safe media that stores very well, such as a DVD.

Tip

When storing evidence for a potentially long period of time, ensure that it is on a commonly available media meant for long-term use. Standard disk drives are complex units not meant to be idle for years.

## Technicalities

So I went back to 7 WTC to visit the evidence locker on the ninth floor, where we retrieved Wesley's evidence. I had one main objective: to get as much data as possible off the five disk drives that were part of the two computers stored as evidence. I also wanted to transfer the evidence onto a more easily readable media.

Because the agents involved in the case were not familiar with the equipment in storage, I assembled my own forensic laptop system. For an operating system, I chose to use FreeBSD instead of Windows. FreeBSD is a free version of

UNIX that runs on standard personal computers. There were a couple of advantages in using it for the forensic unit in this case:

1. The FreeBSD version of UNIX is capable of understanding the files on the Sun system. This would enable me to perform the Sun forensics without having to purchase another Sun system.
2. The UNIX operating systems come with all sorts of great tools for safely retrieving data from a disk drive as part of the standard installation. It is very easy to set access to an entire disk drive as read-only in UNIX, preventing unintended changes to the drive.
3. It has support for advanced storage devices such as SCSI disk drives that were in the evidence locker. This would be very important for the Sun system, where the use of these is very common.
4. FreeBSD could co-exist with a Windows operating system on the same computer. I could copy data from FreeBSD to Windows and vice-versa. This would allow me to use Windows tools to put the data onto a CD-ROM.
5. FreeBSD is very tolerant of hardware failures. Given that we had known about hardware failures, this would be very useful in this case.

To access the data, I just needed to power up a Sun system and stop it from doing its normal boot. This would power up the disks without disturbing the data. Once I connected

the forensic laptop to the Sun with a simple SCSI PCMCIA adapter card, I could gain access to the data. This configuration allowed me to get directly to the physical media and bypass any computer hardware failures. It also allowed me to read the disk information as raw data. In this manner, I would be allowed to skip damaged sections of the disk while still getting useful data. Basically, raw mode allows greater flexibility, but requires great attention.

Note

A very nice feature about using a separate system to perform a forensic examination is that you do not need to disturb any files, including the ones in the computer operating system. This makes for a much cleaner inspection.

Almost immediately, I found out that one of the disk drives was not working at all. Fortunately for me and the prosecution, it contained only the operating system, and none of the evidence was located on it.

The recoveries on the remaining disk drives were far from easy. Each one of them had significant hardware failures on sections of the disk, so I needed to pull data off of the good sections and assemble it. After a few hours of effort, I was able to gather the records, along with notes on the retrieval technique and reading instructions for the defense attorney. All of this was put together on a CD-ROM and shipped out.

## End-Game

We were basically in very good shape, because all the evidence was still readable, and we were able to accommodate Deanna's request. It was a good gambit by the defense, but now they had nothing left. At this point, things were looking very different for Wesley, as you can see in Table 3-3. Let's assume for the moment that he was in fact guilty of the charges. (Not an unreasonable assumption—after all, why would the police ever arrest an innocent person?)

**Table 3-3** Payoff Matrix #2

| | **Pleads guilty** | **Goes to trial** |
|---|---|---|
| Is guilty | (-)Possibility of losing the trial | (+) Possibility of winning the trial |
| | (+)Plea deal would result in small penalty | (-) Losing trial would result in larger penalty |
| Is innocent | (-)Serves time for no good reason | (+) Should win trial |
| | (-)Longer potential prison sentence | |

If the penalty for going to trial and losing or skipping the trial and pleading guilty were the same, then clearly Wesley would ride out the trial. The prosecution doesn't want to have to take this case to trial for two main reasons:

1. Trials are costly in both personnel and time. These are items in short supply for most prosecutors.

2. There is always a chance that a jury will return a finding of "not guilty" no matter how good the case is. Like every other part of the criminal justice system, juries are not perfect.

As the options to poke holes in the case disappeared, Wesley was made an offer he couldn't refuse. His guilty plea would result in a reduced sentence versus the potential full one. He would also get credit for the time served toward his sentence.

Wesley finally pled guilty around July of 2001. He ended up with a felony conviction and is probably out by now. All of the computer equipment involved in the case became property of the federal government, and he lost his original bail.

As it turned out, we were very fortunate that he took the plea deal when he did. It was just about two months later when terrorists crashed planes into the Twin Towers, which resulted in the collapse of 1 WTC, 2 WTC, and 7 WTC. Evidence and case files, nowhere near as important as lives, were lost in the collapses on that day. Fortunately, because he took the plea deal, Wesley did not profit from such a tragic event.