

From the dark corners of the Internet come the

Forensic Case Files

True
Stories of
Cybercrime

Volume 1

"The story you are about to read is true; only the names have been changed to protect the innocent."

Case #2

The Case of the Casanova Con-Man



The manager on the phone from the computer store said he had a client for us, but he strongly suspected the guy was nuts. This was not a problem. We specialize in crazy customers. Most of them turn out not to be so crazy after all. Following a brief discussion with "Harry" by phone, we met the next day for coffee and let him tell his tale.

Harry's father passed away and left his family roofing business to his grown children – Harry, his two brothers and two sisters. By some miracle, the business was still doing well despite the downturn in the housing market. They all worked for the company, especially since their father took ill. Although they each owned a portion, not all of them wanted to remain in the business. That was especially true of Harry's sister, Clarisse.



Clarisse was a recent widow. She and her husband moved to Florida when his health demanded a warmer climate. Despite the distance from Baltimore, she kept her hand in the family business and enjoyed a modest profit

from it. But now, it was tough commuting for annual meetings, and she wanted to be bought out.

Besides, Clarisse had a new beau. She was only 50 when Claude died. After a year passed, Frederico came into her life. He was handsome and charming. They went dancing, and took long walks on the beach. They cruised the Gulf and visited the islands. He wined and dined his way into her heart.

The family agreed to hold the next annual meeting in Florida. This was partly to accommodate Clarisse, and partly to escape the cold Baltimore winter. They also wanted to meet the wonderful man who had waltzed his way into their sister's life. They all liked Claude, but agreed that Clarisse deserved to be happy.

Frederico turned out to be a suave, well-spoken gentleman, slightly younger than their sister. He had a presence about him that put everyone at ease. Clearly, he was a great partner for Clarisse, who doted on him. He was skilled with computers, and volunteered to help when Harry's laptop froze up the afternoon before the business meeting. Freddie stayed behind to work on it while the family held their annual meeting at a local seafood restaurant.

Despite his charm, something about Freddie bothered Harry. He laid in his bed at night and tried to convince himself he was overreacting. Freddie was a great guy, and Clarisse seemed so happy. *Couldn't he just leave it at that?*

continued



An incident the following day only raised more concerns. During a private talk with Clarisse, she revealed that Freddie was a successful entrepreneur, but suffered recent business set-backs. She understood adversity, and graciously offered to help him out financially. Harry asked how much help, and nearly choked when she said she loaned him over \$100,000. She was sure he would be able to recover and do well again, so why not?

Back in Baltimore, Harry began looking into Freddie's past. He always stood by Clarisse. Now that she was part-owner of the family business, he felt an even greater sense of responsibility. His attorney hired a detective who ran a background check on Freddie. The results were disturbing. Freddie had a reputation as a con-man who preyed on wealthy widows in Florida. Two of his past wives died under mysterious circumstances and left him significant sums of money. Both were married to him for less than 90 days. Clarisse's husband left her a small fortune. Combined with the buy-out money, she would be set for life. She fit the profile of the women Freddie targeted. Harry's heart sank.

He emailed his brothers and other sister with the news, and a round of discussion ensued. Fearing Clarisse's life might be in danger, they decided they must warn her about Freddie. Harry was selected as spokesman.

But when Harry called to give Clarisse the news, he was astounded to learn that she already knew. In a heart-to-heart talk the night before, Freddie told her all about the terrible tragedies which had befallen his past wives. She too was in grief, so she understood. Surely the newspapers got their stories wrong. Freddie had nothing to do with those tragic deaths. He was merely the victim of bad luck. Couldn't Harry see that?

Not long afterwards, Harry's attorney called. Their investigator dug up more on Freddie. Under an alias, he ran the same scam on several islands in the Caribbean, minus the marriage angle. He was also implicated in several phony land schemes in the Bahamas, and also on Aruba. In one location, he was charged with assault and battery on a woman who later dropped the charges when he returned

a certain sum of money. This was looking worse and worse.

Once again, Harry forwarded the information to his siblings via email, and once again they all wrote back and forth about the situation. Because the roofing business was spread out over the region, with several small offices, and because conference calls were difficult, email seemed the best way to get everything in writing and reach all of them at once.

Harry again called Clarisse. It was more than a week since they last spoke. By sheer coincidence, she and Freddie had another of their heart-to-heart talks the night before. He enlisted her aid in figuring out the mystery of what went wrong in each of his failed business ventures in the Islands. With her help, Freddie said, he'd never make those mistakes again. Clarisse said it was like being a detective on a TV show, as they discussed the details, the false accusations, and the things which actually happened behind the scenes. *Freddie a criminal? A con-man? Don't be ridiculous, Harry. You're imagining things,* Clarisse told him.

After the call, Harry realized that on each occasion, Freddie only confessed to the cases which Harry and his attorney uncovered.

"It was like the guy was a fly on the wall, listening to all our conversations!" Harry said.

He suspected Freddie installed spyware on his laptop. But none of the three shops he visited could find anything amiss. In fact, Harry's machine seemed unusually free of adware,

spyware and viruses. When Harry became upset while in the third shop, the owner recommended us and gave him our number. What Harry didn't know was the shop owner called us with a head's up about Harry's possible "mental problems."

We agreed to inspect Harry's laptop. Once the papers were signed and Harry's retainer received, we shook hands and the laptop went to the lab for examination.

Although we were not being asked to investigate at a "forensic" level, we took certain routine precautions. We removed the hard drive from his laptop and made a copy, byte by byte, sector by sector, using write protection to avoid making the slightest change to the drive. The original

"It was like the guy was a fly on the wall, listening to all our conversations!"



drive was then sealed in plastic and set aside. One of the clones was also set aside, and all tests were performed on the second clone. This is standard procedure.

At first, it *seemed* Harry's computer was fine. Almost too fine. We found an anti-virus software package was installed at some point. It was up to date, which is unusual for most consumer and small business anti-virus programs. We could see the program found and eliminated some of the most common viruses, as well as some adware and spyware. The computer was essentially clean.

Next, we looked for common "Trojan horse" programs, used to compromise the computer without raising the alarms of the anti-virus program. None were found, nor were any traces of past Trojans found. Testing continued as we worked down the list of usual suspects – worms, key-loggers, etc. Nothing was found.

It seemed perhaps the manager at the computer shop was right. Maybe our client *was* imagining things. Perhaps it was all pure coincidence.

We decided to conduct what we call "behavioral tests." This is where we connect a suspect machine, using a clone drive, and let it run to see what it will do. We hooked up other machines to watch the laptop's behavior, fired it up, and let it run. This is analogous to monitoring a potential crime scene through security cameras, to see if you can catch a thief in the act. The results were quite enlightening.

Anyone familiar with PCs knows that standard Windows updates run on "Patch Tuesday," every third Tuesday at about 2 A.M. Any PC powered on and connected to the Internet on Patch Tuesday will generally run updates then. Therefore it would be perfectly normal for a Windows machine to wake from sleep and show hard drive activity at that time. Harry's computer, with the clone drive inside and connected to the Internet, did exactly that. We were in the lab, working late, when his laptop came to life and began to blink the hard drive light. This seemed reasonable, until we realized it was Friday.

By the light of day, we took the machine off-line and began a deep examination. Careful inspection of the log files revealed which program had activated and what it did. Red flags went up when we realized that the program which ran was not doing what it was supposed to do. By its name, it was a utility which ran only once, when a PC upgraded from XP to Vista. But the log files revealed this utility was running every night, always at 2 A.M. We

wondered what it was doing, so we found the exact program and opened it up in a hex editor.

What we discovered was a script disguised as a typical Windows background utility. This script did two things: it sent a message out over the Internet to a specific IP address, and it opened up a "back door" into Harry's laptop. This enabled someone at the other end to access Harry's hard drive and download anything they wanted from it. A trace of the IP address lead us to an Internet service provider in Florida. This was the secret door into Harry's computer. *But how did it get there?*

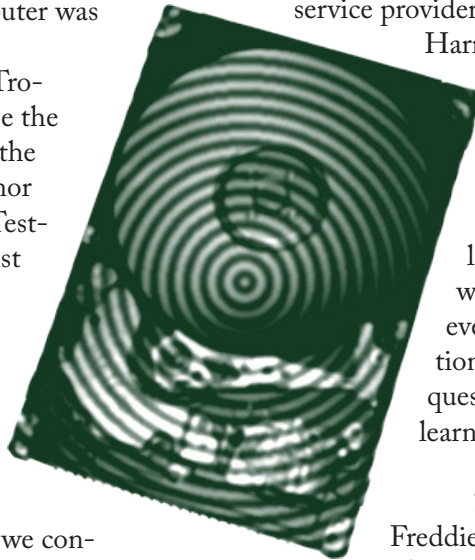
It would have been nice to dig in Harry's log files and unearth the exact date and time when the malicious script was installed, but the perpetrator covered their tracks. They deleted specific log information from a certain point backwards. As investigators know, however, even deletions can yield valuable information. It was time to call Harry and ask some questions. After a detailed conversation, we learned the following:

1) The anti-virus software had been Freddie's idea. He offered to install this "great software" on Harry's laptop, so it would be protected. Harry was a relative novice, so he welcomed the advice and watched as it was installed.

2) The annual business dinner ran from 6 to 9 P.M. The software log file was purged at 7:30 that night. It didn't take a rocket scientist to figure out who had unrestricted access to Harry's laptop during that time.

Harry was satisfied that we accomplished what he hired us to do – learn if his computer had been compromised and by whom. While we didn't have sufficient evidence for a stone-lock in court, both of us realized the only possible answer: Freddie compromised Harry's computer while "fixing it." He then deleted the log files which could have revealed what he did. Only Harry's insistence that something was wrong, and that Freddie knew details from their private conversations, led to uncovering the truth hidden deep in his Windows files.

When we showed Harry the evidence, he was delighted and petrified at the same time. He was happy to be vindicated, but horrified as he realized that all the family's financial information on his laptop was compromised. That would explain Freddie's eagerness to confess and keep himself on good terms with Clarisse. He knew how much she would profit from the buyout agreement.





We provided Harry with the following alternatives:

- 1) We could wipe his hard drive and re-install Windows. This would give him a clean machine, free of spyware and malware. Then we could put his personal information back on the laptop.
- 2) He could purchase a new PC laptop, to which we could then restore his personal files from our backup. This would leave the original computer intact, to potentially be used as a tool to catch the perpetrator.
- 3) He could purchase a Mac laptop, known for their resistance to malware, but then he had the complication of transferring all his Windows-based files to that machine and making them work.

Either of the first two solutions would have worked. But Harry was afraid to use Windows again. He was convinced that transferring his old files to a new PC would somehow repeat the problem. Granted, this was an overreaction, but the final decision was his.

That night, Harry went to the local Apple Store and bought his first Mac laptop. We provided Harry with the laptop hard drive in an external case, which the techs at the Apple Store used to transfer and convert his Windows user files. He signed up for some training on his new computer.

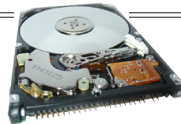
Harry later told us he chose not to confront his sister further, but to instead have the company's attorney talk to her personal lawyer. They all hoped she would listen to reason. Of the family members in the Baltimore area, each of their computers were inspected by competent techs; no other compromises were found.



Author: Drew Janssen, a digital forensic investigator, is President & CEO of Drive Rescue, Inc., a data recovery company, and of Janssen Forensics, Inc., a digital forensics lab, both located in Baltimore, MD. Your questions and comments are welcome. Email: drew@getjanssen.com

Contents & Design © 2010 Janssen Forensics, Inc.

Eddy's Tech Tips



- Only let those you know and trust work on your computer. Similar to a car mechanic or a doctor, you must have a level of trust and confidence in your technician.
- Turn off wireless connections such as Bluetooth, WiFi, or infrared beam when not in use. Every open door is a potential security risk.
- Keep your virus protection software up to date. There are thousands of new viruses released every week, and you if you re not up to date, you re not protected. Ensure that it s properly installed and configured by a trustworthy professional.
- Know and understand the basic processes of your machine. Be proactive. Take a class or get

instructions from a reliable source. Remember only you can prevent forest fires!"

- Always keep a named administrator account. Don't use "administrator" or "admin" as the name. Use strong passwords.
- Change passwords, online and local, at regular intervals at least every 90 days, or sooner if you suspect malicious activity.



Author: Eddy Sullivan, General Manager of Janssen Forensics, Inc., began fixing computers before he could shave. Comfortable on both Macs and PCs, he is positively OCD about backing up data. In our business, we think this is a good thing. Email: eddy@getjanssen.com

News: Drive Rescue, Inc. is proud to announce the birth of a brand new bouncing baby company: Janssen Forensics, Inc. Cybercrime is on the rise, and so is the detective business. It's time for a new kind of investigative agency, using new high-tech methods and old school skills. A new website is being built, full of cool stuff. Yeah, ok, it was supposed to be done before this came out. We're working on it. Meanwhile, you can visit us at www.driverescue.net

Fine print: Forensic Case Files is a publication of Janssen Forensics, Inc., a digital forensics lab and investigative agency located in Baltimore, MD. All contents © 2010 Janssen Forensics. This newsletter is distributed freely, and you are welcome to share it with friends, or even total strangers. Contact number: 443-310-7920. Yes, the stories are true. We couldn't make this stuff up. Names and certain details have been changed to protect confidentiality.
