



BY JESSICA FORSYTH

Into Cyber Space

With the growth of the Internet and all manner of digital technologies, **computer crime** is fast becoming one of law enforcement's biggest challenges. That's why the FBI has teamed up with local agencies to open the new five-million-dollar-plus Orange County Regional Computer Forensics Laboratory – the third such lab in the state – that will be responsible for investigating everything from counter-terrorism to child pornography and identity theft.

It was the era of Nintendo and Michael Jackson, the final years of the Reagan presidency and the heyday of the floppy disk. The late 1980s was a time of drastic change and skyrocketing innovation; it marked the end of some things, like the Cold War, and the beginning of others, like a united Germany after the fall of the Berlin Wall in 1989. Technology was growing at a rapid pace – a reflection of the national mood: confident and optimistic and somewhat risky, with an eye toward the future and its multitude of possibilities. It was the dawn of the modern computer age, a time when terms like “online” and “Web site” hadn't yet worked their way into our collective lexicon, but developments like Atari and arcade video games were already inventions of the past. Computers were fast becoming part of our national normality, machines on which we were becoming increasingly dependent in our daily lives.

By most accounts, these leaps in the tech world were a good thing. Efficiency improved; certain functions like complex calculations and even your annual income tax could be computed almost instantaneously; and entertainment reached new

pinnacles of fabulousness. But there was, inevitably, a downside. It turns out that, as some law of human nature, wherever there is a new development, there is someone who wants to manipulate it. In the late 1980s, that person was Robert T. Morris, a graduate student at Cornell University, who was responsible for developing the Morris Worm, a computer virus that infected thousands of computers and caused an estimated \$10-\$100 million in damages. For the problems he caused, Morris was indicted for the world's first cyber crime in 1989 and was found guilty in 1990 of intentional access of Federal interest computers without authorization, which prevented authorized access and caused a loss in excess of \$1,000. He was sentenced to three years of probation, fines and 400 hours of community service. Morris has since gone on to become an associate professor at the Massachusetts Institute of Technology at the college's Department of Electrical Engineering and Computer Science, and has been instrumental in developing software that has been bought for millions of dollars by companies like Yahoo! – not unlike a high-tech version of the story of Frank Abagnale Jr., the con artist-turned-FBI-informant on whose life the movie *Catch Me If You Can* was based.

But despite Morris's cleverness in hatching the world's first computer worm, those

were still the Dark Ages of cyber crime. Today, computer crimes constitute hundreds of millions of dollars in losses each year and are committed by perpetrators who can be anything from a tech-savvy teenager in the U.S. to a hacker-by-hobby in Israel to a scammer in Nigeria and who steal, launder money or terrorize people through fraud, e-mail scams, terrorism, and even violent crime. Everyday media such as the Internet, e-mail, cell phones, and pagers are at the heart of cyber crime, and with constantly changing technology comes an increasing level of sophistication in both the people who perpetrate the crimes and the types of crimes being committed. Just a few months ago, in Orange County, identity theft investigators at UC Irvine uncovered a Dallas-based ring that filed false federal tax income returns using the Social Security numbers of 198 UCI graduate students – an example of how far-ranging and targeted computer crimes have become, but these are by no means unique or terribly different from all the other similar events that occur almost every day all over the world. So how do we stop these crimes from happening? The FBI thinks it might have the answer.

About the time Morris was finishing up his probation, FBI Supervisory Special Agent Jason Weiss was graduating from law school. A lifelong gamer who “was obsessed

RALPH PALUMBO

FBI Supervisory Special Agent Jason Weiss will oversee Orange County's new Regional Computer Forensics Laboratory.

with computer games and how to make them run,” Weiss had been an FBI honors intern in 1990 during law school, but because of a hiring freeze, had gone on to work as a trial attorney in Central California, practicing civil litigation and insurance and medical malpractice defense. Six years later, in 1997, he was contacted by the FBI. “I loved being a lawyer,” he says, “but the FBI only comes knocking once, so I decided to give it a shot.”

What started as a stint in Virginia learning how to investigate cases, conduct interviews, handle evidence, and work with guns, led to an assignment with the FBI’s violent crime squad in San Diego. A year later, in 1998, Weiss was recruited to become part of the FBI’s computer crime squad as a computer forensics examiner at the nation’s first Regional Computer Forensics Laboratory (RCFL) – a division that has grown to include 14 such labs in the country. That year was a date held in a kind of suspension, halfway between the time Morris wreaked havoc with his devastating computer virus and today, the modern era of digital technology. Since then, the FBI’s RCFLs have become the primary investigatory agency for every manner of cyber crime. “We’re like a funnel,” says Weiss. “Basically every case in the office has to come through our program because almost every case that’s being investigated now has a digital component such as a computer, a cell phone, flash drive, voice recorder – almost anything you can imagine that stores data magnetically in digital format is processed and examined by my group.”

That group, however, which currently works out of the FBI’s Los Angeles Field Office, was becoming overwhelmed with what had become one of the country’s highest concentration areas of crime – an area encompassing approximately 20 million people, about 6% of the nation’s population – many of which necessitated the experienced eye of an RCFL computer forensics examiner. So Weiss, who had been promoted to supervise the Los Angeles computer forensics program in 2006, spearheaded a program for the FBI to put in competitive bids to offices and agencies interested in a new RCFL. “There were 11 offices that put in altogether,” says Weiss, “and we ended up being ranked number one. We were awarded what is now the Orange County RCFL.”

Scheduled to open in early 2010 in

Central Orange County, the OCRFCFL will be the go-to place for law enforcement agencies in the lab’s seven-county service area that need the support of a full-service computer forensics laboratory to examine and investigate the digital component of crimes such as homicide, theft or destruction of intellectual property, child pornography, and fraud, among many others. One of the problems with investigating and prosecuting digital crime, as Weiss points out, is that, until recently, there has not been a unified body of forensics examiners working under a single agency. “I’m a believer that, if we’re going to stay competitive with the criminal class, the future of computer

BY THE NUMBERS:

Computer Crime

74 – Percentage of fraudulent contact that takes place through e-mail

28.9 – Percentage of fraudulent contact that takes place through Web pages

22,940 – Number of complaints received per month via the Internet Crime Complaint Center (IC3) in 2008

1,400 – Number of complaints received per month via the IC3 in 2000

10 – California’s rank for perpetrators per capita; there are 40.09 perpetrators per 100,000 people.

10 – California’s rank for complainants per capita; there are 95.09 complaints per 100,000 people.

SOURCE: 2008 INTERNET CRIME REPORT

forensics is an RCFL-type program,” says Weiss. “By combining all our resources both in terms of staffing and financially, we create a much more potent answer to digital crime.” Part of that formula for the OCRFCFL includes standardizing procedures such as digital evidence recovery and nationalizing standard operating policies in computer forensics, which Weiss says will lead to an internationally recognized laboratory accreditation that only six or seven labs in the world can lay claim to – “basically taking computer forensics from an art form to a science,” he says.

That’s a good thing, because cyber crimes are only increasing on the world’s stage. In 2008, complaints to the Internet Crime

Complaint Center (a.k.a. the IC3, a partnership between the FBI and the National White Collar Crime Center) were up 33.1% from 2007, coming to a grand total of 275,284 complaints that amounted to a loss of \$264.59 million dollars. The United States leads the way in the world for the highest number of perpetrators of these crimes, as well as the number of victims; divided further, California ranks number one in the number of both perpetrators and complainants. (Per capita, however, the District of Columbia ranks first for perpetrators; Alaska is number one for complainants.)

California’s sheer size is a challenge for computer forensics investigators, who are processing more data than ever before on devices that run the gamut of operating systems, computer models and different types of file encryption. “We have to pretty much be on top of everything and that’s a constant evolution in terms of our growth,” says Weiss. “It can be a formidable task.” But with new technologies like live image acquisition, which allows a forensic examiner to make a copy of computer data without shutting the machine down, and the speed and expertise with which agents can process media like cell phones, the FBI is not only keeping up with the criminal element, they are aiming to get ahead of the curve with the help of RCFLs like that in Orange County – especially when it comes to crimes like child pornography and the exploitation of children. “We’ve seen a tremendous growth in crimes against children,” says Weiss, who adds that cyber crime, which includes crimes against children, is the RCFL’s biggest component. “Internet people live in [a] world [where] they’re somehow anonymous, and they may do things that they might not have normally done. I’m sure that for every 10 guys we catch, there are 10 guys we haven’t,” says Weiss. “But we will.”

It’s that kind of determination that characterizes the attitude of the FBI’s RCFLs – a fortitude that allows investigators to sift through piles of data that, if printed from a 40-gigabyte hard drive (small by today’s standards) would go from the ground to the top of the 555.5-foot Washington Monument. “We definitely have job security,” says Weiss, jokingly. “But that’s why we’re lucky to get the new OCRFCFL. Without it, we’d feel like we were running backwards.”

For more information, go to ocrcfl.org.