OCTOBER 7, 2019

Legaltech® news

ONLINE

An ALM Publication

Nervous System: How Legal Tech Helped Catch the BTK Killer

In this month's look at the history of cybersecurity, David Kalat examines how forensic analysis was used to catch one of America's most notorious serial killers after three decades.

BY DAVID KALAT, BRG

With the aggressive pace of technological change and the onslaught of news regarding data breaches, cyber-attacks, and technological threats to privacy and security, it is easy to assume these are fundamentally new threats. The pace of technological change is slower than it feels, and many seemingly new categories of threats have actually been with us longer than we remember. Nervous System is a monthly blog that approaches issues of data privacy and cybersecurity from the context of history—to look to the past for clues about how to interpret the present and prepare for the future.

(AP Photo/Bo Rader, Pool)

Dennis Rader is seen in a Sedgwick County courtroom in Wichita, Kan. during the first day of testimony in the sentencing phase of his trial on Wednesday, Aug. 17, 2005.

In January 1974, a family in Sedgwick County, Kansas, was found strangled in their home. A father, mother, and nine-year-old son had been bound and murdered in their beds. The eleven-year-old daughter was hanging from a water pipe in the basement, partially nude and with semen on her leg. Other children had not been home at the time of the attack—they survived and would reach middle age before the man who orphaned them was caught.

The killer struck again in April 1974, stabbing a woman eleven times and shooting her brother in the head.

The rampage continued for years. In March 1977, he strangled a woman and intended to strangle her children, whom he had locked in the bathroom, but a ringing phone apparently scared him off before he completed his plans.

Another woman was strangled in her bed in December 1977.

In April 1979, he picked another victim and waited for her. And waited. And eventually grew so impatient for his chosen prey that he gave up and sent her a threatening letter instead. Ever since a letter boasting about the first stranglings had been found in a book in the Wichita Public Library, the killer had been carrying on his own hideous PR campaign, sending messages to the press and the authorities describing his crimes and warning of horrors to come. He called himself "BTK," for "Bind them, Torture them, Kill them."

For decades, the Wichita Police Department agonized over every lead, studied every clue. In 1984, it formed a task force, nicknamed the Ghostbusters, to focus on chasing the killer. Famed FBI profiler John Douglas came to help and to distill some perception of the killer out of all the disparate clues. There were five incident's worth of evidence to examine. BTK had been careful not to leave many fingerprints, but he had left some. He also had left copious amounts of bodily fluids, ripe for DNA analysis. And then there were the letters. BTK typed his letters, but sent the originals—and investigators pored over the fibers of the paper, the distinctive alignment of the typewriter keys, trace fingerprints, and stains. Other investigators focused on the content of the letters, their peculiar word choices and distinctive misspellings.

With all these clues, with all the resources of a metropolitan police force backed by FBI specialists, BTK remained at large. The Ghostbusters disbanded in 1987; Douglas retired from the FBI in 1995. BTK continued killing—murdering three more women, in 1985, 1986, and 1991. And in 2004, he resumed sending taunting messages, reigniting public fascination and frustration in the unsolved murders.

Everything changed when a letter from BTK arrived at a TV station on February 16, 2005. This message was not typed on paper. This was a proper twenty-first-century message, an electronic document on a computer disk.

And with that, BTK was caught. Thirty years of law enforcement's best and brightest taking aim at the physical evidence with traditional investigatory methods had stalled out, while a computer forensics examiner looking at the metadata of a deleted file cracked the case.

The package that arrived at the KAKE-TV studio in Wichita contained photocopies of crime scene pictures, a locket belonging to one of the victims, and a 1.44 MB floppy disk. The reporters called the police, and onetime Ghostbuster Ken Landwehr and his computer forensic examiner, Randy Stone, took over.

The disk contained a single file, called "TestA.rtf." The file's contents were the usual BTK taunts and threats, along with a promise that "[a]ny communications will have a # assigned from now on, encase one is lost or not found." BTK's messages were notorious for poor spelling, but was there some hidden significance to this particular spelling glitch? "EnCase" is one of the premiere computer forensic software platforms—and if BTK was knowledgeable about its use, to what extent might he have tampered with his own digital trail to confuse or mislead the investigators?

The disk sole's active, allocated file was this TestA.rtf communique, but running the disk through EnCase revealed a second document, a deleted file—an agenda for a church council meeting of the Christ Lutheran Church, which had been last saved by a user identified as "Dennis." A simple Google search revealed that there was a Christ Lutheran Church in Park City, a suburb of Wichita, whose church president was named Dennis Rader. When investigators drove by Rader's home, they saw a black Jeep Cherokee in the driveway, like the one that had showed up in old security camera footage of BTK. A forensic examination of Dennis Rader's daughter's DNA (obtained from her college's medical clinic) showed a familial match to the DNA of the semen left at the crime scene. They had their man.

The BTK killer had left behind many clues to his identity, and much of it was physical. Thirty years of analyzing that physical evidence was not sufficient to identify the right suspect. But when the killer used his church's computer to compose a weekly bulletin, and then reused the same computer and floppy disk to compose his latest missive to the press, he left a trail that led straight to his front door.

On February 25, 2005, Rader was arrested, and he quickly confessed. As he answered the investigator's many questions and told his horrifying story, there was one sticking point, one detail the BTK killer just couldn't get past. After all these years of a cat and mouse game, had he really been caught because of a deleted file?

David Kalat *is Director, Global Investigations + Strategic Intelligence at Berkeley Research Group. David is a computer forensic investigator and e-discovery project manager. Disclaimer for commentary: The views and opinions expressed in this article are those of the author and do not necessarily reflect the opinions, position, or policy of Berkeley Research Group, LLC or its other employees and affiliates.*