Forensics Work Helps Snare Arrest in Missouri Slaying

The case of a Kansas woman charged with killing an expectant mother and stealing the eight-month-old fetus from her womb likely would not have been cracked had it not been for computer forensics -- specifically the work of cyber-sleuths like Corporal Jeff Owen of the Missouri Highway Patrol.

Owen is a Computer Forensics Examiner at the Heartland of America Region Computer Crime Laboratory in Kansas City, MO. He was asked to search e-mails received on the victim's home computer. Relying on training he received through a Basic Data Recovery and Analysis (BDRA) course offered by NW3C in 2003, Owen was able to retrieve information that led authorities to arrest 36-year-old Lisa Montgomery, of Topeka, KS.

Montgomery is charged with kidnapping resulting in death from the December 2004 murder of Bobbie Jo Stinnett, 23, of Skidmore, MO. Stinnett was strangled and her unborn child was removed from her womb. The baby was later found alive at a Kansas hospital, and is doing well.

Authorities allege that Montgomery met Stinnett through a dog-breeding show, and arranged via e-mail to meet Stinnett at her home to discuss a puppy. Authorities also claim Montgomery later passed Stinnett's baby off as her own after claiming to family and friends that she was pregnant.

Owen never went to the crime scene, but he got involved in the investigation after authorities received a tip about e-mails between the defendant and the victim. Investigators picked up the Stinnett computer from the crime scene, and Detective Curtis Howard, of the St. Joseph, MO, Police Department, conducted forensics analysis on the hard drive. Once Howard was finished with the hard drive, Owen continued the forensics work.

"They knew there was a lot of metadata … so they called me immediately," he recalled.

Once the hard drive was in his possession, Owen hooked it up to a special computer drive that allows examiners to see any and all data that passed through the hard drive. Owen's computer is equipped with a special write-blocker that guards against accidental erasure of evidence.

"We see all the files in the computer that are able to be viewed," he said, "including deleted files and partially overwritten files." By doing so, Owen said, investigators can get a clear understanding of what the victim was doing on her computer -- even pinpoint exact dates and times the computer was in use.

"We had to know exactly when the victim was online," Owen said.

"We don't see the computer as a normal user would," he added, referring to booting up, starting programs, etc. "I could immediately view the files as I was imaging it, in real time."

Within about two hours, Owen said, the evidence was starting to break in the authorities' favor.

Owen traced the suspect's Internet Protocol (IP) address -- which he termed "kind of like a return address on an envelope" -- to a server operated by Qwest Communications in Virginia. A field investigator contacted Qwest, who was able to help them trace the e-mails back to a dial-up connection and phone number at the suspect's home in suburban Topeka.

Owen, who has been an examiner for about two years, attended a NW3C BDRA course taught by Charles Giglia in Jefferson City, MO, and he hopes to take an Advanced Data Recovery and Analysis (ADRA) course sometime this year. He said one always hopes that the training they receive can be used to crack cases, especially large ones. Internet and computer use is "the kind of trend we're seeing more and more of in criminal investigations."

Owen

Owen said it was personally and professionally satisfying to him to watch the case unfold and know he had a part in its investigation - a probe that is far from over. He said he expects to be busy examining cyber data as it is brought to him. Another investigative team is looking at the suspect's computer.

"It's very rewarding, especially since this was one of the most heinous crimes we had here in a long time," Owen said.