

ROCHESTER BUSINESS JOURNAL

VOLUME 23, NUMBER 13

DAILY EDITION: rbjdaily.com

JUNE 29, 2007

Forensics firm digs in computers for evidence

By MARY STONE

Forensics is not limited to analyzing strands of hair or traces of cotton fibers; it extends to computer files.

Computer forensics experts may not be looking for DNA, but they are looking for evidence—a deleted e-mail or a temporary file from a shredded and incriminating document.

Louis Germain has a new company devoted to the field. It is related to, but independent from, his computer reselling firm, Lumarc Computer Corp., he said.

Function Five Technology Group Inc.'s aim, Germain said, is to fill a gaping need for computer forensics services, which can be defined as the scientific examination of computer data, potentially to serve as evidence in a court of law.

Experts say it is an extraordinarily regimented field and costly to enter due mainly to the nature of computer forensics, which requires strict adherence to the evidentiary process. Any forensics case can wind up in court.

The goal of computer forensics is multifold and centers on confirming whether a computer crime has been committed, explained Yin Pan, assistant professor at Rochester Institute of Technology's department of networking, security and systems administration.

Data must be considered potential evidence, analyzed and preserved so examiners can look for traces of illegal activities and present admissible evidence in court, Pan said.

Right now, she said, the supply of such services does not meet demand.

"There is a bottleneck of highly trained personnel to do computer forensics work," Pan said.

Function Five has two certified examiners, to which a third soon will be added, Germain said. Investments in equipment, including a 1,500-square-foot laboratory, and certification have cost Germain \$30,000 to \$40,000 over the last 12 months.

The cost of equipment and certification provides a strong barrier to market entry. Germain said that is why the sector is underserved, and he hopes that will give the company an advantage.

Lumarc's previous extension beyond hardware reselling was asset recovery or hardware disposal. In a way, he explains. Lumarc



Photo by Kimberly McKinzie

"Computer forensics is the science of investigation: where, when, how and by whom a breach was perpetrated," explained Lumarc Computer's Louis Germain, who has started a new company, Function Five Technology, devoted to the field.

focuses on the external side of hardware, while Function Five focuses on the inside.

Lumarc ranked 10th on the Rochester Business Journal's most recent list of computer resellers with \$5.2 million in gross sales last year. The company has 10 employees.

Many of the people who have the qualifications to do computer forensic examinations are former members of law enforcement who already know procedures for handling evidence, explained Christine Siedsma, project manager at the Computer Forensics Research and Development Center at the Economic Crime Institute of Utica College.

For the people who do not have that training, she said, getting certification and the tools necessary for examining hardware are prohibitively expensive.

"I attended a conference a couple of weeks ago down in Myrtle Beach and talked to a lot of people who pretty much say the same thing—that there is such a huge demand for people in this field, for any kind of expertise," Siedsma said. "A lot of students are being hired right out of our program here, and I have to say I don't think

college programs prepare them for this kind of thing, but there's a need."

Function Five works mainly with attorneys whose clients are investigating a breach of some sort, sometimes caused by a former employee.

Because of the legal considerations, strict protocol is required for transporting and storing the equipment before, during and after the examination process.

"At the end of the day, when someone comes in with a forensics case, we have to think this case could go to court. If our examiners get called to the stand, we want to make sure they're credible," Germain said. "We built out a state-of-the-art forensic lab, where only our examiners are allowed in, with fingerprint readers, secure cameras and forensic, fireproof lockers that the hard drives are stored in."

The turnaround for forensics services is tight, usually two to three days, Germain said. That is to reduce the amount of exposure and better ensure the integrity of the investigation. Transportation is another factor and one reason Germain decided to start a forensics lab here.

Attorneys try to avoid sending hardware

out of state to better guarantee the authenticity of an examiner's findings. Clients in Rochester and surrounding areas, Germain explained, need a local examination provider.

Computer forensics is a developing field that differs from more common data retrieval services.

"Computer forensics is the science of investigation: where, when, how and by whom a breach was perpetrated," Ger-

main explained. "Basically the difference between data recovery and computer forensic, even though they're very much aligned, is that in data recovery you are looking for a specific file that you know you lost. In computer forensics, you're going in deeper and wider, and you're not sure what you're looking for exactly until you find it."

The company now has one of its examiners on a site in Boston, to avoid shipping

equipment that could serve as evidence. In that case, a company suspects a former employee of malfeasance.

"They're not sure exactly what he has done at this point. What they're looking to do is retrieve e-mails, instant messages, documentation," Germain said. "After they gather that information, they'll sort through it, and maybe find what they're looking for."

mstone@rbj.net / 585-546-8303