# Uncovering computer porn

*By Tim Grace, Enterprise staff writer*
The pictures were damaging. Image after pornographic image — dredged out of then-East Bridgewater Treasurer-Collector Frank Savino's Town Hall computer — were projected on a 5-foot screen for selectmen during a June disciplinary hearing.

Each image came with details about where it had come from, when it was viewed and who was logged onto the computer at the time — its electronic footprint.

Finding the footprints is Rod Sherpardson's job. He's a specialist in computer forensics, and can uncover almost every bit of data that has ever flickered across a computer's monitor.

Shepardson, one of two Raynham police officers assigned to the Regional Electronic and Computer Crime Task Force (REACCT, retrieved dozens of images showing men and women engaged in sex acts from Savino's machine.

"Unless someone has gone through and tried to clean up their tracks, it's really likely that what we're looking for will still be there," Shepardson said.

The pictures and other evidence were enough to cause Savino's dismissal.

Less than a month later, Abington Sewer Department Superintendent James Howell would be fired after a similar investigation, done by a different forensics group, revealed Internet pornography had been accessed from the computer in his office.

In the Abington case, the private Raynham computer firm MX Consulting was called in to conduct the investigation.

MX Consulting provides a raft of computer installation and support services, as well as forensic data recovery.

President George Kavgic said his company doesn't discuss the forensic work it does for fear of "looking a little like Big Brother."

But how do cyber sleuths like Shepardson uncover computer evidence that has long been deleted?

"There are no trade secrets," said Kevin Ripa, a forensics expert with Computer Evidence Recovery in Alberta, Canada. "We make a copy of the hard drive and see what's there."

Ripa, whose company has done forensic work in Boston for a few large law firms and a few very, very large companies, said computer users typically make only the clumsiest effort to cover their electronic tracks.

"Many of these folks believe that once they've deleted an item, it's gone forever. The truth is they haven't deleted it at all," Ripa said.

He explained that when a person drags a file over to the "recycle bin" or tap on the delete key, "all you've done is delete the table of contents entry for the file itself."

He said a computer's hard drive retains the actual file after it has been "deleted," but marks the space it takes up as available to be written over should the need arise.

So, even though it doesn't show up on a desktop or in a file folder, the data thought to have been removed is probably still intact on the hard drive.

"It's like you've gone into a library, walked up to the card catalog and burned the card for a book. Is that book gone? Of course not," Ripa said. "We go in and find that book."

Those more concerned with computer security will sometimes use what is known as "wiping software" to "overwrite each and every character on the hard drive," Ripa said.

But even then, there are likely fragments of the removed files, or references to them, drifting around in the machine's guts, waiting to be uncovered.

And what sort of things are being uncovered?

Yahoo.pcworld.com reported that half of America's Fortune 500 companies have dealt with at least one incident of computer porn in the workplace during the past 12 months, according to a study by Delta Consulting. Sex Tracker reported that the bulk of Internet porn, 70 percent, is accessed between 9 a.m. and 5 p.m.

In criminal cases, knowing what information has been stored on a computer has become a crucial piece of police work.

Since its creation in 2001, REACCT has been handling computer and video forensics for 28 police departments in the region.

Raynham Police Chief Louis Pacheco helped to get the task force off the ground.

"Most of it is child porn, but there's also Internet fraud, identity theft and missing persons investigations," Pacheco said.

"They've handled almost 1,000 cases."

Shepardson worked as a computer forensics specialist in the private sector for nearly two decades before joining the Raynham Police Department. He and officer Kelli Hutchings handle the bulk of the work that winds up on REACCT's door step.

"The first key is to get the computer," Shepardson said. "Then we make an exact copy of the entire hard drive."

Using forensic software that allows him to view data on the drive without altering it, Shepardson said he is able to see nearly everything that has ever been accessed on a computer.

Gathering evidence is one thing, but presenting that evidence in a way that will convince a jury can be challenging, particularly when the evidence is highly technical.

But Ripa, who has been on his share of witness stands, said data collected through computer forensics "can be very forceful evidence to put before a jury," in part because it's so easy to show jurists what was found on a computer and how it got there.

"I always set up a display computer with a screen so I'm showing them graphically," he said.

"Say there's a question of a picture on a hard drive. We can prove where that picture came from and we can show if the person using that computer would have known if it got there ... every picture viewed will be on the hard drive," Ripa said.

David Traub, spokesman for Norfolk County District Attorney Richard Keating, said there are some caveats prosecutors are mindful of when dealing with computer data.

It's not enough to show that something was downloaded onto a computer, Traub said. It has to be clear who did the downloading for the data to become evidence of a crime.

"You need to be able to link it back to an individual" Traub said.