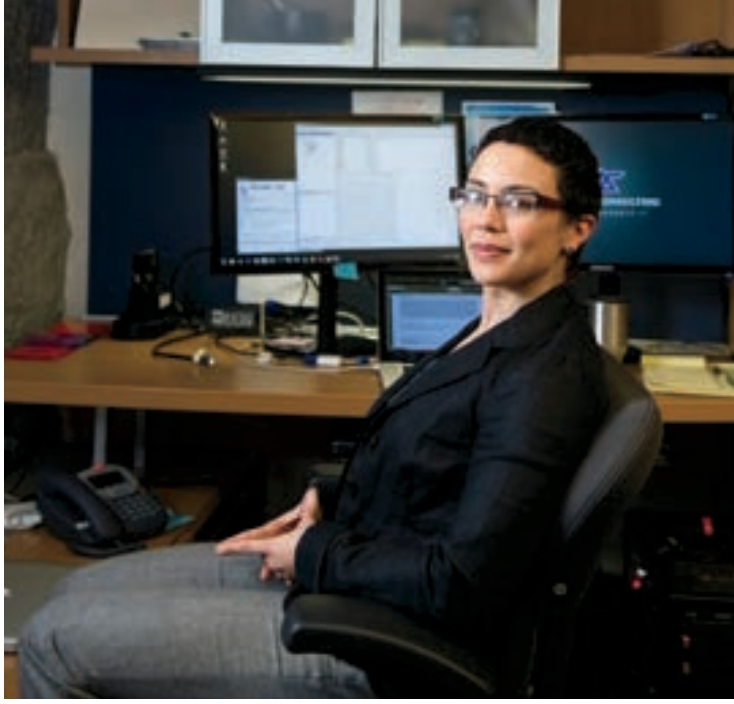
# The Cybersleuth

## As a computer forensics examiner, Lodrina Cherne tracks the digital clues



CYDNEY SCOTT

One of Lodrina Cherne's most interesting cases involved analyzing information about plans for an alleged military coup in Turkey.

THE CASE HAS been dubbed Sledgehammer, and it has led to the conviction of more than 300 officers in the Turkish military, charged with plotting to overthrow the government of Prime Minister Recep Tayyip Erdoğan in 2003. But to some, including a Harvard professor whose father-in-law was one of the officers convicted, the evidence appeared to be trumped up. To find out, he contacted Arsenal Consulting, a small firm in Chelsea, Mass., to examine CDs entered into evidence by Turkish prosecutors and a hard drive that had been seized from a military base.

One of the experts on the case was Lodrina Cherne, a computer forensics examiner with Arsenal. At first, says Cherne (CGS'02, CAS'07), the evidence did look damning. The documents on the CDs were from 2003, and they outlined plans for a coup that would be ignited by fostering unrest and bombing mosques.

A cybersleuth's job is to dig deep into the digital data, which can be found in computers and on servers, networks, removable storage drives, mobile phones, security cameras, and even in the cloud. Cherne uses software to reveal a trove of information: users on the system, last log-in time, frequently run applications, and documents recently opened, burned to a CD, or moved to the recycle bin, as well as a device's internet history.

The field of digital forensics is relatively new, and practitioners have played a role in some recent high-profile criminal cases. Technicians with the Connecticut State Police computer crimes unit, for example, extracted evidence—websites visited, images downloaded, and other information—from the computer of Adam Lanza, who fatally shot 20 children and 6 adults at Sandy Hook Elementary School in December 2012. Experts searched the computers in the home of Casey Anthony, the Florida woman who was acquitted in 2011 of killing her two-year-old daughter. (One testified that someone had searched for the word chloroform and the phrase "how to make chloroform.")

Cherne's cases aren't quite so lurid; most involve intellectual property theft. "Our clients might say, 'We think some data might have left with this employee. Can you tell us what they were doing the last week they worked here?'" she says. "We can come back and say, 'Here are the documents they were accessing on thumb drives. Here are webmail remnants we were able to recover. Here's what they were browsing on the internet. Is any of this interesting to you?'"

The Sledgehammer case was different. After analyzing the CDs, Cherne could tell that the documents were indeed created with a version of Microsoft Word that would have been in use from 2002 until now. But when she and her colleagues worked their way down to "the lowest level of the documents, almost down to the ones and zeroes," they found something troubling: a reference to a typeface called Calibri. Cherne spent weeks tracking down knowledgeable Microsoft representatives and testing versions of Microsoft Office software that would have been in use in 2003. It turns out that Calibri wasn't introduced to the public until 2007.

They found other problems: the dates and times when the CDs were allegedly burned had been forged, the computer language, XML, wasn't available to the public in 2003, and the dates and times on many of the documents had been electronically altered.

It wasn't Arsenal's job to determine whether the alleged coup had been in the works, or if, as some believe, the entire business had been fabricated. (The Harvard professor who'd contacted Arsenal wrote in the *Washington Post* last fall, "The case is widely seen as the means by which Prime Minister Recep Tayyip Erdoğan has decapitated the military, a powerful institution that has long opposed Islamist forces in Turkish society.") Rather, says Cherne, "we were able to say, at a technical level, this CD could not have been created in 2003. While our findings haven't been acknowledged by the courts over there, they have been verified by another university in Turkey and other forensic practitioners in Germany."

It's always satisfying to find a smoking gun, Cherne says. "There's somebody out there who went to such great lengths to forge documents, and at some level succeeded really well," she says. "But they didn't do it perfectly."

Cherne has long been interested in computer security, having grown up in San Francisco during the tech boom. Digital forensics fits her personality: meticulously detail-oriented, inquisitive, and focused.

She's also competitive. When Cherne is not at her desk delving into computer records, she is breaking another kind. An avid cyclo-cross racer at BU and after, she picked up powerlifting in 2010. The sport involves three movements—squat, bench press, and dead lift—all of which Cherne learned to do with an empty barbell (45 pounds). Soon she was competing, and this year, she set Revolution Powerlifting Syndicate world records in the 123-pound class, in the squat (250 pounds), the bench press (145 pounds), and the dead lift, where competitors pick up a barbell from the ground, stand up, and put it down (330 pounds).

"It's a great complement to sitting at a keyboard all day," she says. And unlike her job, she can talk about her feats at length with her fiancé if she wants. "I can only speak about cases in general terms," she says. "It's tough to come home and not have a very good answer for what I did that day." *Cynthia K. Buccini*