MAGNET FORENSICS®

CUSTOMER CASE STUDY

# Partnering to Reduce Digital Forensic Backlogs

## Fast Processes and Portable Cases Enable Forensic Examiners, Investigators to Collaborate on Cases

## THE ISSUES

- Rising digital evidence volumes
- Increased demand for digital evidence on nonviolent as well as violent crimes
- Complex cases with multiple pieces of evidence
- The need to involve investigators in cases without adding to workloads

## MAGNET FORENSICS TOOLS

- Making processing speeds faster to help reduce backlogs from months to weeks
- Enabling a greater variety of cases to be solved
- Allowing examiners and investigators to collaborate with minimal extra time using Portable Cases

**Name:** Carol Gudbrandsen

**State:** Illinois, U.S.

**Investigation Type:** Computer & Mobile

"[Using AXIOM] I can show that I have only three cases waiting, not twelve, and I know I'll deliver a short turn-around on those three."

## BACKGROUND

Located just north of Chicago, with a population of more than 700,000, Lake County, Illinois is the third-most populous county in Illinois, with 42 police departments investigating a broad spectrum of violent and nonviolent crimes.

As a cybercrime forensic analyst with the Lake County State's Attorney's Office, Carol Gudbrandsen is responsible for supporting all 42 agencies with their mobile device and computer forensic examinations. She's also a member of the state's Internet Crimes Against Children (ICAC) Task Force, which allows her to assist agencies that have no one at all to examine their digital evidence.

Gudbrandsen estimates that she processes 500-600 or more pieces of evidence per year. Of those, about 60 percent are mobile devices, with the other 40 percent being computers and tablets. Those are proportions that have shifted over the last two years. "It used to be 60/40 the other way," Gudbrandsen explains.

In prior years, limitations with tools and experience meant she could work only the most serious cases such as homicides and sexual assaults. "If someone made a request for an identity theft case, we referred them to the [Regional Computer Forensics Laboratory] because we had a six-month backlog," she says.

That's because a single identity theft case might contain 20 pieces of evidence. Such complex cases are commonplace, and not limited to these types of crimes; Gudbrandsen often joins the ICAC Task Force in the field to serve search warrants. "The task force is proactive, and we take everything—flash drives, hard drives, and so on," she says. She expects the volume to increase even further once the task force's electronic evidence dog is introduced.

However, Gudbrandsen says she's worked more than a dozen such complex cases this year, as well as a variety of lower-priority investigations, including ten drug-induced overdoses, which she notes are "just as important to those victims and their families as homicides, assaults, and ICAC cases."

## MAGNET AXIOM AND IEF INTEGRAL TO BACKLOG REDUCTION

Key to her success in decreasing backlogs and expanding her ability to address more crimes: Magnet Forensics tools, which have been a staple in Gudbrandsen's lab for many years. In one identity theft case, IEF retrieved an artifact of a bank deposit slip in PDF format. "That gave us a name and account number to run through another forensic tool. When we searched on those, all kinds of things came up," she says.

Switching from their other main forensic tool to AXIOM was a matter of ease of use. "We especially found it easier initially to put things in front of an investigator who was observing, and get to know the case that way," she says.

AXIOM's format also seemed more thorough. "It was better at parsing out data into an easily readable format," Gudbrandsen says. Justifying the new software, after learning about it through attending the annual ICAC conference and talking to other investigators, was easy, as is justifying continued licensing: "I can show that I have only three cases waiting, not twelve, and I know I'll deliver a short turnaround on those three."

From a five- to six-month backlog, using Magnet Forensic tools, Gudbrandsen's lab now can generally keep waiting times under 30 days for computers—and for cell phones, just a day or two. "That might rise to sixty days if we have a large case, but we'll have processed tons of other evidence in the meantime," she says.

## PORTABLE CASES GIVE INVESTIGATIONS TWO SETS OF EYES

A large part of the time savings that Gudbrandsen and her team have found is that they no longer have to manually pull the evidence to give to the requesting investigators. Other forensic tools, she says, are "good for certain things, but don't always tell me what's important. Information, like a second subject in an image, or a particular contact name, may have no value to me, so it is beneficial to have a detective to go over it and get a second set of eyes on the evidence."

Yet it's time- and cost-prohibitive for investigators to sit with her to go over the evidence as she finds it. It's often next to impossible to coordinate schedules, and a waste of investigators' time to sit and watch the more laborious aspects of digital forensics processing and examination.

**That's where AXIOM's Portable Case comes in. Gudbrandsen can process all the digital evidence in a case, obtain the artifacts, verify their place within the file system structure, and then offer easy-to-read reports that enable the investigators to help with an investigation to a greater extent than they had been able to before.**

"It's a way for the investigators to let me know what to do, where to start," Gudbrandsen says. "They don't have the technical expertise to know when, for instance, a drive might be partitioned or how to identify and analyze that, but they can identify and corroborate leads that I can't. It's much more thorough. If they want more information about a photo, they can tell me that, and I'll dig in the areas where I know it means something."

Portable Cases are so effective, says Gudbrandsen, that even the county's cyber attorney has begun to use them to learn where evidence resides on digital media. A tech-savvy individual, the prosecutor quickly learned how to interpret more technical aspects such as shellbags, a set of Windows registry keys that maintain directory information even if the directory or files within are deleted.

This turned out to be a critical factor in an ICAC investigation in which police knew child abuse material existed on the suspect's PC, but couldn't prove how it had gotten there or whether it had been accessed. "We were still going through all the evidence," says Gudbrandsen, "but playing around with the Portable Case enabled the attorney to find, on his own, where the shellbags showed that the defendant had copied a directory from his old PC and then accessed it on the new PC. It was the evidence the prosecutor needed to make his case."

## IMPROVING INVESTIGATIVE EFFICIENCY AND CREDIBILITY

Gudbrandsen has built these capabilities over seven and a half years—and believes this time is crucial to forensic expertise. “People think that one to two years of experience is enough, but that isn’t the case for forensics,” she says. “Only training and experience can teach you what tools to run and how to utilize them more to their capacity.”

She likens forensic tools to Microsoft Excel. “You can learn basics on your own, but it’s so powerful that when you learn how to use the additional pieces, it makes your life so much easier and your investigations so much better,” she says. “You can find evidence that would otherwise be overlooked.”

She offers databases as an example. “I now know how to decode things that the tools don’t decode from databases”—a skill that has only come with time, and has proven critical in building cases. “An IP address I found, that hadn’t been automatically parsed, was the deciding factor in whether this case was going to have a codefendant,” she says. “A few years ago, I wouldn’t have known to look for that.”

> “You can find evidence that would otherwise be overlooked.”

In fact, Gudbrandsen’s skills are such that the attorneys tell investigators not to run their own evidence if they think their case will go to trial. “A lot of them have their own tools, especially to run cell phones,” she explains, “but they’re often promoted or rotated out, and then they lose their skills and knowledge. Forgetting how they found their evidence can hurt their credibility at trial.”

Maintaining this credibility is so important that Gudbrandsen offers an unusual service: she types search warrant and court order applications for the investigators, rather than the investigators writing their own. Although this adds time to her overall workflow, she says it offers an underrated benefit. “Each vendor wants their particular language to be used,” she explains, “and most people aren’t aware of those differences. Many also don’t know to include [separate sources of evidence such as] SD or SIM cards.”

## TECHNOLOGY-ASSISTED PROBLEM SOLVING

Part of a good forensic tool, says Gudbrandsen, is technical support that helps a forensic examiner understand aspects of the tool that may not be as apparent as others, including the simplest fixes such as needing to put a Portable Case on a flash drive rather than on a DVD. “You can have the greatest tool in the world, but if tech support doesn’t get back to you for days, how great it is makes no difference,” she says.

In fact, the flash drive requirement enabled Gudbrandsen to solve a logistical problem both she and the investigators had encountered. Previously, police had to bring a drive to her lab, leave it, then return to pick it up once their evidence was processed. Not only did this add travel time to their workdays; it also meant an interruption in Gudbrandsen’s own workflow, as she would then have to reopen the case file and wait for the report to populate before saving it to the flash drive.

After obtaining authorization from the county to order 24 64GB flash drives, Gudbrandsen instituted a new policy: investigators needed only to make a single trip, to obtain the completed Portable Case. “Now, I process the evidence, create the report, save it to the drive, then email them to tell them the case is ready and they need to bring a blank 64GB drive. When they arrive, we swap the blank for the Portable Case drive, and that’s it.”

This places Gudbrandsen in a unique position to act as an advisor or consultant to investigators. She works closely with her division chief, a prosecuting attorney, to help the investigators understand what to do and why to do it that way. “I’ll advise them on what they can look for and investigate, which may then give them the probable cause they need for a warrant,” she explains, adding that she brings the benefit of this experience to the classroom: teaching the technology portion of the state’s 40-hour homicide investigator training course.

As Gudbrandsen’s experience shows, high case and evidence volumes from a very populated region don’t always have to mean lengthy backlogs or delays in justice—not even for nonviolent offenses. Rather, technology can help forensic examiners to solve investigative problems both at their own level and for detectives. This improves law enforcement efficiency, credibility, and overall service to the community throughout Lake County—and beyond.

## SEE MAGNET AXIOM IN ACTION FOR YOURSELF

If you’d like to learn more about Magnet AXIOM and how it can help find evidence you may be missing with other solutions, visit magnetaxiom.com. While you’re there, you can learn more about the product, request an in-depth personal demo from an AXIOM expert, and request a free 30-day trial.

Learn more at magnetforensics.com

For more information call us at 1-844-638-7884
or email sales@magnetforensics.com

MAGNET
FORENSICS®