MAGNET FORENSICS

CUSTOMER CASE STUDY

How Magnet AXIOM Helps Deliver Justice in South African Criminal and Civil Cases

Versatile, Speedy Forensic Software with Portable Cases Offers Competitive Advantage

THE ISSUES

- An unregulated forensic market where speed and process are competitive advantages
- Travel demands a versatile tool that can work in any environment
- Need for rapid evidence, forensically sound acquisition and processing on time-sensitive civil and criminal cases

MAGNET FORENSICS TOOLS

- Acquiring speedy, accurate evidence when investigators need it most
- Allowing investigators to deploy on any hardware that suits their examination requirements
- Making it easy to communicate with stakeholders via Portable Cases

Name: Craig Pedersen

Country: South Africa

Investigation Type: Mobile & Corporation

"AXIOM's 40-minute average processing time for cell phones is ideal when investigators seek accelerated results."

BACKGROUND

As a small information technology service provider based in South Africa, Craig Pedersen's company, The Computer Guyz, is frequently called upon to offer digital forensics services for both public and private sector clients. Whether it's corporate clients that need his team to acquire and process forensically sound digital evidence, a civil matter that morphs into a criminal case, or law enforcement that need support on a tough case, the importance of powerful tools cannot be overstated.

About 60 percent of Pedersen's cases are civil in nature. They include things like internal disciplinary matters. "AXIOM has helped us work more quickly than ordinarily to investigate matters like employees contravening company IT policy," he says. "Even features like skin tone analysis can help us find porn collections saved on company resources." He adds that the depth of searches undertaken with AXIOM has led to successful outcomes for his clients in Labour Court.

"We're very cautious with a lot of the civil cases because depending on the results and severity, they often lead to criminal prosecution for fraud or other matters, even if they start as an internal process," says Pedersen. "Therefore, we treat everything as if it will go to criminal court until we're satisfied that it won't."

> "Magnet AXIOM has helped us work more quickly than ordinarily to investigate matters like employees contravening company IT policy..."

TIME SAVINGS WITH A HIGH DEGREE OF ACCURACY

That diligence serves Pedersen and his team well in the 40 percent of criminal cases they support police with. Whether they're assisting South Africa's specialist law enforcement or provincial police services, their support helps to offset what Pedersen calls "astronomical" digital backlog among forensic services that serve 15 million people.

"The police are stretched in terms of resourcing," he explains, "so a priority crime—one that's politically sensitive, or could have a ripple effect—gets first preference in their queue." The result: given a specific brief, Pedersen's team can turn around police requests within five to seven days, as opposed to three to four months.

"Magnet AXIOM is an enormous time saver," says Pedersen, estimating that using the tool has enabled him to cut processing time by 50 to 75 percent. "We have a small team, and time is always at a premium because when we travel, that means a core skill is out of the office for a week. This puts strain on others' workload, so wherever we can gain time back is a huge benefit."

Speed also matters to casework itself. "Police generally want results soonest, particularly with cell phones that come directly out of a crime scene," says Pedersen, adding that AXIOM's 40-minute average processing time for cell phones is ideal when investigators seek accelerated results.

Pedersen's ability to provide police with professional digital forensic services is no small feat in a nation where digital forensics is wholly unregulated.

That's because most anyone with IT tools or product demo versions can declare themselves a forensic business."Just in the last year, an astronomical number of startups have begun to offer forensic services, but they do so based on products like Wonder Share's [Android data recovery software] dr.fone," Pedersen says. "It's only a matter of time before they find their evidence subject to court challenge, which won't go well for them."

To counteract this effect, Pedersen says, his company tries to follow standards, like those set forth by the SANS Institute, as much as possible within the market and its constraints. "We work as closely as we can as to what will be permissible in court," he says. The end result is a better reciprocal relationship with the police.

Pedersen estimates that AXIOM has enabled his team to cut processing time by 50 to 75%.

A COMPETITIVE ADVANTAGE IN FORENSIC ANALYSIS

These factors give The Computer Guyz an enormous competitive advantage. Detectives unable to get useful information from digital devices using the tools they have turn to Pedersen's team —and that's where AXIOM is most useful.

"We get great feedback from clients and colleagues on the depth of data we can extract using AXIOM," Pedersen says. "They may bring us a physical dump of a mobile device extracted using another tool, but they prefer AXIOM to do the analysis because of the level of data digging that the other tools don't achieve. The current recommendation locally is to use Cellebrite to root or bypass the phone to create a physical dump, then use AXIOM to drill down for the results we're looking for."

More than that, though, is the value of Portable Case in Magnet AXIOM, which has proven to be a significant time-saver and has made all the difference to third party stakeholders who must review digital evidence. "Nothing compares to the speed or depth of detail or simplicity of Portable Case file creation," says Pedersen. "AXIOM wins hands down."

He adds, "This is a great help because it's opened up a different market to us"—that of traditional investigators, whose digital skills tend to be very limited.

Even so, he says, having to rely on a forensic company for digital evidence is a hard decision for the investigators to make because it can mean someone else is doing work they might otherwise be able to bill for. This can be especially challenging in smaller matters where budget-sensitive attorneys don't want to pay for imaging and analysis, or where police need to maintain chain of custody over their data.

Those cases are where Portable Case is most useful. "Before we purchased AXIOM, we would have to do the image, analysis, and report," says Pedersen. "Now, the investigators can come into our lab and book in whatever equipment they need. We create the image and the Portable Case file. The simplicity of the file is that it's logical and easy for them to understand, to walk out the door and analyze at their own leisure."

The value is clear even in larger cases, where forensic analysis could mean what Pedersen calls, "a horrendous game of ping pong, back and forth on the phone with a constantly changing scope." Relying on AXIOM to deliver Portable Cases, conversely, empowers his clients to do the needed work themselves.

"This meets their needs and feeds their business model," says Pedersen. "None of the attorneys or advocates bat an eyelid once we've explained AXIOM... They might get the same result, but AXIOM is more robust and we don't have to explain every single step of the process. That makes it more defensible in court because AXIOM stands on its own legs."

> "Nothing compares to the speed or depth of detail or simplicity of Portable Case file creation... AXIOM wins hands down."

USING MAGNET AXIOM TO FIND EVIDENCE TO CORROBORATE WITNESS STATEMENTS

The results have been plain. In two recent cases, AXIOM recovered evidence that proved wrongdoing.

"In April we worked an internal investigation, a contractual dispute between two parties over an email that had been sent in 2012," says Pedersen. "According to Party A, the email was definitively sent to him and received around August 2012. He was only using his laptop for email and browsing, so there was plenty of slack space on the one-terabyte drive.

> "Using AXIOM, we were able to recover an attachment that everyone was adamant didn't exist..."

"Using AXIOM, we were able to recover an attachment that everyone was adamant didn't exist. Even though we couldn't recover the email itself, the fact that the attachment existed was more than adequate, and we matched the email metadata to Party A's version of events. We were impressed because acquiring data from five years back was looking for the proverbial needle in the haystack."

Around the same timeframe, Pedersen's team analyzed a digital photograph in advance of the trial of a defendant in a vehicle burglary case. In the early hours of an August morning, a homeowner had seen a man of about 5'4", wearing a red jersey, breaking into car and later, running from the scene. Security officers picked the suspect up about a block away. One of them took a photograph of the suspect.

However, no one took the suspect's clothing into evidence—and the defendant was stating that he had been wearing a white jersey, rather than the red one the witnesses were reporting. That made it his word against the security officer's.

HAVE AXIOM, WILL TRAVEL

Another advantage to using AXIOM is its portability as software, enabling Pedersen to travel as needed. Not only does he divide his time between his offices in Cape Town, Johannesburg, and Durban; he also travels throughout Africa and offshore for work. This means that relying on other forensic tools, which are bound to the MAC address of one workstation, would hamper his ability to get the job done—as would having to travel in and out of restricted or secure environments.

Instead, Pedersen simply unplugs the AXIOM dongle from his main workstation and sets it up on an i7 Nook tablet with 32GB RAM, a screen, and a keyboard. "It fits into the corner of a pocket and still works as well as a normal PC, even though it's just 18x12cm," he says. "It's very handy and versatile being able to work off that machine for quick cell phone acquisitions, or to triage anything, process a few things, exclude others, and bring back to the lab only what I need."

Using AXIOM, Pedersen's team quickly recovered the image from the phone. "It showed the defendant standing in his red jersey," Pedersen recollects, "time and date stamped perfectly according to the security officers' version of events."

In fact, he says, going to court was "an absolute breeze; our shortest court appearance ever —ten minutes!" This was significant. Pedersen explains that normally in South African courts, cases can drag on for a couple of days: defense attorneys challenge findings, and magistrates expect practitioners to justify forensic product and methodology in layman's terms. "I expected a challenge to the software," he adds, "so I literally stood and rattled off Magnet Forensics' industry pedigree before I presented the report." That report was so clear and concise, Pedersen says, that the magistrate had no questions. The report was accepted, and the defendant received a three-year sentence.

TOOL TESTING DEMONSTRATES MAGNET AXIOM BENEFITS

At the beginning of the year, Pedersen's team set up a test lab environment and purchased unused smartphones and computer hard drives. After creating a set of test data complete with photos, locations, text messages, and even control logs of their activities, they ran the different pieces of media through a variety of tools including AXIOM, Oxygen Forensic software, Susteen SecureView, Paraben E3, and others.

The point of the test was to see which tools came closest to acquiring 100% of the data. Pedersen says AXIOM came out on top, outstripping some tools "by miles" owing, in part, to its ability to acquire the widest range of data from both computers and smartphones. (In fact, AXIOM was the only tool unexpectedly to acquire additional, non-test data from a "new" Samsung Galaxy, which contained images from someone's holiday in London.)

Another factor in Pedersen's decision to purchase AXIOM licenses was its reporting, which turned out to be user friendlier in a forensic environment than other tools. And in the time trial, running on an i5 processor with 16GB RAM, AXIOM took 20% less time than other products to acquire and process data.

As digital evidence continues to challenge both public and private sector investigators in South Africa, AXIOM's strengths in processing both computers and smartphones, its speed, and its versatility all factor into a competitive advantage that Pedersen says is ultimate about doing the right thing in the right way—whether it's traveling to a client site, obtaining a faster extraction for police, or providing Portable Cases for private investigators and attorneys to move forward with their cases.

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 version.

Learn more at magnetforensics.com

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

MAGNET FORENSICS®