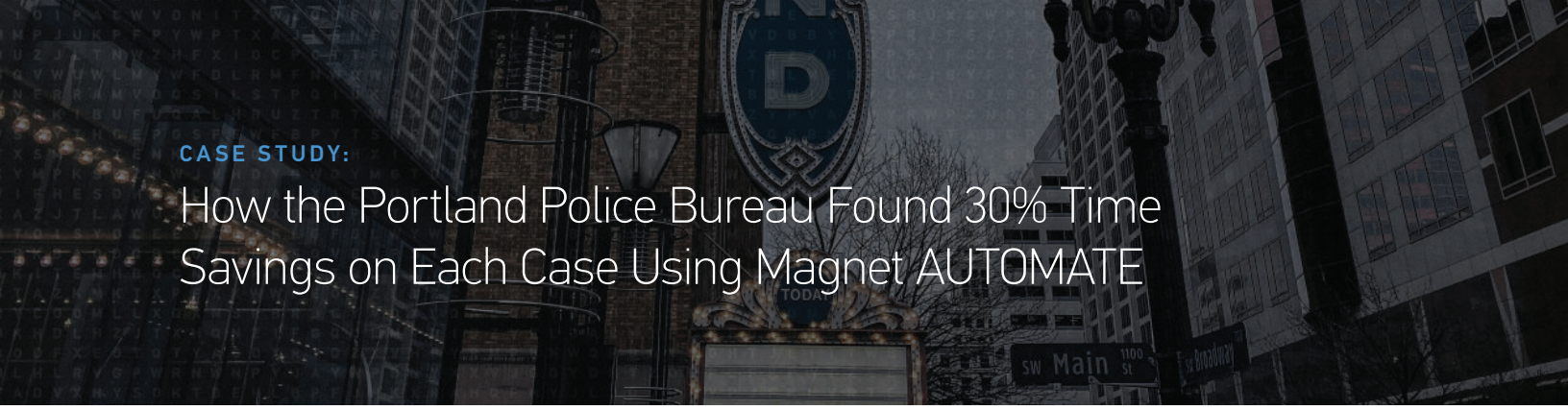


CASE STUDY:

How the Portland Police Bureau Found 30% Time Savings on Each Case Using Magnet AUTOMATE

> We recognized there had to be a better, more efficient way."

THE CHALLENGE

"One of the biggest, growing challenges all agencies face is the increasing volume of evidence coming into the lab for processing and analysis. No matter how many expensive workstations you purchase, or how hard you try to parallelize workflows, you're still working cases on a one to one basis: one examiner to run one piece of evidence through the workflow" says Aaron Sparling, Officer, Investigations Branch, Digital Forensics Unit at the Portland Police Bureau. To combat this growing challenge, Aaron's made it his mission to rethink how Portland's digital forensics lab operates with a goal of getting evidence into the hands of investigators in under 72 hours. "We took a critical look at each step of the process - we're not going to do it because that's how it's been done. However, it needs to hold up in court and so we consulted with our peers to ensure any changes we made are fully defendable, articulated, and documented."

First, he made a goal to reduce inefficiencies by minimizing the downtime between each step of the forensic workflow. But most importantly, reduce non-technical interaction with the evidence by his small team of two other examiners so that they could focus on their work, instead of keeping their tools running. "We recognized that it isn't absolutely necessary for an examiner to click a button that kicks off the imaging, processing or creation of Connections and building a Portable Case. By allowing technology to initiate these non-technical steps, the consensus was that this isn't something the defense can challenge. The tools are still imaging and processing evidence in a forensically sound way and its very defendable."

Using custom scripts and a small investment in one powerful piece of hardware, he was able to automate the imaging of three devices in sequence. This experiment proved to Aaron and his colleagues the potential time-saving power of automation in the digital forensics lab. But significant gaps of downtime — in some cases 14 hours or more — still regularly occurred. Plus, his team was still unnecessarily pulled away from their analysis, meetings, and sometimes pulled into the lab during non-work hours to ensure evidence continued to move through the workflow. The team was feeling overwhelmed, there had to be a more efficient way than manually imaging and processing evidence. A solution was needed that could automate imaging and processing across various forensics workstations to get the work done even faster and into the hands of investigators within 72 hours.

AGENCY OVERVIEW

The three digital forensics unit team members of the Portland Police Bureau are responsible for serving over 2.1 million people in the Portland metropolitan area, focusing on investigations such as:

- Major Crimes
- Dark Web
- Fraud
- Limited CSAM cases
- Incident response
- Network intrusion

BENEFITS

- Evidence guaranteed into hands of investigators within **72 hours**
- Average reduction in machine downtime estimated to be around **9 hours 43 min**
- Time saved on each case estimated to be around **30%**

Building An Automated, Integrated Digital Forensics Lab

> Magnet AUTOMATE has allowed us to get evidence into the hands of our investigators in under 72 hours. We're excited about the almost unlimited potential of the solution; partnering with Magnet's experts will allow us to continue optimizing and transforming our lab."

– Aaron Sparling, Officer, Investigations Branch, Digital Forensics Unit

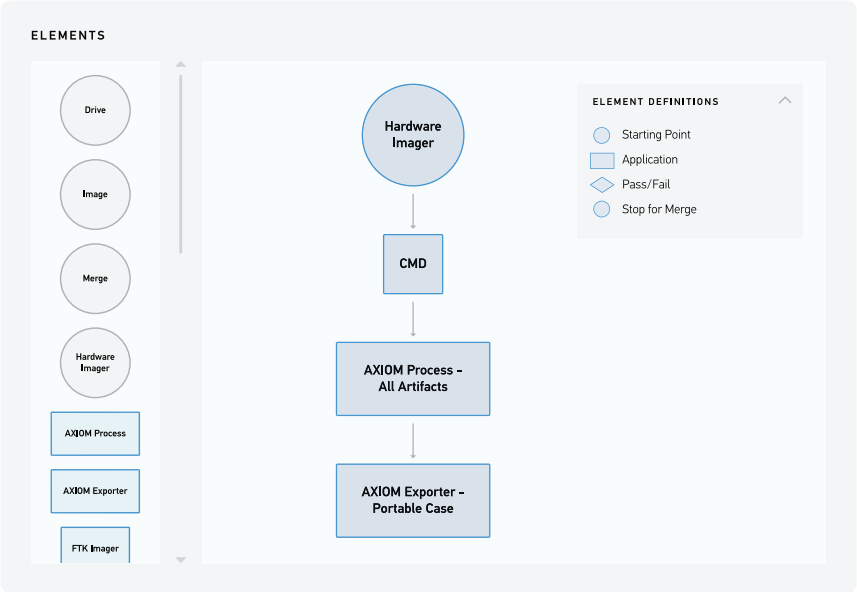
After deciding that automation and orchestration technology would help Portland's digital forensics lab achieve their goals, Aaron partnered with the Magnet Forensics experts from the Professional Services team, to assess their existing infrastructure and deploy Magnet AUTOMATE. Automation generally refers to the ability to complete a single task without human intervention, making time-sensitive processes more efficient, accurate and reliable. Orchestration refers to the ability to seamlessly optimize and streamline a series of tasks in a repeatable workflow, within a distributed network environment whether on-premises, on virtual machines, in the cloud, or as a hybrid.

Portland Police Bureau's AUTOMATE lab setup.

Every lab's infrastructure is different, and oftentimes what exists in the lab is adequate for the installation of AUTOMATE. The Magnet Professional Services team was able to successfully work with Portland's existing lab infrastructure, hardware and software. Post-installation, Aaron and Magnet optimized AUTOMATE by creating a standard workflow to automate the triage, image and processing of external drives across the available hardware and software.

With Magnet AUTOMATE, immediate improvements in turnaround time were realized. On one dark web, multijurisdictional case that consisted of 5TB of data across six PCs, one external hard drive, and two USBs, Aaron was able to triage out over half of the data at the outset leaving 2TB across two PCs to move to image and processing. **AUTOMATE completed both tasks – without any examiner intervention – in 40 hours and 48 minutes.** This is about 30% less time than the 58 hours and 5 minutes it took to process the evidence manually. By removing the need for examiner intervention between each step, the workflow can continue to progress during off hours such as evenings and weekends, saving Aaron's lab a significant amount of time.

Compound the time savings over several cases a week, and it nets out to thousands of hours saved a year. “Beginning to end, the only human interaction was attaching the drive, starting a workflow from the AUTOMATE dashboard, validate the results and we’re done,” says Aaron, as he describes how easy it is to use AUTOMATE.



Screenshot of the Magnet AUTOMATE workflow builder depicting one of several custom-built automated workflows utilized in Portland's lab.

“Without orchestration and automation in your workflow, your workflow can be very frenetic. With Magnet AUTOMATE, we were able to get back that bandwidth that is taken up by monitoring the hardware and software in between other tasks like meetings, analysis and calls. Examiners have a tough job; they experience mental fatigue and burnout at a higher rate. For us, alleviating some of that burden by removing tedious tasks and constant context switching, resulted in a huge improvement in productivity and examiner wellbeing.”

Most importantly, Aaron is excited to be able to spend uninterrupted time focusing on what matters most: serving the agency by getting them the information they need fast. “Our team serves the Portland Police Bureau; our job is to make them more successful. If we can find evidence faster, or close cases faster, that is very significant. I’m excited about AUTOMATE not just because of how it could help those of us in lab but most importantly all of the cases that move through the agency.”

ABOUT MAGNET FORENSICS

Magnet Forensics is a global leader in the development of digital investigation software that acquires, analyzes and shares evidence from computers, mobile devices, the cloud and more. Magnet Forensics tools are used by over 4000 agencies in 93 countries and has been helping investigators fight crime, protect assets and guard national security since 2011.

Learn more at magnetforensics.com/automate

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

MAGNET FORENSICS®