
MSAB

# Unlocking Evidence: How the Canadian Police Used the Power of XRY to Bring a Perpetrator to Justice in a CSAM Investigation

CASE STUDY

MSAB.com

March 2023

# Introduction

**DIGITAL EVIDENCE IS BECOMING** increasingly ubiquitous in investigations and legal proceedings around the globe. It's often pivotal in solving crimes, putting criminals behind bars, and protecting the innocent.

However, the challenges surrounding collecting and handling digital evidence persist.

The process of extracting data can be cumbersome and complex. Analyzing and making sense of it can be overwhelming and ensuring that the evidence you collect is admissible in court is a beast of its own. Not to mention the huge workloads and backlogs police officers encounter, the training (or lack thereof) concerns for both specialist and non-specialist users, and the proliferation of devices, data and encryption.

It's not easy staying ahead in the field of digital forensics, but it must be done. And with the right tools, it can be done.

Police officers from one of the largest law enforcement agencies in Canada would vouch for that.

In this case study, we focus on a recent investigation conducted by a large Canadian agency. MSAB XRY was the only product that supported a specific device seized during a warrant for a child sexual abuse imagery investigation.

Digital evidence extracted from that particular device ensured a criminal was put behind bars. But how did they manage to extract it when other tools weren't up to the task? What challenges did they have to overcome?

Stick around to find out.

It's not easy staying ahead in the field of digital forensics, but it must be done.

And with the right tools, it *can* be done.

# The Challenge

Working for one of the largest deployed police services in North America has its benefits. The organization has a big forensic team – over 50 people working in the digital forensic unit (DFU). On top of that, they have access to several forensic solutions to ensure they can access the latest devices and crack the cases that come through their unit.

In a particularly sensitive investigation, there was only one tool that turned the tide in the case when no others could: MSAB XRY.

During a warrant, a team of Canadian police officers from the aforementioned organization seized a device from a suspect, an older individual accused of being involved in a child sexual abuse imagery case.

Soon, they realized that despite having the phone in evidence, they had no way of extracting the information from the device. Which is when they turned to the experts in the DFU.

“I’ve had numerous members of my unit come to me and say: ‘We don’t have any way to get into this phone. Do you have anything for me?’” recollected one of the top investigators from the DFU regarding the first interaction with the challenging device.

Fortunately, their organization was well equipped for the task.

During a warrant, a team of Canadian police officers from the aforementioned organization seized a device from a suspect.

Soon, they realized that despite having the phone in evidence, they had no way of extracting the information from the device.

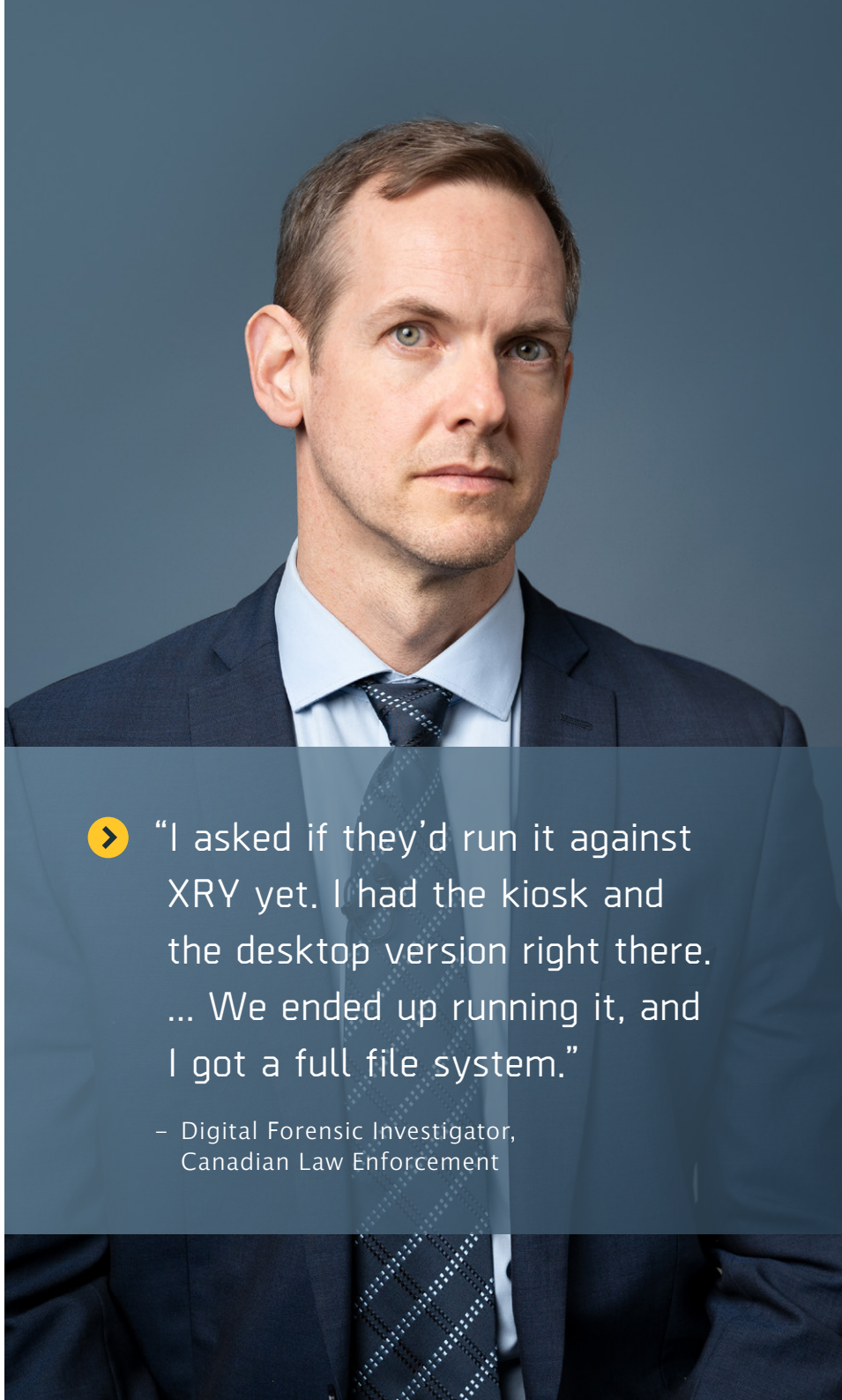
# Solution

"I asked if they'd run it against XRY yet. I had the kiosk and the desktop version right there; I checked if it was supported. I ran that model number, and I was impressed when I saw that it was. We ended up running it and I got a full file system," said the investigator.

Now that they had access to the phone data, the team was able to extract the information and further analyze it to show that it supported the case. Subsequently, they could prove that the perpetrator not only possessed child sexual abuse materials on his device, but he also had visited indecent sites containing CSAM and that he had actually downloaded indecent images to his device.

All of this data came to support the charge of child sexual abuse imagery in court.

"Without XRY we had no way of extracting that data other than maybe taking screenshots using a camera, going through the device one page at a time. But that would be painfully inefficient."



> "I asked if they'd run it against XRY yet. I had the kiosk and the desktop version right there. ... We ended up running it, and I got a full file system."
>
> – Digital Forensic Investigator, Canadian Law Enforcement

XRY proved instrumental in the solving of this case. But the tool has been crucial in extracting data from many other devices, as the investigator mentioned:

"I have personally seen several devices that were not supported by other well-known forensic software solutions, but MSAB XRY was able to provide data extractions for those devices yielding positive results for the investigations. XRY filled that void. Which is a bonus for us, obviously."

**How XRY Helps Modern Police Forces Meet the Demands of the Job:**

To ensure productive workflows, reduce backlogs, and limit the time that personal devices are taken away unnecessarily from victims and witnesses, there needs to be cooperation between DFUs and frontline officers. When frontline officers extract as much data as possible on scene, experts in the unit have more time to focus on more challenging cases, reducing backlog issues, and ultimately, increasing overall productivity of the police force. A special constable working for the organization notes:

"Part of my role revolves around enabling frontline members – patrol officers, crime units or specialty unit members to be able to process devices right on the scene, so that only the more serious offenses and the ones that really require forensic analysis and expertise come into our unit. Things such as domestic abuse, thefts, robberies, impaired driving, accident scenes, can be processed at the frontline level, and we equip them with the skills and tools to do that."

This particular organization has been using XRY as a frontline solution to steer investigations faster and acquire more productive results.

"What we manage to achieve – the number of devices that we steered away from not coming into labs is impressive. Last year, we had close to 800 devices that had been processed right then and there without the need to send them back to labs and have them sit in backlogs. And that's only with 16 copies of a program in various locations."

When frontline personnel encounter a more complicated device that cannot be extracted at the scene, that's when they bring it to the lab, where forensic experts take over – just like in the case we described.

**Six Benefits of XRY according to the Canadian police force**

Reflecting on this particular case and other investigations that were aided by XRY, the investigator highlighted the following benefits of MSAB's flagship product:

- "It's very fast."
- "The user interface is user friendly. That's a significant improvement to the product."
- "It's very intuitive. I like the fact that I can preview the devices. It shows me installed applications and then the file system down below. And through that we save a lot of time."
- "The other thing that's great is the fact that you get the choice of just getting the download and analyzing it later to speed up the process if I need to return the device back to a witness or a victim. The amount of time that I have the device in my possession – it matters because people don't want to part with their devices. Courts are recognizing that, too."
- It's very customizable. In certain scenarios, whether it's CSAM, human trafficking, counterfeiting, or money laundering, we can create custom extractions using XRY, which helps immensely when we're on scene. That way, I don't have to touch certain areas on the phone that I'm not entitled to be looking at.
  (For a closer look at **how you can tailor your extractions with XRY**, check out our **#MSABMonday** series)

**Digital forensic training is key for successful investigations**

In order to truly take advantage of XRY's full potential, it's crucial to be equipped with the skills and knowledge to operate that tool in line with your job level. That's where training makes all the difference. As the Canadian investigator highlighted:

"I train frontline officers on how to use XRY. This way, they'll know how to – in just a few steps – download a phone, unplug it, and hand it back. They're not spending half a shift in the office processing devices instead of being on the road helping the community by doing other police-related duties. Plus, if we can lower the number of devices that we bring back with us to the lab, it works for everybody."

If police officers want to expand their skillset after the initial training, they can pursue certification courses from MSAB and focus further on forensic data extraction using our XRY products.

**To learn more about MSAB's full suite of tools and solutions, visit msab.com.**