

The background image shows a man in a dark suit jacket and white shirt, seen from behind, looking towards a group of police officers. The officers are wearing blue uniforms and black helmets. The scene is set outdoors, possibly in a public square or a city street, with a large stone building in the background. The entire image has a blue tint.

MSAB

Implementing the MSAB Ecosystem saved a UK Law Enforcement Agency £80K over three years

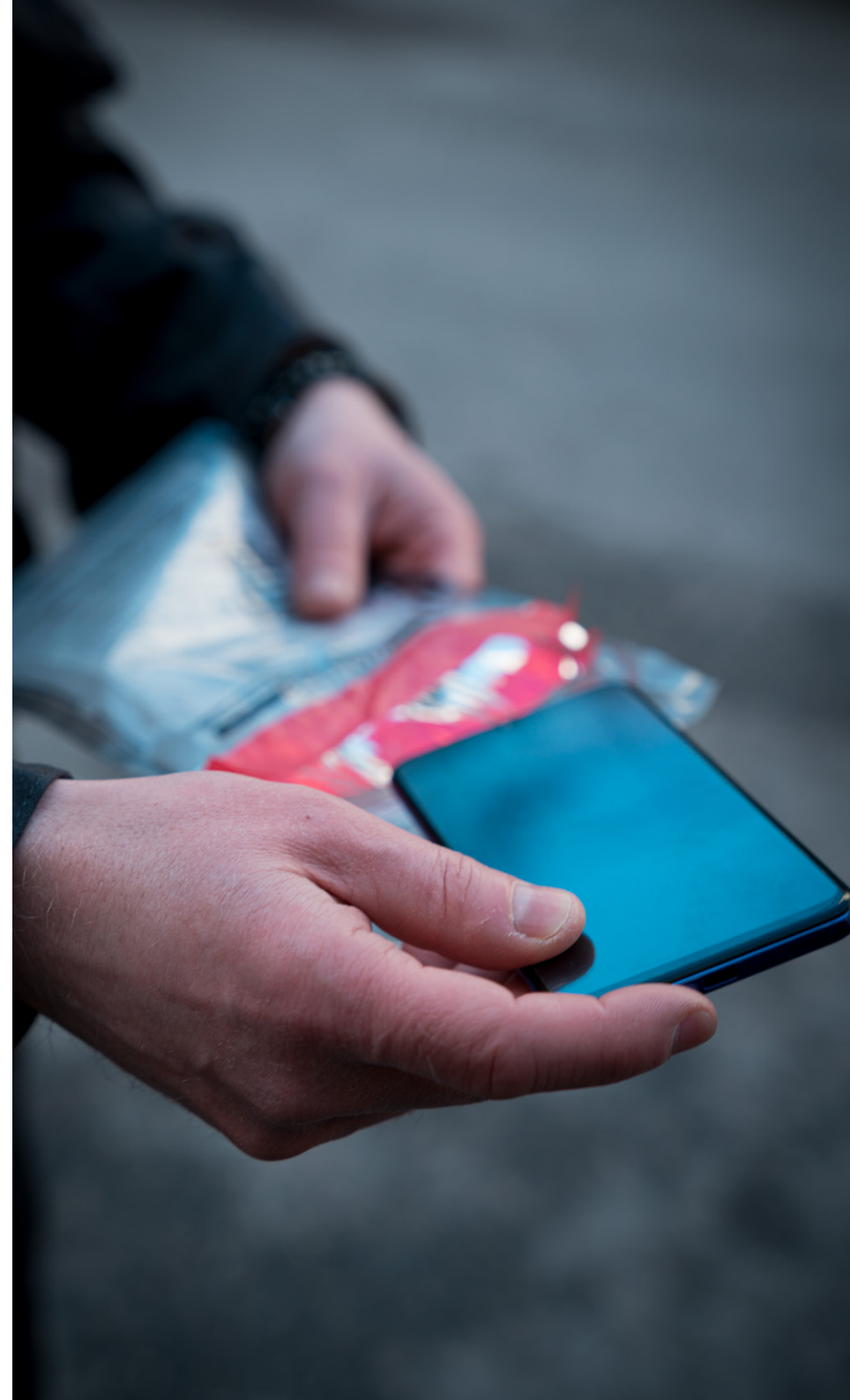
CASE STUDY

The Challenge

THE USE OF DIGITAL EVIDENCE has significantly increased in the past few decades as the courts have increasingly started to accept digital files as evidence.

Regardless of their specific missions or locations, given the enormous growth of digital evidence, law enforcement agencies and other organizations using mobile forensics face many of the same challenges:

- **The need for speed** – They need to extract and decode the data from mobile devices quickly so they can speedily view, analyze, and find useful evidence and intelligence.
- **The need for efficiency** – They need to have trained users with the right skills successfully performing extractions and analysis, at the right places and at the right times, to be able to quickly use the intelligence or evidence.
- **The need for cost effectiveness** – Public sector organizations usually operate under tight financial controls, often with limited funding, and they need to have their technology investments deliver on their objectives.
- **The need for consistent processes, data quality and forensic integrity** – Evidence recovered from mobile devices may be critical to a prosecution case and must stand up to challenges. It must be accurate, and methodology needs to be consistent from case to case.



A former law enforcement leader in a UK Law Enforcement Agency faced a number of these difficulties.

This case study tells the story of how the MSAB Ecosystem solution helped his agency speed up the extraction and analysis of mobile data and play a key role in identifying multiple people involved in organized crime.

“I was a Police Sergeant at a UK Law Enforcement Agency where we first started looking into digital forensics in 2009 as we realized that in the modern world, we needed to gather digital data.”

“We also realized that when it comes to criminal investigations, mobile devices have become one of the most important pieces of evidence for investigators as they show communications, associations and locations.”

“When we started, we just had a simple SIM reader, and at the time this was sufficient. We got some good data but the process was not efficient, nor was it future proof. Then, we decided to formalize our process and we researched all the available tools. We were after speed, completeness of download, numbers of devices supported, ethics, ease of use, etc.”

“We tested and trialed the available products, which included XRY, the MSAB data extraction solution, and matched them to our test criteria. We were looking at the speed of extraction, speed of decode, number of real phones supported, logging, forensic integrity and ease of use for the frontline user.”

“The speed was the real test, and in most cases XRY won hands down. For the extraction XRY was often the fastest, though not always, but for decode, and then presenting the results to the user, XRY always won.”

“We also found that XRY log was particularly useful for court as it gives a more detailed account of what is going on.”

“Protecting the digital integrity of the evidence and preserving the chain of custody is very important for courts. XRY extracts the data, then encrypts it and puts it into its own file format – an ‘xry’ file. This means that the original data is hidden, which in turn means there is much less likelihood that the data was tampered with.”

Reducing Case Backlog with the MSAB Ecosystem

“Later on, I took a long hard look at the processes in place and concluded that we could do things far more efficiently and cheaply if we had a network. Best practice back then was to copy all the data from the computer to a hard drive, hand deliver it to the lab, then copy it back to a computer. This was costly, inefficient and risky, all things that could be solved by using a network,” the former law enforcement leader explained.

“Having championed allowing ‘frontline officers’ to complete downloads, we found that most were not actually doing so, primarily because they were too nervous about the technology.

For us the big “ah-ha moment” came with the introduction of the Kiosks to our system.”

“A major insight was that in the vast majority of crimes like local drug dealing, burglary, robbery, etc. investigators are only after small data sets – calls, contacts, SMS and chats – so why do agencies still use highly trained and expensive Digital Forensic Experts? Surely their time would be better served dealing with devices from high priority crimes such as murders, rape, terrorism, etc.? We needed a system that would allow us to deploy the right level of expertise for optimal efficacy in both confidence, time and cost.”

“When I first saw an MSAB Kiosk being demonstrated, I quickly saw the benefits for the frontline user as the Kiosks use a workflow that could be customized to our needs. This would enable the frontline users to follow the local legislation, policies and procedures. It would also free up our digital forensic experts to deal with cases where their specialist knowledge would be invaluable.”

“I created a business case showing that by investing in MSAB Kiosks we could save time and money. Initially the bosses were skeptical – but the business case was solid and that, together with the results of our testing, was enough to allow them to acquiesce.

A few years later, we had a solution that allowed frontline users to follow a set process and enabled them to obtain a forensically sound download of a device that was automatically sent to a central server where it could be processed quickly instead of waiting for weeks for the data to be analyzed.”

“We had achieved the goal of getting a system that was both cheaper and more efficient while at the same time allowing officers to be confident that the chain of evidence would be preserved and thus more likely to be accepted by the courts as sound.”

Using the Kiosk or Tablet, frontline users with only 1 or 2 days training can complete a forensically sound extraction

“The workflow guides them through their process, which results in more devices being reliably imaged, more data getting to analysts and more crimes dealt with.”


“Using MSAB Kiosks took away most of the thought processes for the non-tech users. It also provided an extremely adaptable workflow. The MSAB Kiosk is designed for maximum ease of use by frontline officers and investigators who are not digital forensic experts. The Kiosk enables them to quickly extract and view the data on a mobile phone without delay instead of sending it to a lab. The toughest phones and those in more complex cases can still be sent to the lab for extraction and analysis by your most skilled examiners. This ability to prioritize levels of specialization allows for an increase in efficiency and productivity. Performance improves. Cases get solved faster and money gets saved.”

“The aim now was to efficiently manage the Kiosks, and for that I turned to XEC Director. XEC Director is a centralized mobile forensics management tool. It effectively controls any MSAB tool that it can see – be that Kiosk, Tablet or XRY Office. You can update the software version, the workflow, the users and what they can do, and can produce timely reporting for senior officers.”

“By the time I left the unit our agency had an Ecosystem that allowed them to conduct operations 24/7, and where data flowed from the point of collection to analysis far faster, cheaper and more efficiently, reducing from four weeks to merely hours the time taken for the data to travel. The whole system was secure and reliable, and, due to the use of the Kiosks, the frontline officers felt more confident in actually conducting extractions, so more data was being collected.”

“I know the data we collected has had a positive impact on our agency through;

- Gathering evidence to be used in trials, helping remove vulnerable people from potentially radicalizing environments, and referring subjects into the prevent program, allowing others to work on deterring them from taking a criminal path.
- Swifter justice through the early identification of offenders.
- The prevention of potentially large numbers of future crimes.
- Reductions in investigation times allowing us to move on to other cases and solve more crimes.
- Reductions in court costs, with digital forensic evidence potentially leading to an increased number of early guilty pleas and quicker trials.



➤ “By implementing the system, we saved approximately £80K over 3 years.”