MSAB

How 2 UK Police Forces dramatically improved efficiency and control by centralizing their digital evidence management

CASE STUDY

MSAB.com

March 2022

The Challenge

A COUPLE OF YEARS AGO, two UK police forces combined their digital forensic teams to save money and increase efficiency. The team included approximately 200 trained officers spread across several remote locations. They had been using XRY software to investigate anything that had a digital aspect.

But the Digital Forensic Unit was struggling with a number of challenges:

- Backlogs of mobile devices needing to be extracted and analyzed
- Computers used to store mobile forensic extraction case files were constantly running out of storage space. As a result, officers were often reluctant to download phones that needed processing
- It was difficult to keep the XRY software updated to the latest version because the computers were not linked in a network. Software updates were sent to the field locations on disks, but getting the software updated was “hit and miss.”
- Consistency and quality were difficult to maintain across all locations
- Users often changed the download profiles in spite of the unit manager’s guidance
- Individual users changed their passwords, making it difficult to recover login credentials
- Extracted case files were burned to DVDs and had to be physically transported to wherever the data was needed, requiring driving times of up to 3.5 hours and creating “a minefield of issues and constant worry.”
- “We had no idea who was accessing the machines, for what reason, how often, how much data was being downloaded, where the data was and who had access to it,” was how the Digital Forensic Analyst and Unit Manager, summed up the challenges.

"When I saw the MSAB Kiosk and learned about the network capabilities, I fell in love with it," said the Digital Forensic Analyst and Unit Manager. "But it took me literally years to get it signed off."

In the UK, all police digital forensic laboratories are required to follow the ISO 17025 Quality Management System to ensure consistency and quality in their work.

Changing the status quo: The turning point

"I argued that ISO 17025 would be implemented to the frontline of mobile forensics. So if we want to have the same capabilities for areas where we have frontline staff, in order to consistently produce valid results, then we will need a networked infrastructure in the future anyway. Why not implement it now. It will help us to become ISO 17025 compliant."

"I pitched the line that by implementing a networked environment we can have one officer in each police force downloading the data instead of sitting at their disks waiting to receive the data. Travelling around and updating units took two days. That time could be much better used helping with the investigation."

"We have 30 plus police stations staffed with people trying to get through their day to day work, so it is not unusual the when the suspect's phone information is downloaded, the person who is waiting to analyze the data is actually at a different location."

Another factor favoring a change in the status quo was the adoption of the General Data Protection Regulation policies (GDPR) protecting privacy rights and setting high monetary fines for violations.

"My argument was that if we lose a disk with someone's personal data, that's up to a one million pound fine".

Getting things done: Implementation phase

"It was super quick to get everything up once all the approvals were in order. It took us 8 weeks from the day the Kiosks arrived to "go-live,". "We didn't face any problems at all. We literally hit the button."

"MSAB was great, offering us excellent support. We had the team on the phone several times. We required team members on site a few times to help with the install and proof of testing. That happened on site before we were ready to go live. MSAB are the best at support. Since then, everything has been running smoothly."

Customer value

Since the two police forces installed XEC Director software and linked all their Kiosks, extraction files are now sent to a central server, so files are no longer burned to DVDs and each Kiosk user has his or her own folder. There is no more running out of storage space.

"The MSAB solution had a positive impact on our combined forces through;

- The data being accessible across both forces almost instantaneously so if we have a murder in one county and the investigation team are in another, there is no waiting for DVD's to arrive and copying it off the disc. We now have almost real time access to data.
- Bring able to manage all the XRY software updates by using XEC Director. This means no more wasting time driving around, plus we saved lots of money. So far, the Kiosks have been exceptionally stable, and their auto detect function has been outstanding.
- Users not fiddling with XRY after providing them with the Kiosks. Also, as the workflow is there to support them step-by-step they no longer shy away from using the software. They love how quick it is. They don't have to worry about the system crashing or running out of space.
- Users feeling empowered by the control it gives them. Software updates can easily be pushed out. If there are problems, managers are able to help users without being on site. As a manager I can see how much data we're producing. The reporting function is great for me. And as a result of being able to report clearly and concisely to senior management we are going to pursue getting more Kiosks.

— To sum up. I now have a centrally configured and controlled environment with all data saved to a central storage solution. Our users are able to use the latest versions of XRY and the XAMN mobile forensic data software. And an important additional plus is that our senior management has been seeing the benefits."

"Moving to the MSAB Kiosk and networking system was the best decision we ever made. Today for example we are better able to support high risk victims of domestic violence.

Before, relying on the lab delayed the process by at least a month. Using the Kiosk now enables us to confront the abuser with the extracted evidence in the interview, and a charge could be pressed within the first 8 hours."

– Digital Forensic Analyst and Unit Manager