WHITE PAPER

TAKE AN “ECOSYSTEM APPROACH” TO MOBILE FORENSICS: WHAT IS IT? WHAT ARE THE BENEFITS?

MSAB
SUMMARY

An Ecosystem approach puts the right mobile forensic tools in the right places with the right people and training. In some cases, all the mobile forensic computers are also linked into a single network. This approach helps organizations unlock the full potential of mobile forensics to help them fulfill their missions. It helps eliminate processing backlogs, improves the speed and effectiveness of investigations, provides oversight and reporting that managers need for efficient, high performance operations and ensures the consistent quality of digital evidence through the use of custom-designed workflows and processes.

INTRODUCTION

Being able to access and use digital evidence from mobile phones has been an important issue for law enforcement since mobile phones came into widespread use. Today, it’s hard to overstate the importance of mobile forensic evidence in most criminal investigations. It continues to grow in importance now that virtually every person carries one or multiple mobile phones, uses scores of mobile apps, uses wearable digital devices, and more. As former FBI Director James Comey, speaking to a law enforcement conference, put it: "In most investigations today, the single most important piece of evidence is a mobile phone."

But too often, the power and potential of mobile forensics are not being realized. Many police agencies send every phone to a lab, creating backlogs and delays. It can take months for investigators to get results, and cases don’t move forward.

We asked the question: “What if front-line police officers and investigators could acquire and evaluate mobile evidence in minutes or hours rather than of weeks or months?”

That was a key inspiration for designing a system of mobile forensic software and hardware tools that we call the MSAB Ecosystem, with different tools designed for specific roles, tasks and environments. For example, the MSAB Kiosk is designed for maximum ease of use by frontline officers and investigators who are not digital forensic experts, while also addressing the concerns of digital forensic professionals about maintaining high standards and the continuity of evidence.

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 the more complex cases can still be sent to the lab for extraction and analysis by your most skilled examiners. With this specialization model, efficiency and productivity go up. Performance improves. Cases get solved faster.
For most law enforcement organizations, mobile phones are extracted in order to recover digital evidence with forensically sound methods so that it can be presented and accepted in the courts.

There are multiple stages or functions in law enforcement mobile forensics operations:

- Extracting and decoding the data
- Analyzing the data to find critical evidence and intelligence
- Sharing and reporting on the evidence (with supervisors, prosecutors, other agencies and the courts)
- Managing the entire process (including reporting, tracking, updating software, managing IT policies, ensuring compliance with standards and procedures, etc.)
- Determining how best to store digital evidence and/or integrate with digital evidence management system (DEMS).

To harness the full potential of mobile forensics, MSAB products are designed based on these key stages: XRY for extraction and decoding, XAMN for viewing, analyzing and reporting on the digital evidence, and XEC for management and control.
Successful investigations rely on fast, high quality extraction and decoding of data from mobile phones. Accessing, extracting and decrypting mobile device data are frequently cited as the main challenges in mobile forensics. Forensic experts need a comprehensive set of advanced tools and skills to accomplish that with as many devices as possible.

Decoding support is often just as important as extraction. Automated decoding saves considerable time for forensic examiners, and yet it is one of the most challenging levels of support a mobile forensic technology vendor can offer.

Investigators who can acquire and analyze mobile data sooner rather than later secure an advantage. Suspects being investigated may be more likely to admit wrongdoing when confronted early on with hard facts, which can change the course and length of an investigation, leading to significant cost savings and efficiencies for the organization.

That is why enabling operational frontline users to perform extractions and analysis proves tremendously effective. The MSAB Kiosk offers the proven power of XRY mobile forensic software and has been instrumental in empowering many organizations worldwide to scale up their capabilities and decentralize their mobile forensic operations for increased efficiency, eliminating delays and device processing backlogs. With the Kiosk, non-expert users can process most devices, to free up digital forensic experts in the labs to focus on the most challenging cases.

The customizable workflow on the MSAB Kiosk enables organizations to tailor individual user sequences for different types of users and skill levels. A sequence can work like a software “wizard” which enables almost anyone to perform mobile device extractions with confidence. Step by step guides and sequences can be configured to align with an organization’s practices and regulations. They can instruct and even lock user groups to specific instructions and actions – ensuring that every user follows approved, consistent processes – in turn ensuring evidence integrity and compliance.

**THE NEED FOR SPEED**

Today, investigators and forensic specialists are often tasked with sifting through thousands – even tens or hundreds of thousands – of messages and pictures as well as gigabytes of data.

With XRY and XAMN, data is indexed once and then doesn’t need to be indexed again, so when you’re ready to view extraction data, files open quickly. No waiting. That’s true if you are opening the same file multiple times a day or multiple files.

XAMN products were designed with one goal in mind: To increase analytical efficiency and speed – so that you can find what you are looking for quickly and successfully.
The trustworthiness of the mobile forensic tools impacts the trustworthiness of the data. Investigators need to ensure the integrity of the digital evidence. This means that data collected should remain unmodified from the time it is acquired from the source through the rest of the investigation process.

Unlike some mobile forensic tools which were originally designed for other purposes, XRY was designed from its inception to be forensically secure. The XRY file format keeps evidence secure and accounted for at all times, with a full forensic audit trail and protection of the evidence from initial extraction through analysis to reporting and presentation in court or in other administrative processes.

So, your investigators and examiners can testify in court with confidence and defend the accuracy of their digital evidence, while demonstrating respect for protecting personal data and compliance with privacy regulations like GDPR.

Linking mobile forensic resources – both people and tools – over a shared network can provide multiple benefits. Data can easily be stored, moved and accessed from remote locations by different roles and teams in the organization.

However, if law enforcement agencies increase the number of people working with digital evidence and that evidence is distributed to a wider group of users, then there need to be proper controls and management systems in place. Agencies must ensure the work they do is compliant with standards and can be defended in court.

XEC is a centralized management solution that enables law enforcement agencies to connect all the MSAB mobile forensic extraction tools into a single network. It streamlines the software updates and compliance with your organization’s policies and IT security standards.

“From my experience, sitting with XEC in one central location there were huge savings to be made in time and efficiency,” said Simon Crawley, Senior Consultant at MSAB – formerly with the Metropolitan (London) Police.

With the Ecosystem approach, leaders and supervisors can track who's doing what where, safely move forensic data from point to point, set policies, and control usage. The Ecosystem makes it easy for an entire organization to cooperate and perform more effectively.
GET STARTED

MSAB provides professional services to help improve your digital forensics processes and develop personnel so that your organization can use the full potential of the Ecosystem. MSAB can help you discover and develop how to speed up workflow, boost skills and increase extraction speeds and success rates using mobile forensics.

Contact sales@msab.com or visit www.msab.com to learn more.
About MSAB

MSAB is a pioneer in forensic technology for mobile device examination. With offices worldwide and our products in use in more than 100 countries, we have a global reach. The company has been involved with mobile communications since 1984, with a singular focus on the forensic recovery and analysis of data from mobile devices since 2003. MSAB’s products include XRY software for extraction, which can run on virtually any Windows–based computer; XAMN software for analysis and XEC Director software for management and reporting.