Using mobile forensic tools in corporate investigations & e-discovery: Best practices, challenges & trends
Over the past 15 years, police departments, government agencies and the U.S. military have all increased their reliance on mobile forensic technology to extract and analyze data from mobile phones, tablets and other mobile devices --- as evidence and intelligence in crime investigations, in law enforcement operations and on hostile battlefields.

Now, mobile forensics technology is also becoming a key tool in corporate security and investigative teams’ toolkits.

Of course, corporate security and investigative teams have a different set of rules and responsibilities compared to law enforcement agencies. But they have this in common:

Today, mobile phones and tablets are much more than personal communications devices. They are essential business tools (with millions of Americans reporting they use their personal phones for company business and their business phones for personal communications), and they can store tremendous volumes of data.

A single phone with 256 gigabytes of storage can carry data the equivalent of 250 hours of video, 62.5 hours of DVD-quality film, or 78,000 photos, for example.

Former FBI Director James Comey said that in many criminal investigations today, the single most important piece of evidence is a mobile phone. The same can be said of mobile devices in corporate investigations in any of these areas:

- HR policy violations and alleged employee/officer misconduct
- Fraud, insider trading or other financial crimes
- Intellectual property theft
- E-discovery cases
- And other corporate investigations

Interested in learning more about mobile forensics?

Contact bob.bonaventure@msab.com and visit www.msab.com
An increasing share of data and communications activity by corporate employees occurs on mobile devices compared to desktop computers. The sources of evidence include emails, text messages, voice mails, contact lists, photos, videos, written documents, location data, browsing history, and a range of other digital evidence. Of course, the vast majority of corporate employees, consultants and contractors conduct themselves responsibly and ethically.

So is mobile forensic technology currently an essential tool for your investigations and e-discovery efforts? Should it be? What are other companies reporting?

We recently surveyed corporate officials with security, compliance and investigative responsibilities, and we’re publishing the results here—with an emphasis on the most intriguing responses—in an effort to prompt further conversations on this important issue.

Survey timeframe: August, 2018
Audience: Security Management Magazine subscribers worldwide
Respondents: 129 total

Here are the edited results, with a focus on the most interesting findings:

Question #1: Do you currently use mobile forensics technology to extract and analyze data from mobile devices?

20.9% of respondents say they are. These early adopters are already using mobile forensic technology, either with in-house staff or by contracting with outside service providers. On the other extreme, 18.6% of respondents are not using mobile forensics and do not currently see a need for it. The plurality of respondents were in the middle, with 60.5% responding “No, but we could potentially benefit from mobile forensic technology.”

These are companies that may begin to explore mobile forensic technology as it becomes more prevalent, as corporate champions emerge within their companies … or when the risks of not deploying it become too great.

Question #2: What factors have kept you from purchasing mobile forensic technology?

Here, respondents (who were asked to choose “all that apply”) were almost evenly split among concerns that mobile forensics would not be used often enough to justify the initial investment (49.6%), perceived price barriers (52.9%), and concerns about the skills / training needed for implementation (49.6%).

These are typical concerns for emerging technologies, and may reflect outdated perceptions about applications, costs, training, and user-friendly interfaces now available. Many companies are now fulfilling their mobile forensic needs with tools and training beginning at around $10,000 annually.
Question #4: Writing or enforcing policies that allow investigation of our employees’ mobile devices — a major challenge or not?

Not surprisingly, 43.8% of respondents report that this is a “major challenge,” with 44.4% saying it is a “minor/moderate” challenge and only 14.8% reporting that it is no challenge at all.

Drafting policies concerning the investigation of employee mobile devices should be a part of every employee/HR handbook going forward. These practices and procedures need to be a part of both HR training and employee orientation.

Question #6: More and more mobile phones are unable to be unlocked by investigators with existing tools and/or the data is unable to be decoded or decrypted — a major challenge or not?

The major phone manufacturers have added more and more rigorous security measures to mobile devices, and the challenges of breaking into locked devices seems to have influenced responses to this question, with 53.9% of respondents citing locking and decryption as a “major challenge,” and only 9.4% responding “not a challenge.”

The majority of respondents here may be considering the law enforcement challenges of breaking into locked personal devices. They should know: the rules are different with company-owned phones supplied to employees. Companies generally have the right to recover the phone and to compel disclosure of the password from their employees.

Question #11: Indicate your level of interest in providing company investigators with easy-to-use, in-house mobile forensic technologies.

This question offered respondents five options—from “not interested at all,” to “very interested.” The responses revealed the growing understanding that mobile forensic technology is here to stay and is being adopted by more and more businesses. 88% of respondents indicated some level of interest, with the highest category being “very interested” at 40.8%.

Corporate investigators and security leaders have a growing interest in mobile forensic technology. As more companies become aware of the range of mobile forensic technology options available at affordable prices and with training and support, both interest and adoption rates are expected to increase.
**Question #17:** “Improving our mobile forensic operations would help meet our department and corporate objectives more effectively.”

54.8% of respondents agreed with this statement, while only 10.6% disagree.

Even if they are not able to access mobile data currently, a majority of corporate leaders, managers and investigators recognize the value of mobile device data for their investigative work and related objectives. And they recognize the potential for improving their capabilities in this area, and seem positive that improved operations will lead to improved overall effectiveness.

**Question #18:** “I believe we should consider mobile forensics to be a higher priority than we do now.”

More than two thirds of respondents -- 68.2% -- agreed with this statement, while only 9.3% percent disagreed.

This finding is remarkably similar to the views expressed by law enforcement leaders and police officers in a similar research survey on mobile forensics, conducted in 2018 in conjunction with Police Magazine and Digital Forensics Magazine. In that survey, 64% of respondents agreed with the statement: “My organization should consider mobile forensics to be a higher strategic priority than we do now.” Many employees on corporate security and investigative teams are, in fact, former law enforcement officers so perhaps the similarity in attitudes should not be surprising.

**Other learning from the research survey:**

We asked two open-ended questions in the survey, and received very interesting responses. Here they are, with selected responses quoted verbatim:

**Question:** For my organization, the most valuable change that could be made regarding the use of mobile forensic technology would be:

“Improved ease of use”

“Easy to use tools”

“To incorporate mobile forensic technology into our day-to-day investigations”

“Developing in-house mobile forensic acquisition tools”

“Using mobile forensics as a proactive tool”

“Implementing mobile forensics and making it a must”

“Convincing the C-suite that this is a necessary and useful tool”
Regarding ease of use, it is worth noting:

#1 – Many employees on corporate internal investigations teams have prior experience as law enforcement officers and investigators, and many of those bring direct, hands on experience with mobile forensics technology with them.

#2 – Virtually every maker of mobile forensics technology has focused on delivering easy to use software, and all of them offer user training and certification to help ensure that users have the skills needed to operate successfully to extract, decode and analyze the data in their investigations. Some of these courses provide certification after only two days of training.

Question: What are other challenges you face in mobile forensics?

Quoted verbatim:
“Wearables” (such as smart watches)
“Legislative and legal issues”
“Local phone models in different geographic markets” <that are not supported as well as the most popular brands/models in the U.S.>
“Lack of trained employees with the right skills”
“Processing large volumes of data” (from mobile phones)

Should your internal investigations / security team consider acquiring mobile forensic technology?

Each company needs to make its own decision about mobile forensics technology, but the trends are clear. More corporate security and internal investigation teams are adopting and employing these tools, and as the survey data show, more companies that haven’t moved to mobile forensics are beginning to make it a priority.

If you are interested in learning more about mobile forensic technology, visit www.msab.com or contact sales@msab.com.
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.