In 2013, a panel of mobile forensics experts predicted that the year would see nine factors affecting their industry. Among them:

- "Bring your own device" (BYOD) was expected to impact the forensics industry, along with critical app data, smarter phones with tougher encryption, and malware
- Mobile operating systems were anticipated to force investigators to consider a variety of file systems and structures
- Likewise malware, which was expected to target Android devices much more strongly last year
- Mobile devices were anticipated to take center stage in both civil and criminal investigations in the year ahead

Indeed, the incidence of mobile malware infections rose by 20 percent last year, and 2013 saw several cases in which corporate defendants were sanctioned for failing to preserve or produce mobile device evidence, particularly text messages:

These trends continue to accelerate, according to survey and interview data among the Cellebrite customer base. Consumers’ increasing reliance on mobile devices means that data sources are diversifying to include social media and other apps. It also means that more people are at a greater risk for mobile malware attacks.

As a result, investigators find themselves shifting their approach to mobile device data. First, more extractions and analysis are shifting from the lab into the field. Second, they are coming to rely much more on analytics, including data filtering and visualization. Finally, they are expanding their horizons, learning new skills such as mobile malware analysis.

Consumers Increasingly Rely on Multiple Devices

According to Pew Internet Project’s research on mobile technology, smartphone, tablet and other mobile device ownership continues to increase. By comparison, the rate of ownership of desktop or laptop computers has remained relatively steady over time, an average of 76 percent of American adults between 2006 and 2012.

---

Worldwide, Nielsen’s Mobile Consumer Report stated in 2013, mobile phone adoption rates are high across both developed and high-growth countries: from 81 percent in India, to as high as 99 percent in South Korea. In addition, multiple device ownership is high in Russia and Brazil – about half the population in each country owns multiple devices – and in Italy and China, where about a third of each nation’s population owns more than one device.

It’s no surprise, then, that the ratios of mobile forensic exams to computer forensics exams have been steadily increasing as well. Statistics from three cities in North America anecdotally show this increase, which has generally trended upward since mobile device evidence began to be steadily collected around 2005.

One mainland European customer reported a ratio as high as 70 to 1 for mobile devices – smartphones, GPS devices, tablets and MP3 players – in 2013.

As for how consumers use their devices, Pew’s study reported:

- 81 percent of cell phone owners send or receive text messages
- 60 percent access the internet
- 52 percent send or receive email
- 50 percent download apps
- 49 percent get directions, recommendations, or other location-based information

All are potential sources of evidence in civil and criminal investigations, which means that mobile forensics practitioners must be prepared to manage multiple sources of data.

---

2 No standards exist for the tracking of forensic lab statistics, so not all labs report the same way. In addition, labs’ own reporting may be inconsistent from year to year. Other variables, such as trends in investigations themselves, have not been accounted for.
Extraction and Analysis Go Local, Shift from the Lab to the Field

A survey of Cellebrite customers showed that 44 percent of public sector users extract mobile data outside of a forensic lab environment, while 31 percent of litigation support users split their time between lab and field. These use cases have many variations, but all have one thing in common: the need to manage mobile evidence so that lab-based specialists can focus their expertise on the devices and cases that require deeper examination.

In the public sector, lab-based examiners may perform forensic previews of digital media while executing a search warrant at a suspect’s home or workplace. Effectively, this means that devices not found to contain evidence can be released back to their owners.

Examiners have conducted previews of computers, gaming devices, routers, digital cameras, and other media for several years, but without a way to conveniently preview mobile devices, these were often left out of the mix and simply seized to bring back to the lab. With mobile devices storing as much data, and often owned in the same quantities, as other digital media, mobile device previews are as important as those for other media.

In the private sector, a mobile forensic extraction may take place at a data custodian’s office rather than in the lab proper. This is done for convenience’s sake. Multinational firms may prefer to upload the extraction to a central server for remotely located specialists to analyze.

In-field forensics has a place on law enforcement’s front lines, too. First responders to certain complaints, or to incidents such as a motor vehicle collision, may ask to conduct a consent search in order to evaluate a complaint. A logical or file system extraction can reveal evidence that substantiates a claim of stalking, harassment, criminal threatening, or other activity. Following a motor vehicle collision, mobile device extraction can support or refute officers’ theories around whether distracted driving may have been a cause. In some states, officers may conduct searches incident to arrest in order to prevent mobile device evidence destruction.

Probation/parole officers may also, to ensure that convicts are complying with the terms of their release—that they are not associating with known gang members, or engaging in activity for which they were convicted—conduct logical or file system extractions as part of routine property searches. By comparing their results to database information, officers can quickly determine whether the convict is in violation of his/her probation or parole.

Whether in the public or private sector, broadening the range of people who have access to other people’s private data requires controls to prevent abuse. Automated mobile forensics tools should include access control and permission management.

Many organizations may determine permission management by the level of training the operator has received. If the operator is trained and certified only in logical extractions, then his or her permissions can be set only for those types of extractions. An operator with file system and physical extraction training and certification may receive permission to perform both types of extractions, or only file system extractions.
The operator’s role can determine permissions, as well. For example, a highway patrol collision reconstructionist may be trained and certified on logical extractions, but only be allowed to extract text messages and call logs—not images, videos, or other data. However, a detective or a corporate internal investigator may need access to all types of data that could potentially be important to a complaint or investigation.

Policy and standard operating procedures should govern these rules. SOPs should set clear expectations for operators and examiners at all level, including when to escalate mobile devices to specialists.

**Mobile Evidence Gets Social, Data Sources Diversify**

In general, social networking and messaging apps grew by more than 200 percent in 2013, according to Flurry Analytics, while utilities and productivity apps use grew by nearly 150 percent, and overall app usage grew by 115 percent. Indeed, Cellebrite’s survey revealed that 77 percent of respondents believed that mobile apps were the most critical data source, followed by the cloud at 71 percent. By comparison, fewer than half of respondents deemed data from offline PCs or crime databases to be critically important.

Investigators are likely to find that app data, phone-based data, cloud data all complement one another, each providing different facets of context to an individual’s life.

- An individual may use one or two apps to text- or instant-message their immediate circle of friends, but use a different app to connect with a victim
- Call logs may show heavy phone communication between two or more people, who are not the same people that the individual most heavily text-messages or emails
- The person’s social graph online likely overlaps the social graph of contacts on their mobile device — but may contain a few key differences, too

These relationships help investigators to develop stronger leads, even suspects, in a criminal or civil investigation. If the call logs show a list of contacts who were already ruled out as suspects, then the social media graph may identify entirely new regular contacts.

Mobile data relationships can also be important in developing victimology, the story of how an individual came to be victimized in a crime. A workplace or domestic violence offender may use a victim’s daily routine against him or her, stalking or attacking at a favorite coffee shop, or at home at a certain time of day. GPS app data might show this type of activity, while text or other messaging apps can show a pattern of violent, escalating, and/or persistent communications.

On the civil side, social and messaging apps can be important in employment law cases, such as establishing harassing communications or inappropriate relationships. Productivity apps might come into play in intellectual property or trade secret theft cases.
Complex investigations, like those for fraud, organized crime, and many narcotics and gang cases, require robust analytical solutions that can process data from a wide variety of sources including personal computers, servers, and others. Less complex investigations, however, require simpler tools that enable investigators to develop leads more quickly and efficiently.

Big Data, Focused Analytics

That investigators have a wealth of data to help them establish a case’s facts is irrefutable. However, the vast quantities of data can be a problem. Not all data will be relevant to a case, and investigators need ways to filter and sort it in order to arrive at actionable leads.

Timeline analysis has been foundational to digital forensics for several years. Investigators use it to narrow their focus only to content sent, received, or stored around the time an incident occurred.

However, timelines by themselves remain limited. By limiting a search’s scope to only a particular date or time, or even a range of dates or times, investigators may miss important and relevant information: an argument that occurred several weeks before the homicide, for instance, or a pattern of harassing behavior with more victims than just a single complainant.

Link and geographical location analysis further narrow down important data. Link analysis shows people’s relationships to one another, not just between mobile device owners, but also between the contacts within each mobile device. These relationships can be strong or weak based on the frequency of communication, whether by phone, text, social media, or other avenue.

Comparing these communications over timelines both before and after an incident can contextualize both normal and anomalous behavior patterns. The links can also help to identify victims and/or suspects previously unknown to investigators.

Mobile data can be key to establishing—or demolishing—witnesses’ credibility in court. Known associates and posts on Facebook can impeach or help strengthen witnesses whose attorneys, on either side, are trying to paint a different picture of their character.
The impact of analytics would be reduced without visualization. The ability to use maps, charts, and graphs to deliver concise summaries of people’s relationships to one another, events, and organizations is important for both complex and basic cases, as investigators seek to help attorneys, jurors, and judges understand where digital evidence fits in the case’s broader story.

Location analytics can provide further context by showing what places people had in common, not just during the same timelines, but also at other times. Suspects can be shown “staking out” a crime scene before committing the act, or returning to the scene after the fact. Stalkers may show up at the same times and places as their victims.

Mobile Malware Impacts Civil and Criminal Investigations

Infosecurity Magazine reported that mobile malware infections had increased 20 percent in 2013, affecting more than 11.6 million mobile devices. Sixty percent of those infections involved Android devices via third-party app stores, Google Play Store, or phishing scams; fewer than one percent of infections involved iPhone and BlackBerry devices in 2013. McAfee Labs’ 2014 Threat Predictions report noted that new Android malware samples had grown by 33 percent in 2013, while the rate of new PC malware growth was “nearly flat.”

In September 2013, IDG Connect listed prominent types of malware: Trojans that send SMS messages, steal data — including private banking and social networking login or authentication credentials — and command and control other malicious activities.

On top of that, McAfee Labs predicted that 2014 would bring the first ransomware attacks against Android devices, as well as attacks on valid apps. McAfee also expects attackers to target corporate enterprises and exfiltrate confidential information, especially as “bring your own device” continues to gain ground.

These predictions focus on mobile malware as a factor in fraud and identity theft, but mobile spyware—including keyloggers, audio monitoring, and GPS data-stealing—may also come into play in domestic and intimate partner abuse, as well as corporate and state espionage.

Investigators should not only be aware that mobile malware exists, but also how to scan for and identify it as part of their forensic analyses. This is part of due diligence in showing either that malware was or was not a factor in a crime, and either way, why it was or was not. Investigators should also be able to explain how the malware did or did not taint other evidence on the device, and why it does or doesn’t support the case against a suspect. To do this effectively, investigators require a mobile forensics tool with regularly updated malware definitions.
In Conclusion

The trends in this paper have been evolving for some time, but are quickly reaching the point where they’re no longer unevenly distributed. Mobile forensics tools have automated many of the time-consuming and painstaking methodologies that originally defined the profession. However, the higher mobile-to-PC ratio in forensics labs, together with mobile devices’ larger storage capacities and newer challenges posed by apps and malware, demands investigators to rethink the way they work.

**Offloading some basic skills, such as forensic collections, to first responder-level professionals, while adapting computer forensic best practices, such as field previews, to mobile devices.** Reducing workload in the lab means examiners are better able to focus on the data and cases that require their expertise.

**Adopting analytic and/or case management software.** Case investigators need only the most relevant data for the cases they’re trying to build. Whether it supports or refutes other evidence they’ve gathered, mobile data, and the patterns within it, are often difficult to comprehend or help laypeople to understand. Software that helps them to sort, filter, and organize timelines, geospatial data, person-to-person links, and other information helps to reduce human error in showing how people, places and events are connected.

**Learning new skills.** Whether it’s decompiling malware APK files to understand how the malware works, programming a script that extracts and decodes app data, performing complex JTAG and chipoff extractions, or learning to data carve, new skills help forensic examiners respond more readily to the challenges their cases pose.

In addition, both public and private sector entities must be prepared with policies and practices that protect consumers’ private data by controlling who access what information, under which circumstances.

**About Cellebrite**

Founded in 1999, Cellebrite is a global company known for its technological breakthroughs in the cellular industry with dedicated operations in the United States, Germany, Singapore, and Brazil. A world leader and authority in mobile data technology, Cellebrite established its mobile forensics division in 2007, introducing a new line of products targeted to the law enforcement sector. Using advanced extraction methods and analysis techniques, Cellebrite’s Universal Forensic Extraction Device (UFED) is able to extract and analyze data from thousands of mobile devices, including feature phones, smartphones and GPS devices. Cellebrite’s UFED is the tool of choice for thousands of forensic specialists in law enforcement, military, intelligence, security, government and private sector organizations in more than 100 countries. Cellebrite is a wholly-owned subsidiary of the Sun Corporation, a listed Japanese company (6736/JQ).