Yuval Ben-Moshe argues that advances in digital forensic technology are enabling examiners to perform detailed link analysis in the field, speeding investigations and potentially saving lives

JOINING THE F

The role of a forensic lab practitioner is to work within the justice system to provide key evidence for criminal and terrorist investigations. Their responsibilities include classifying and performing a forensic examination of specific pieces of evidence lifted from a crime scene which, in today's digital world, often consist of mobile devices, be it of the suspect or victim. Following the forensic process, the data collected is reported and used in building up evidence to help establish fundamental issues in a case. But, thanks to advances in technology, this traditional approach to forensic investigations is now changing.

With the number of mobile phone subscriptions increasing from one billion worldwide in 2002 to seven billion in 2014, it is clear that analysing mobile forensic data should no longer be the role of an individual or small group of select experts in the laboratory. Workloads for specialist investigators have, in some cases, become unworkable in recent years, so it is vital that field-level examiners are given the tools to extract and analyse evidence.

Limited resources and lean budgets mean investigative agencies need to find ways to empower field personnel with intuitive, investigative tools. Integrated software and hardware solutions allow them to efficiently perform simple, real-time live data extractions onsite. Raw data and reports can be shared securely via an agency's encrypted network helping to speed information sharing between the field and lab.

Advances in technology have enabled field personnel to explore one key investigative method in particular: link analysis. Link analysis is a data-analysis technique used to evaluate relationships and communications patterns used between multiple devices. As the number of mobile phone users continues to grow, the demands being placed on mobile forensic investigators are causing a substantial backlog. With the growing importance of mobile device data to investigations, backlogs of any duration – even days or weeks – can jeopardise the length and outcome of criminal cases.

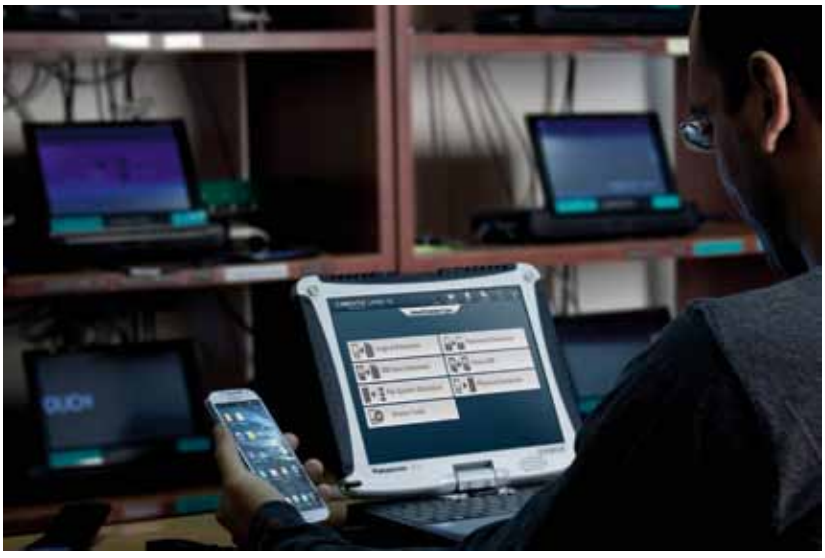
Nearly 80 per cent of respondents to a recent Predications Survey reported experiencing some level of device backlog in the last year, with 44 per cent experiencing backlogs of one to 12 months. Respondents indicated they are open to new mobile forensics solutions that support multi-tier workflows and tools to extend basic data preview capabilities to field personnel. But in order to deal with investigations effectively, there needs to be a shift in mind-set. Police authorities are recognising this, and have identified the range of new technology that can now be used for link analysis as a way of addressing the situation.

The link analysis investigative technique allows field examiners to develop critical leads during the "golden hour" of an investigation when both physical and digital evidence is most current, and therefore most crucial. Traditionally, link analysis is a rather complex method, carried out by highly skilled professionals in highly demanding technical environments with the use of very sophisticated software tools. But advances in technology, brought to the field with the introduction of new tools optimised for mobile forensics, have brought ease of use and flexibility to this powerful technique, making it more suitable for mobile forensic investigators.

The technology used in link analysis enables examiners to build an immediate visual picture of communications, and helps them understand the relationship between those involved in a criminal case, and piece the puzzle together. Detection of critical communications via texts, calls, emails and social media apps puts the power in the hands of the field examiner at a vital stage of analysis; something that would have previously been unheard of with more traditional forms of forensic investigations.

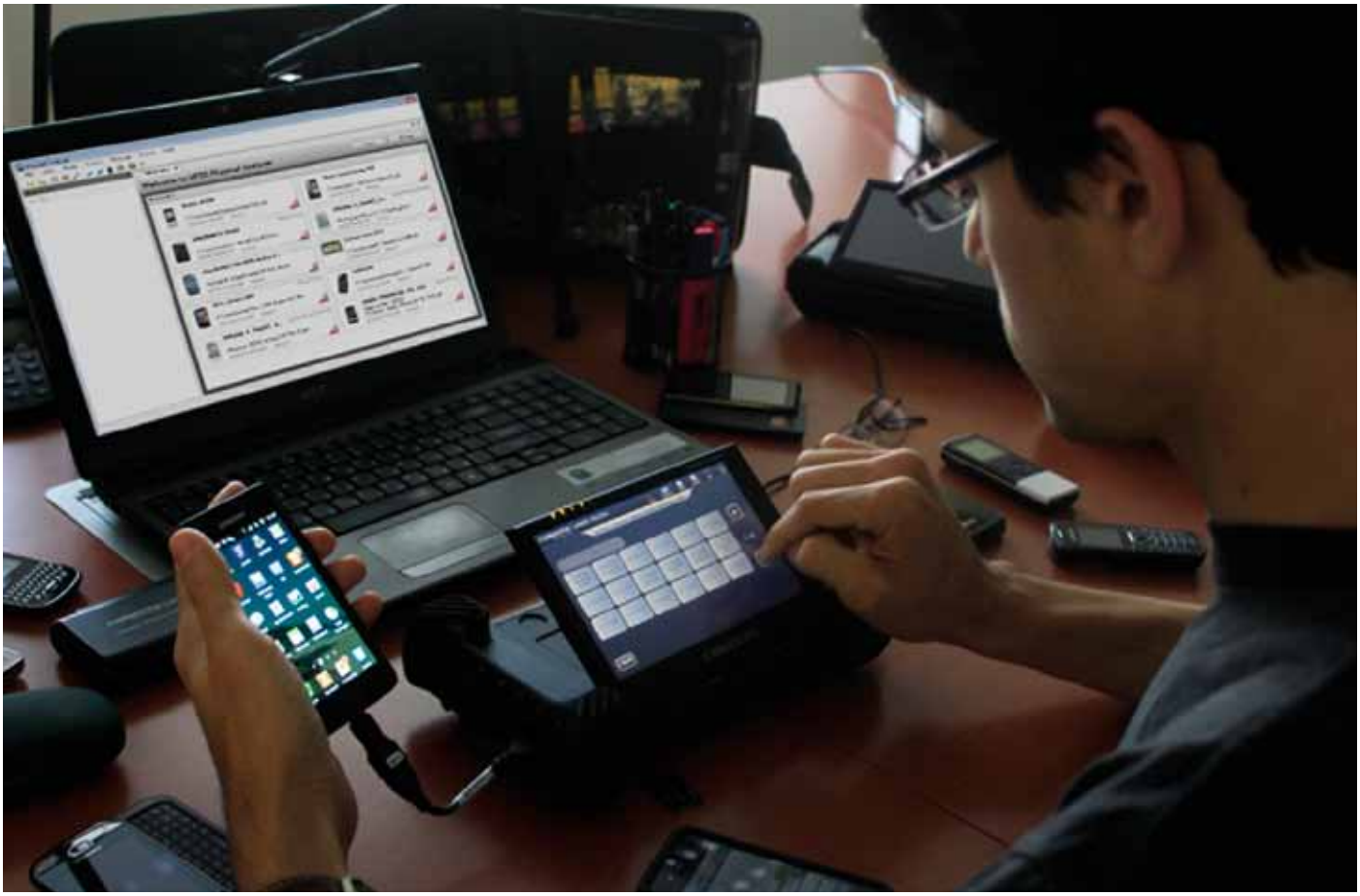
By conducting link analysis in the field, investigators can speed up their enquiries and reduce pressure on overworked labs

> **"Link analysis helps examiners to build a visual picture of communications between those involved in a criminal case"**



©Cellebrite

ORENSIC DOTS



©Cellebrite

Link analysis allows examiners to visualise case data from multiple devices, analyse mutual device users on a single map and share findings with investigators involved in the operation. There are clear steps in the process of this type of analysis, from generating physical and logical extraction reports and adding additional data and pictures, to creating watch lists and filtering information for reports. Field examiners are not just passing data to the specialist but identifying and gaining an understanding of how vital it can be to a criminal investigation. Link analysis practiced in this way has improved the effectiveness and the speed of obtaining actionable data close to where it is needed to take forward as evidence.

With some specialised training, officers involved at various stages of the investigative process can now practice it. This has alleviated the pressures on specialist investigators, allowing them to focus on analysing other types of critical data that requires further expertise – a major benefit to the investigative process.

With seven billion mobile phone subscribers across the globe, it has become essential that field-level investigators have the technology to undertake more refined critical digital evidence collection. Many criminals now use mobile devices to plan and execute criminal activity, and it is therefore vital that officers at various stages of the investigation know how to detect digital evidence. Field personnel now have access to the technology in the field that allows them to extract data and supply key evidence and make valid and insightful links between the evidential data in a case.

Mobile devices are now considered the most important data source in criminal investigations. Forensic examiners need quick and efficient ways to tap into protected data, in the cloud, as well as service provider and third-party data sources, when a situation demands. Accessing cloud-based data is a top mobile forensics challenge, but new technology exists which can deliver the exclusive capability to access third-party data to help progress criminal investigations. The ability to unify disparate data for easier analysis helps bring key insights to the surface quickly. When the popularity of the mobile phone began to grow in the 1990s, digital forensic analysis was an extremely specialist area. Today, it is becoming commonplace for officers at all levels of the investigative process to detect, extract and analyse mobile forensic data through link analysis. The technology is available and authorities are using it to draw conclusions faster and carry out criminal and counter terrorism investigations more efficiently.

Yuval Ben-Moshe is the Senior Director of Forensic Technologies at Cellebrite, a provider of forensic solutions for mobile devices including smartphones, tablets and portable GPS devices. In this role, he acts as a subject matter expert for the company and a central knowledge hub, assuring the company's tight and intimate connection with the forensics community of law enforcement agencies worldwide.