The challenges of digital forensics

March 17 2015, by Richard Boddington

Forensics is a very different business when it comes to technology. Credit: Chris Isherwood/Flickr, CC BY-SA

Forensics is changing in the digital age, and the legal system is still catching up when it comes to properly employing digital evidence.

Broadly speaking, digital evidence is information found on a wide range of electronic devices that is useful in court because of its probative value. It's like the digital equivalent of a fingerprint or a muddy boot.

However, digital evidence tendered in court often fails to meet the same

high standards expected of more established forensics practices, particularly in ensuring the evidence is what it purports to be.

Technology changes evidence

This is not the first time that technology has impacted the way evidence is gathered and presented in courts. And it's not the first time that there have been problems in the way new evidence is used.

You might remember the case of the death of Azaria Chamberlain at Ayers Rock (Uluru) more than 30 years ago. Forensics played a key role in the conviction of Lindy Chamberlain in 1982. However, her conviction was later reversed in 1988 following closer scrutiny of the evidence.

Subsequent coronial inquests, a court case featuring controversial DNA forensic evidence, and the subsequent Australian Royal Commission into Azaria's death, resulted in a fundamental reconsideration of Australian forensic practices.

There is still a vigorous debate in the legal world over the usage and reliability of DNA evidence, for example. This is now being mirrored in more recent court challenges over the use of digital evidence.

The special properties and technical complexity of digital evidence often makes it even more challenging, as courts find it difficult to understand the true nature and value of that evidence.

In fact, my first role as a digital forensics consultant is typically to act as an interpreter, explaining what the evidence means in a legal context.

Cyber evidence

It is increasingly common for criminal trials to rely on digital evidence. And, regrettably, it is not uncommon for innocents to be convicted and guilty people acquitted because of digital evidence.

There are several reasons for this. Firstly, the evidence might be compelling at first glance, but it could be misleading. The defendant may also have limited financial resources to rebut the evidence. The defence lawyers might also misread the evidence. Plea-bargaining offers can also lessen sentences.

Conversely, other investigations may not get to trial because of the complexity or incompleteness of the evidence.

Worryingly, some defendants are pleading guilty based on what appears to be overwhelming hearsay digital evidence without robust defence rebuttal. In these cases, the defence lawyer – whose job it is to analyse the evidence – may simply not understand it. This is why external digital forensics consultants can be so important.

However, the high cost of mounting a defence using forensic practitioners is often beyond the financial reach of many. For those qualified to receive legal aid, it is increasingly hard to obtain sufficient funding because of stringent budgeting regimes in various Australian jurisdictions.

Other factors can affect the validity of the evidence, including: failure of the prosecution or a plaintiff to report exculpatory data; evidence taken out of context and misinterpreted; failure to identify relevant evidence; system and application processing errors; and so forth.

Investigators undertaking these important but tedious tasks are often under-resourced, over-burdened with complex cases, increasingly large and complex datasets, etc.

Forensic analyses and evidence presentations are sometimes confounded by inexperienced investigators and communicators, which is further exacerbated by faulty case management.

Another problem issue is the paucity of reliable forensic tools and processes that meet the needs of investigators and the expectations of the courts. However, I also suspect some courts in Australia and elsewhere may be unaware of these undercurrents, or what standards they should expect of the evidence.

Getting it right

Digital forensics is still in its infancy, and it is more of an art form lacking broad scientific standards to supports its use as evidence.

There is a call among researchers to test and trial better forensic practices and forensic tools. This is especially important due to the increasing size of data storage on some personal computing devices, let alone cloud and network storage, which presents greater recovery and jurisdictional challenges to practitioners.

We also need new tools and processes capable of locating and recovering sufficient evidence from larger data sets quickly, efficiently and thoroughly. Forensic tools are often commercial products, thus profit-driven rather than science-based, and do not fulfil real forensic needs. They increasingly fail to identify all evidence from larger datasets in a timely manner. The processes used by law enforcement tend to be agency-centric with little consensus on practice, standards and processes and sharing of case knowledge.

Cyber security threats to governments, businesses and individuals highlight our vulnerability to malicious attacks on our information assets and networks. Prevention and threat mitigation is topical, but we often

overlook the simple act of bringing miscreants to justice and proving the innocence of those framed by their actions.

There is an old adage in forensics (thanks to Arthur Conan Doyle's fictional detective Sherlock Holmes): "There is nothing more deceptive than an obvious fact." This also applies to digital forensics, where I have all too often encountered cases of investigator bias and a laziness when seeking the truth.

Encouragingly, sounder tools and processes are emerging that I expect will rejuvenate this emerging discipline.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation