Can we trust digital forensic evidence?

October 2 2018

Research carried out at the University of York has suggested that more work is needed to show that digital forensic methods are robust enough to stand-up to interrogation in a court of law.

Digital forensics is the recovery and investigation of digital devices and digital materials, often related to serious crimes, such as terrorism and murder, but also more localised issues within the workplace such as employee misconduct and cyber bullying.

New research at the University of York examining digital forensic laboratories in England and Wales has shown that evidence of the accuracy of digital forensic methods may be missing from the regulatory framework.

International standards on digital forensic methods were initially created for calibration and testing laboratories, which use proven scientific techniques to test metals, chemical compounds and other industrial and manufacturing products. These are based on tried and tested methods and published industry standards.

The same framework is being applied to digital forensic labs within the criminal justice system. To understand how the framework was being met across the industry, the researchers compared the way the framework is applied to digital forensic labs with the way it works for calibration and testing laboratories.

Angus Marshall, an expert in digital forensics at the University of York's

Department of Computer Science, said: "As digital forensic scientists we are pretty confident that the methods we use to recover data and interpret it are sound, but that's not good enough to meet the standard. The challenge is to find a way to provide evidence that backs up that confidence.

"How do we show that our tools and methods are correct when we're trying to recover data from something which we haven't seen before and where the manufacturer won't tell us exactly how it works?

"There is a solution to this through accreditation and use of proven tools, much like we have in DNA analysis evidence, but this requires a unified approach from the industry and exploring the possibility of sharing the cost of it rather than individual labs having to pay in excess of £10,000."

Digital forensic laboratories are accredited by the same body that accredits DNA analysis labs, and for DNA evidence there is a standard certification that proves the validity of the methods used. The accreditation is evidence that regulatory frameworks have been met and that information can be trusted by a judge, jury, or employer for example.

Angus Marshall said: "Digital forensic methods should be tested before they're used and customers should be offered known good methods before anything else is considered.

"Unfortunately, the way the regulatory guidance has been written, it's not absolutely necessary to do this. It looks like it's possible to have a method accredited because it does what the customer wants, but this doesn't necessarily mean that it is correct.

"There's a lot of work to be done, and the industry needs to take control of it and maintain it to keep pace with new developments."

More information: Angus M. Marshall et al, Requirements in digital forensics method definition: Observations from a UK study, *Digital Investigation* (2018). DOI: 10.1016/j.diin.2018.09.004