Accepted Manuscript

Title: Digital Forensic Evidence — Flaws in the Criminal Justice System

Author: Jan Collie

PII: S0379-0738(18)30237-8
DOI: https://doi.org/10.1016/j.forsciint.2018.05.014
Reference: FSI 9307

To appear in: *FSI*

Received date: 28-4-2018
Accepted date: 3-5-2018

Please cite this article as: Jan Collie, Digital Forensic Evidence — Flaws in the Criminal Justice System, Forensic Science International https://doi.org/10.1016/j.forsciint.2018.05.014

Digital Forensic Evidence – Flaws in the Criminal Justice System

Jan Collie

Senior Forensic Scientist
Discovery Forensics Ltd,
1, Fetter Lane,
London EC4A 1BR
+ 44 20 7117 7946
info@discoveryforensics.co.uk

How would you feel if you lost your liberty because evidence was misinterpreted or misrepresented? How would you feel if you lost it because vital evidence was withheld? And what if it wasn't you but a loved one standing in the dock and you watched, helpless, as they were sentenced and taken down?

Couldn't happen here? Think again. The UK's Criminal Justice system is, as prominent prosecuting barrister Jerry Hayes has commented: ' …not just creaking but about to croak.' [1] While much of the problem lies in lack of funding, a worrying trend for the Police to be conviction focused has been noted in the press[2]. The impact of technology is also significant. The sheer volume of digital data that investigating Police officers have to trawl through has become a serious burden.

One consequence of the Information Age is that a large amount of evidence is now digital. It will be held on computers, mobile phones, tablets, all manner of peripherals and, increasingly, in the Cloud. Information everywhere means potential evidence everywhere. Knowing where to start can be difficult, even for professionals in the field. Knowing how to retrieve digital evidence, particularly in a forensically sound way, can complicate things further. But it is upon knowing how to interpret the data, once collected, that justice will hinge. And this, frequently, is where the system falls apart.

On any given day on a street near you, someone will be arrested and their mobile phone taken away. In London, that phone is highly likely to be given to a regular Police officer. That is, an officer who has hardly any applicable training outside of how to attach a mobile phone to the station forensic machine and produce a reading. In a life-or-death situation or where information is needed to contain some crisis, the help of these officers could be crucial. But for everyday policing, habitual use of this facility has wide implications. This is largely because any results that are produced will be handed to someone with even less or, more likely, absolutely nil training in digital forensics: the Officer In Charge of the case (OIC). S/he will look at the outputs and decide whether they provide useful evidence. Even where the phone is sent off to an external forensic lab, as happens in other parts of the UK, the procedure will be the same. Results from an automated analysis performed by clever software will be returned to the OIC for review. Whatever they make of it will go before the court.

If this revelation is not frightening you yet, it should be. The same sort of push-button forensics has become prevalent in computer analysis, too. In the quest to drive costs down, many contractors are using specialist software to interrogate hard disks for e.g. indecent images of children. Certain system data, web browsing history and search terms will be retrieved as will any image which appears to contain skin tones, but usually nothing else. Nothing to give the data context. Nothing to show what else was happening on the the machine when X or Y occurred. The reader of any cheap detective novel will know that nothing happens in a vacuum – solving crime involves understanding surrounding events as much as investigating the given scene. Yet once again, and without any specialist guidance, the OIC will review the outputs and make a conclusion. The chances of that conclusion being ill informed or just plain wrong are major.