Trust me, I'm a computer scientist: A comparative study in the interpretation and evaluation of computer forensic evidence

Burkhard Schafer
Joseph Bell Centre for Forensic Statistics and Legal Reasoning,
School of Law, University of Edinburgh
B.Schafer@ed.ac.uk
Izwan Iskandar Ishak
Policy Research Executive, Strategic Policy Research & Implementation,
CyberSecurity Malaysia

Abstract

The paper reports and discusses some of the results of a research project into the legal regimes governing the admissibility of electronic evidence in Europe AE2C (http://www.cybex.es/AGIS2005/general.htm) The research was carried out under the auspices of the Directorate General for Justice, Freedom and Security of the European Commission within the AGIS framework programme and coordinated by CYBEX, a provider of computer forensic services based in Spain. It involved researchers from across the European Union and the spectrum of professions involved with computer forensics, (legal academics, social scientists, police officers, practicing lawyers, technicians, businessmen, and Computer Forensic experts).

The interpretation and evaluation of computer forensic evidence in court takes place in the interface between different professional and intellectual cultures, involving scientific experts (often from different sub-disciplines in computer science) lawyers and police officers. An additional level of complexity is generated if the collection of electronic evidence involves more than one jurisdictions, and the proposed European Evidence Warrant forms the legal background for our analysis. This creates what Perkins (1999) called 'troublesome' knowledge, knowledge in the interfaces between different areas of expertise, which forces lawyers to reconsider their own assumptions about causality, plausibility and reliability of science. The research analysed how legal rules of criminal procedures in different jurisdictions facilitate or hinder rational evaluation of this "troublesome knowledge".

For this, it was necessary to go beyond the conventional "law in books" accounts common in comparative legal analysis. Rather, we tried to establish how different legal roles shape the perception of computer forensic, mediated through legal rules. Our approach combined a "leximetric" (Siems) approach with semantic or conceptual network analysis. Structured interviews of different legal actors were carried out and analysed using traditional content and structural analysis, and semantic or cognitive networks. The latter is a novel method which focuses on the interaction between the elements observed, whatever their level of aggregation (significant, individual, groups, or organizations) may be.

After first introducing this new methodology, we describe the findings for two of the jurisdictions analysed, Germany and the UK as representatives for inquisitorial and adversarial system respectively. We focus on the notion of "trust" as the crucial "glue" that ties different stakeholders in the criminal justice process together. Under which conditions can or should legal actors put their trust in either computer scientists or computer technology, and what role do laws, best practice guides and police manuals play in building up this trust?

Some of the results seem paradoxical: trust seems highest in jurisdictions where objectively, it is least warranted. We develop an explanation that draws on socio-legal research into the wider issue of "trust rich" and "trust poor" societies (Fukajama) In a final step, we test the validity of our analysis by comparing the results against a non-European jurisdiction, Malaysia.