The first e-Forensics conference attracted a specialist crowd of 70 digital forensics researchers and practitioners from around the world to hear over 30 papers on a diverse range of digital forensic topics. One of the aims of the conference was to recognise that digital evidence gathering and analysis now goes well beyond conventional data security, audit trails and data recovery. Digital still and video cameras, mobile phones and of course combined units are now ubiquitous and have wide applications in both crime and law enforcement. The Internet offers new opportunities both to commit crimes and to combine efforts to solve crime across international borders.

It is therefore timely to consider how to investigate a diverse range of digital evidence, and how to analyse that evidence to the advantage of a criminal or civil investigation.

This collection of papers has been chosen in part to highlight the diversity of digital forensics research, and represents a mere sample of high quality research papers presented at the conference. Authors have extended their papers to include additional background, clarification or updated results.

In *A Model Based Approach to Timestamp Evidence Interpretation*, Willassen formulates an algorithm for the analysis of file system timestamps. Such analysis can indicate tampering with timestamps or internal clocks to identify where file manipulation has occurred.

In *Conditions for Effective Detection and Identification of Primary Quantisation of Re-Quantized JPEG Images*, Sorell considers the effect of requantisation of JPEG images and the conditions under which residual evidence of the primary quantisation of the JPEG image can be detected and estimated. Such a technique is a useful tool in digital image provenance, particularly in identifying the characteristics of the source camera.

In *Conducting Forensic Investigations of Cyber Attacks on Automobile In-Vehicle Networks*, Nilsson and Larson consider the possibility of tampering with computer-controlled motor vehicles, the potential contemporary equivalent of cutting a brake line or otherwise causing a vehicle accident. They formulate the requirements for auditing the embedded computer control units to provide both security and post-accident analysis.

In *Reversible and Blind Database Watermarking*, Gupta and Pieprzyk propose an algorithm based on difference expansion to distribute a distorted database which can be restored by sup-
plying a secret key, with applications in Digital Rights Management.

Eggendorfer investigates the junk email (spam) industry and proposes the mechanism of distributed tar pits to track email address harvesting as a means of reducing spam in *Methods to identify spammers*.

While virtual reality might seem quite a long way from real-world crime, in fact virtual environments are likely to become increasingly important as places where people trade virtual objects or where real business meetings take place and where real money changes hands. Sablatnig et al therefore consider a key question in *Dealing with Multiple Truths in Online Virtual Worlds*, which is how to establish the meaning of truth in an environment where simulation takes place on multiple platforms and so multiple versions of the truth may exist. This is not merely a philosophical question but a key challenge which the law will at some stage need to address in resolving disputes which occur in such virtual environments.

The conference Web site is www.e-forensics.eu.

Matthew Sorell
General Chair, e-Forensics 2008

Matthew Sorell is senior lecturer in telecommunications and multimedia engineering in the School of Electrical and Electronic Engineering at the University of Adelaide, South Australia. He is general chair of e-Forensics - the International Conference on Forensic Applications and Techniques in Telecommunications, Information and Multimedia; an associate editor of the International Journal on Digital Crime and Forensics, and a recent Short-Term Visiting Fellow at the University of Warwick. His research interests include a range of commercially relevant telecommunications topics, public policy relating to regulation of multimedia entertainment, and forensic investigative techniques in multimedia. He holds a BSc in physics, a BE in computer systems (with first class honours) and a Graduate Certificate in management from the University of Adelaide, and a PhD in information technology from George Mason University (Virginia, USA).