Guest Editorial Preface

Theo Tryfonas, Faculty of Engineering, University of Bristol, Bristol, UK

Nathan Clarke, Digital Forensics Laboratory (CSCAN), Plymouth University, Devon, UK

Ron Dodge, Army Acquisition Corps, United States Army, United States Military Academy-West Point, West Point, NY, USA

This year's workshop ran again in conjunction with the Symposium on Human Aspects of Information Security and Assurance (HAISA 2012), as it has been the established pattern over the past years. We were privileged to host both events alongside IFIP TC-11's flagship conference, the 27th IFIP International Information Security and Privacy Conference (IFIP/SEC 2012). To this effect we were also delighted to receive the kind support of IFIP's TC11.8.

The event attracted once more a truly international audience, comprising over 40 delegates from four continents. WDFIA's track featured a selection of thirteen paper presentations, accepted after a rigorous double blind peer-review process, which considered a total of twenty-one original submissions.

A further review of the accepted papers resulted in the selection of the four extended articles contained within this special issue. We are pleased to have included high-quality works addressing issues extending from the very scientific foundations of the discipline of digital forensics (Batten et al. & Haggerty et al.) to engineering and technology applications (Lempereur et al.) as well as the related investigative processes (Vlachopoulos et al.).

Batten et al. discuss the need for an automated approach to forensic digital investigation. They aim to assist the forensics investigator with the generation and testing of hypotheses in the analysis phase. In doing so, they present a new architecture which facilitates the move to automation of the investigative process; this new architecture draws together several important components of the literature on question and answer methodologies including the concept of 'pivot' word and sentence ranking. Their architecture is supported by a detailed case study demonstrating its practicality.

Haggerty et al. discuss the increasing use of social media and applications or platforms that allow users to interact online and how current tools for the examination of digital evidence find this data problematic as they are not designed for the collection and analysis of online data. Their paper presents a framework for the forensic analysis of user interaction with social media. In particular, it presents an inter-disciplinary approach for the quantitative analysis of user engagement to identify relational and temporal dimensions of evidence relevant to an investigation.

Shifting to the engineering and technology side of digital forensics, Lempereur et al. discuss how live digital forensics presents unique challenges with respect to maintaining forensic soundness, but also offers the ability to examine information that is unavailable to quiescent analysis. They identify numerous approaches to live digital forensic evidence acquisition in the literature, but note that relatively little attention has been paid to the problem of identifying how the effects of these approaches, and their improvements over other techniques, can be evaluated and quantified. In their paper, they present a novel platform enabling the automated, repeatable analysis of live digital forensic acquisition techniques.

Vlachopoulos et al. discuss how the boundaries between traditional crime and cybercrime are vague – a crime may not have a defined traditional or digital form since digital and physical evidence may coexist in a crime scene. Various items found in a crime scene may worth be examined as both physical and digital evidence, which they consider as ‘hybrid’ evidence. In their paper, a model for investigating such crime scenes with hybrid evidence is proposed. Their model unifies the procedures related to digital and physical evidence collection and examination, taking into consideration the unique characteristics of each form of evidence.

The above were some of the key highlights of a particularly enjoyable workshop, which explored key issues such as scientific approaches to analysis of digital evidence and appropriate investigative frameworks. We would like to encourage readers to visit the workshop’s web page (http://www.wdfia.org) and to look out for next year’s call for papers. In 2013 WDFIA is organised once again alongside HAISA and other IFIP events, this time in beautiful Portugal.

Theo Tryfonas
Nathan Clarke
Ron Dodge
Guest Editors
IJDCF