J Comput Virol
DOI 10.1007/s11416-006-0018-9

ORIGINAL PAPER

Winning the battles, losing the war? Rethinking methodology for forensic computing research

Vlasti Broucek · Paul Turner

Received: 13 January 2006 / Revised: 11 February 2006 / Accepted: 16 April 2006

Abstract In the last 10 years, Forensic computing (FC) has emerged in response to the challenges of illegal, criminal and other inappropriate on-line behaviours. As awareness of the need for the accurate and legally admissible collection, collation, analysis and presentation of digital data has grown, so has recognition of the challenges this requirement poses for technical, legal and organisational responses to these on-line behaviours. Despite recognition of the multi-dimensional nature of these behaviours and the challenges faced, agreement on coherent frameworks for understanding and responding to these issues, their impacts and their interrelationships appears to remain a long way off. As a consequence, while significant advances have been made within technical, organisational and legal 'solution centred paradigms', the net result appears to be a case of 'winning the battles but losing the war' on computer misuse and e-crime. This paper examines this situation and reflects on its implications for academic researchers' methodological approach to understanding and responding to these challenges. This paper suggests the need to reconceptualise the term 'solution' and advocates an additional methodological step, (that it is anticipated will generate data) for the development of a framework to map the value propositions of, and interrelationships between the individual sets of responses within the dynamically evolving FC landscape. By exposing issues, responses and underlying assumptions it is anticipated that this will improve the possibility of calibrated responses that more effectively and coherently balance the interests for security, privacy and legal admissibility.

V. Broucek (✉) · P. Turner
School of Information Systems, University of Tasmania,
Private Bag 87, Hobart, TAS 7001, Australia
e-mail: Vlasti.Broucek@utas.edu.au

P. Turner
e-mail: Paul.Turner@utas.edu.au

1 Introduction

The last decade has seen an explosion of research and development by computer security specialists, legal professionals, information managers and others on technical, legal and organisational issues arising from illegal, criminal and/or inappropriate on-line behaviours. Researchers drawn from a variety of disciplines have explored different aspects of the issues and advocated different solutions to these forensic computing (FC) challenges (for example [31,35–37]). To date however, despite numerous attempts, there is a lack of agreement on frameworks for either understanding and/or responding to these issues, their impacts and their interrelationships. This can partly be explained by the fact that with growing demand for practical solutions to the challenges faced, different business, legal and organisational imperatives drive developments in ways that militate against coherence in the name of competitive advantage.

Significantly however, it is evident that this lack of coherence is of more than purely academic interest and has, directly inhibited awareness of the issues and challenges in the community, impaired the development and diffusion of specialised FC skills and, most importantly, impacted directly on the effectiveness of responses to computer misuse and e-crime [12,14]. Indeed, whilst many FC specialists have advocated the need for more integrated solutions that balance the requirements for network security, individual privacy and legally

admissible digital evidence, there remains little evidence of these emerging.

From the perspective of academic research this situation raises a series of questions about the nature of the discrete technical, organisational and socio-legal responses being developed towards computer misuse and e-crime, including:

- What is the nature of the frameworks that individual sets of responses use to conceptualise the issues and challenges their solutions aim to address?
- How do individual sets of responses conceptualise the relationships between themselves and other sets of responses?
- What key value propositions underpin individual sets of responses and how does this influence their perceptions of what constitutes a solution?
- How can a framework be developed that will more explicitly map the value propositions of, and interrelationships between the individual sets of responses?

This paper considers these issues and reflects on their implications for academic researchers' methodological approach to FC research. The paper commences with a review of attempts to define and model the FC domain. This review highlights the limited agreement that exists on models for understanding and/or responding to issues, their impacts and interrelationships. The paper also presents evidence highlighting how the interrelatedness of these issues means that responses in one area can have negative consequences for developments in another area, thereby inhibiting the overall effectiveness of the current approaches. On the basis of this analysis, the paper acknowledges that whilst, in the short term at least, technical, organisational and legal responses to computer misuse and e-crime will remain fragmented, academic researchers need to reconceptualise the notion of a 'solution' and take steps to develop a framework to map the value propositions of, and interrelationships between these individual sets of responses. In this context, the paper outlines an additional methodological step that is anticipated to generate data that will enable the development of this framework. By exposing issues, responses and underlying assumptions it is anticipated that this will improve the possibility of calibrated responses that more effectively and coherently balance the interests for security, privacy and legal admissibility.

1.1 Models and frameworks: a help or hindrance?

Previous research has identified the absence of an overarching conceptual framework for FC and revealed how this has contributed to limiting exploration of the interdisciplinary dimensions of issues concerned with the identification, collection and analysis of computer evidence [7,8]. However, given that this paper is directly concerned with the reasons for, and methodological implications of this lack of coherence, the first part of this paper reviews existing models and frameworks as a way to explore their differences and underlying suppositions.

In this context, it is first important to examine the definitional ambiguity that has surrounded FC itself. In this regard, the following definitions can be presented as being representative of the range of definitional approaches:

- The process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally acceptable [28].
- Gathering and analysing data in a manner as free from distortion or bias as possible to reconstruct data or what has happened in the past on a system [21].
- The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorised actions shown to be disruptive to planned operations [29].

As the above quotes indicate, Forensic computing (it is useful to note that the term 'forensic' is defined as: 'used in or connected with court of law' [24]) has continued to remain problematic to define. Broucek and Turner's [7,8] preliminary taxonomy of FC highlights how, as an academic discipline, FC builds on knowledge drawn from several other fields of expertise. This taxonomy also illustrates the broad range of issues and approaches within FC and suggests the following working definition of FC as being:

> Processes or procedures involving monitoring, collection, analysis and presentation of digital evidence as part of 'a priori' and/or 'postmortem' investigations of criminal, illegal or other inappropriate on-line behaviours.

Subsequent work expanded this initial taxonomy to include law enforcement and the basic taxonomy of the FC domain is illustrated in Fig. 1. For further information on this approach refer to [7,8,25,26]. It should, however, be noted that this taxonomy is by no means

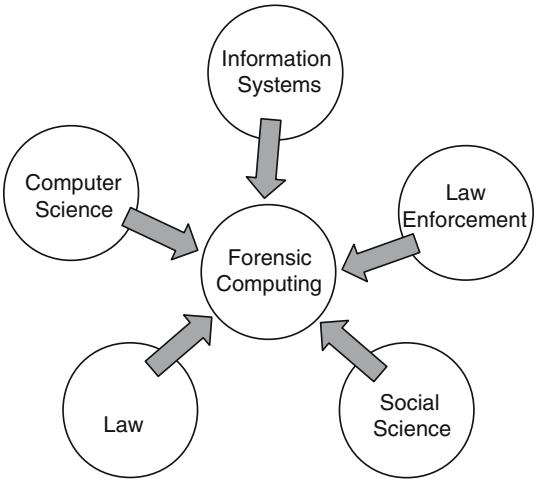

Fig. 1 Forensic computing domain

the only attempt to define the domain.Indeed, as a result of work at the First Digital Forensic Workshop (DFRWS) in 2001 an entirely different approach based not on constitute disciplines but rather specific fields of computer forensic activity led to the development of an alternative model referred to as the 'Nucleus of Digital Forensic Research'. This model is displayed in Fig. 2. Interestingly, both the 'taxonomy' and 'nucleus' frameworks emphasise the need to stimulate cooperation and collaboration amongst the various disciplines and fields concerned with forensic computing issues. The same urgency to support interaction and collaboration has also been suggested by Spafford [cited in ref. 29, p. 7]. Spafford argues that it is necessary:

- To abandon the current 'band aid approach' to forensics. The same approach was and still is often observed in the security world – the security elements are added into the existing or new systems, instead of designing the systems with security already built in.

Fig. 2 Nucleus of digital forensic research (from [29])

- To know exactly how much information and what type of it needs to be collected for further analysis in particular circumstances.
- To understand social aspects of 'the game'.

Spafford concludes that in the FC domain 'All aspects of the problem are essential. Therefore, it is imperative that each collaborates with the other. Researchers, investigators, legislators and jurists must all work toward a central goal. This requires constant discussion within groups that have representation from all essential parties' [cited in ref. 29, p. 7].

What is significant about these remarks is that despite their apparent conformity and agreement, an academic analysis of the work arising from, for example, the First Digital Forensic Research Workshop reveals the markedly different aims/goals/objectives underpinning the approaches of different domain experts.

As the presentations of the main speakers at the DFRWS workshop illustrate (i.e. Eugene Spafford representing academic research and government, Charles Boeckman representing DOD operations, Chet Hosmer representing commercial tools development, David Baker representing critical infrastructure protection and John Hoyt representing law enforcement), the different underlying positions can be summarised as follows:

- Law enforcement agencies appear primarily interested in gathering evidence that can later be used for prosecution. It is worth pointing out that such evidence must follow rules of evidence established by particular jurisdiction to maintain evidential integrity (chain of custody) and that the digital evidence should form a part of 'whole case' and non-technical elements should also be taken into an account.
- Business requirements are more or less driven by economic pressures of remaining viable and competitive.
- Academics are interested in exact, scientific methods and data and the advancement of new knowledge.
- Military and Information Warfare Operations are mainly interested in what is referred to as Defensive Information Operations (DIO). DIO represents a multi-disciplinary approach to protecting digital systems. It includes communication, computer, information and operational security as well as physical security and other tactics used in active systems protection. The main differentiation of defence operation requirements from those in law enforcement is the willingness of DIO to sacrifice absolute and/or even measurable accuracy for quickness in order to serve a mission's timeline.

The result of DIO is research conducted in defence operations concentrated mainly on:

- Optimisation of data collection
- Minimisation of data corruption or destruction risks
- Accommodation of operational time constraints

Table 1 adapted and extended from Palmer [29], clearly demonstrates that investigators from each area deploy different paradigms when approaching FC and its analysis. Furthermore, the workshop appears to agree that they also attempt to do this in different environments (that the authors here would prefer to call time frames). Significantly, it is suggested that law enforcement is only interested in 'post-mortem' while all the other players tend to anticipate and try to take an action to thwart a possible threat even before it happens including such factors as financial cost, reputation and service availability. It is noticeable that the approach advocated by DFRWS can be directly linked to models that subsequently emerged focused on how to respond in conducting/implementing FC investigations. Broadly, these models can be divided into three categories: simple, advanced and complex. These are discussed below.

1.1.1 Simple models

Arising directly out of the DFRWS was the development of seven-step linear model, for the conduct of FC investigations:

- Identification
- Preservation
- Collection
- Examination
- Analysis
- Presentation
- Decision

Reith et al. [30] extended this model to nine steps and called it the Abstract Digital Forensic Model. The nine steps included are:

- Identification
- Preparation
- Approach strategy
- Preservation
- Collection
- Examination
- Analysis
- Presentation
- Returning evidence

These models concentrate on processing digital evidence. They do not identify flow in investigation, do not include issues like chain of custody and different requirements and needs of different groups of users as defined above and in [29].

1.1.2 Advanced models

Carrier and Spafford [15], after analysis of several other models, developed their 'Integrated Digital Investigation Process (IDIP)'. This model is based on crime scene theory for physical investigation. They argue that this investigation process has been refined over time through its use in thousands of investigations, and as such, is the most suitable model upon which to establish a model for digital investigations. As a result their model is premised on the assumption that the computer should be treated as a separate crime scene to the extent that they use the analogy that the computer should be treated the same as a "body at the murder scene" [15]. Carrier and Spafford's model has been extended more recently by Baryamureeba and Tushabe [1] with their Enhanced Digital Investigation Model (EDIP). The EDIP expands the IDIP to enable tracing back to address the issues of digital investigations in networked and wireless world. However, even with this enhanced model it is useful to consider how far the physical investigation analogy can be pushed given the challenges of incidental/multiple digital copies of any individual data element and the capacity of systems to 'tamper' with data during analysis.

1.1.3 Complex models

Most recently, one of the most complex models/frameworks has been developed by CTOSE. Discussion of this model has been widely published and it can be examined in depth through the following papers [4,14,17,27,32,34] and on the CTOSE website (http://www.ctose.org/). In summary, the CTOSE model was developed as a high level tool aimed to assist companies or other individuals/groups to respond correctly during the investigation and analysis of on-line behaviours in order to generate legally admissible evidence. The CTOSE approach was to develop an 'expert system' to guide users (for example, a company's security officer) in their preparations and responses to e-security incidents.

Importantly, the aim of the CTOSE approach is to bring to these organisations an overall benchmark against which to compare their own operations and procedures relating to evidence handling. CTOSE framework offers integrated functionality across a whole spectrum of involved actors in different groups that have

Table 1 Suitability guidelines for digital forensic research

Area	Primary objective	Secondary objective	Environment/ time frames
Law Enforcement	Prosecution		After the act/post-mortem
Military IW Operations	Continuity of Operations	Prosecution	Real Time
Business and Industry	Availability of Services	Prosecution	Real Time
Academics	Advancement of knowledge	Dissemination of knowledge	Variable: subject to externalities

Adapted and extended based on Palmer [29]

a stake in the process of evidence handling, whether organisations, IT, law enforcement or the legal establishment. It appears that CTOSE framework is the only framework to be comprehensive across the entire chain of evidence handling, flexible across different types of organisations as well as portable across countries. However, questions now arise over adoption and use of this comprehensive approach and what factors would stimulate more widespread implementation of the approach.

Finally, it is useful to review [16] the 13 step model that integrates each step with sequence of activities and information flows. To date, attempts have been made to validate this model through the conduct of interviews with police investigators and to deploy the model as part of genuine police computer forensic investigations. The 13 steps of this model are:

- Awareness
- Authorisation
- Planning
- Notification
- Search for and identify evidence
- Collection of evidence
- Transport of evidence
- Storage of evidence
- Examination of evidence
- Hypothesis
- Presentation of hypothesis
- Proof/defence of hypothesis
- Dissemination of information

In summary, it is evident that despite numerous attempts to model the FC domain, definitional heterogeneity remains. It is evident that this heterogeneity is at least partly due to the differing assumptions, aims, goals and objectives underpinning the approaches outlined above. Significantly however, despite widespread recognition of the multi-dimensional nature of on-line behaviours and the challenges of understanding and responding to them, little progress has been made. Indeed, even where comprehensive frameworks have been developed the additional challenges of adoption and utilisation have emerged to limit the benefits as the problems of computer misuse and e-crime continue to grow.

At one level, all the models examined above can usefully be classified as either 'organisational' or 'procedural'. As a consequence, these models do not explicitly consider how actual practices, for example, variations in the technical hardware and/or software, impact on the conduct and result of investigations. Similarly, these models also do not explicitly consider the impact of variability in the abilities and skills of investigators. In this regard, it is useful to note that within many jurisdictions it is sufficient to hold an undergraduate degree in computer science to enable an individual to act as expert e-forensic witness. Furthermore, these models tend to concentrate on the defence side of the problem and do not sufficiently describe the 'offensive or attack side' of the problem. These observations support the argument that there is the need for a more detailed conceptual/theoretical approach. Perhaps drawing on insights from information theory as suggested by COMSEC and TRANSEC need to be revisited for more serious consideration or perhaps the option of adopting a purely mathematical model style of approach would be beneficial [22].

While some readers may consider these issues merely of academic interest, the next section highlights how this lack of coherence has directly inhibited awareness of the issues/challenges in the community, impaired the development and diffusion of specialised FC skills and, most importantly, impacted directly on the effectiveness of responses to computer misuse and e-crime [12,14].

2 Winning the battle and losing the war

The increasing incidence of computer misuse and e-crime has led to strong demand across the public and

private sectors for effective ways to address these behaviours and has contributed to the stimulation of research, development and commercialisation of technical, organisational and socio-legal responses. Whilst individual responses can be complemented for their innovation in continuing to address the evolving challenges faced, it has become increasingly obvious that truly effective offensive and defensive solutions will require both integration and implementation of insights from each.

Following Spafford [cited in ref. 29, p. 7] further research must address individual challenges in the technical, procedural, social and legal realms as well as the integration between them "if we hope to craft solutions that begin to fully 'heal' rather than constantly 'treat' our digital ills". More specifically, Spafford advocates the need to 'incorporate forensic hooks into tools rather than use our current band aid approach that produces point solution tools' and also mechanisms to begin to answer the problem of training and experience. Much more effort is required in producing user interfaces that address deficiencies in skill levels that will always be with us and will no doubt get worse as the problems grow. We need to know how much information and what type exactly we must collect to afford the most accurate analysis under particular circumstances. Common terms of reference are needed as well as common analytical standards and practices.

In working towards more integrated solutions that balances requirements for network security, individual privacy and the need for legally admissible digital evidence, it is useful to reiterate the recommendations previously articulated by Broucek and Turner [4].

- Best practice for digital evidence handling should involve deployment of the highest investigative standards at all stages in the identification, analysis and presentation of digital data.
- Targeted training and education of network administrators and end-users in the key principles of digital evidence handling is urgently required as well as education and awareness amongst users of the consequences of their on-line behaviours for system security.
- Opportunities exist for the further refinement of e-forensic methodologies and processes such as those developed by CTOSE and these must include a recognition of the dynamic and multi-faceted nature of the FC domain.
- Enhancing e-forensic professionalism through the rapid development of processes for e-forensic computing competences and certification is an essential element in building and implementing integrated solutions. Interestingly and as pointed out before, a degree in computer science is still a sufficient qualification for expert witness in court proceedings in some countries.

Unfortunately, despite these recommendations and recognition of the need for integrated solutions, there is still only limited evidence that these are actually emerging. While the lack of collaboration and integration can be at least partially explained by the complexity of the individual sets of issues faced, it is clear that this fragmentation of effort is inhibiting the development of awareness and specialised skills required, as well as having detrimental impacts on individual responses developed. Following Broucek and Turner's [12] argument, there is the critical need for the development of integrated solutions that acknowledge how in digital environments developments in one area have serious implications for developments in another. Their paper revealed how, without a conscious recognition of the interrelatedness of these responses, we will continue to create vulnerabilities and/or problems that may actually impair the effectiveness of our overall response to computer misuse and e-crime – this in turn impacts directly on the ability of industry, government or academia to improve things, i.e. we are 'winning our respective battles but possibly losing the war'.

The commercial pressures driving research, development and commercialisation further complicate the situation. These pressures often militate against mutual cooperation. For example, major players in the computer anti-virus industry still cannot reach agreement on a common naming system. This appears to be partly because of the desire of different organisations to acquire a 'commercial edge' and partly due to an inability or perhaps unwillingness to share knowledge for the same reasons. Another example of development of security tools without taking into account the forensic capabilities has been identified by the authors' recent analysis of a premier digital data visualisation tool that appears to have been constructed and developed without consideration as to whether or not the output of its analysis would be legally admissible.

2.1 Anti-forensics

While several tools and solutions were previously developed as tools for enhancement of privacy and/or security, they can now be also considered as 'anti-forensic' tools, i.e. tools/solutions that directly inhibit, hamper or at least limit accurate investigation of digital evidence. For example, as soon as any form of cryptography is introduced, an e-forensic investigation is significantly hampered. As previous work by Broucek and

Turner [9,10] observes and confirms the network-based intrusion detection tools (NIDS) like SNORT can be rendered useless by simply using SSL for http protocol (https). Collected encrypted data has none or minimal forensic value. The same applies for antivirus software. The majority of the detections are signature based and as such it is practically powerless against viruses that are distributed in encrypted form.

Privacy enhancement tools such as PGP again decrease the ability of forensic investigators unless they have legal powers to recover encryption keys. Significantly, in the post 9/11 era, it has been argued by some that using such tools also increases suspicion on individuals by raising questions over 'why these individuals exchange encrypted e-mails'. However these arguments are, in the authors' opinion, problematic and appear to challenge the basis of a number of fundamental human rights. From a conceptual perspective, it is critical that perspective is retained when examining these complex issues to prevent 'knee-jerk' policy responses that potentially do more harm than good and end up stimulating more of the behaviours they perceive than they are actually trying to address. Noticeably, the use of encryption by individuals as well as by public and private sector organisations has become increasingly common. For policy-makers access to encryption creates issues in relation to law enforcement, privacy and surveillance powers. Clearly for criminals, hackers and other individuals engaging in illegal or inappropriate behaviour, encryption provides protection. As the Aldrich Ames Spy case illustrated [31], encrypted data files obtained as part of an investigation are basically useless as evidence.

This reintroduces a key topic on the socio-political agenda at national and international levels being privacy versus encryption control and involving debates about Key Escrow (the old clipper debate) [18,19,31] versus PGP [38,39].

A simple search on Google with the term 'anti-forensic' confirms that there indeed must be a significant commercial benefit seen in the market place for developing tools with antiforensic capabilities. While it is acknowledged that currently there is no widespread awareness of these tools, perhaps this is only a matter of time. It can also be anticipated that cyber-criminals are already aware of and using these commercially available tools. Some of these tools are actually built into existing software. For example, tools like CIPHER.EXE included in the standard distribution of WindowsXP can significantly hinder forensic analysis. While some recent research (for example, Mathew Geiger's work at Carnegie Melon University) suggests that many of these anti-forensic tools are less effective than they claim to be and some actually do not work at all, their existence is illustrative of the nature of the problems faced and the need for integrated responses that balance the needs for security, privacy and legal admissibility.

3 Methodological implications for forensic computing research

While perhaps, for the near future at least, we may have to accept continued fragmentation of efforts, there remains a clear need for consideration of how well each approach is balanced in relation to addressing security, legal admissibility and privacy issues. Ultimately of course, we also need to remember that the digital domain itself is also intimately related to the physical world, where corroborative evidence and conventional investigative techniques have a role to play [12]. For academic researchers, this situation also presents a challenge in terms of how to conduct on-going research into FC and suggests the need for researchers to reconceptualise the notion of a 'solution' and take steps to develop a framework to map the value propositions of, and interrelationships between these individual sets of responses.

In the context of the discussion above, this section reflects on the implications of the current landscape for academic researchers' methodological approach to FC research.

Previous work by the authors has:

- Developed a taxonomy of FC and explored models and frameworks for understanding and responding to the issues, their impacts and interrelationships arising from online behaviours [7,8,25,26].
- Investigated and analysed technical, organisational and socio-legal approaches and consequences [2,4, 9–11,14,32].
- Advocated approaches to education and training as well as the conduct of FC investigations [3,5,6,13].
- Explored implications of uncoordinated approaches of ensuring more integrated solutions [3,12].

However, as the discussion above illustrates, an additional methodological step is required to generate data that will reveal the value propositions, attitudes, insights and experiences of domain experts in each stream of research, development and commercialisation. It is anticipated that by generating this data it will be possible to develop a framework that will more clearly expose the issues, responses and underlying assumptions and thereby contribute to improving the possibility of calibrated responses that more effectively and coherently

balance the interests for security, privacy and legal admissibility.

At the broadest level, it is argued that the data required can be generated through the conduct of qualitative semi-structured interviews with selected domain experts using methods of grounded theory for analysis of the data. More specifically, this section argues the need to explore a series of research questions about the nature of the discrete technical, organisational and socio-legal responses being developed towards computer misuse and e-crime including (but not limited to):

- What is the nature of the frameworks that individual sets of responses use to conceptualise the issues and challenges their solutions aim to address?
- How do individual sets of responses conceptualise the relationships between themselves and other sets of responses?
- What key value propositions underpin individual sets of responses and how does this influence their perceptions of what constitutes a solution?
- How can a framework be developed that will more explicitly map the value propositions of, and interrelationships between the individual sets of responses?

3.1 Interview process

The interviews will be conducted using a semi-structured question frame to guide the flow of interview. Transcripts will be constructed and analysed via a coding process drawing on the principles of grounded theory [23,33]. The question frame will be divided into the following sections:

Section 1: Participant's background The aim of the first section of questions is to collect background information about the participant, his/her knowledge of and involvement in FC and his/her organisation. Questions will be framed to determine core business of the organisation and its requirement for FC readiness.

Section 2: Forensic computing expectations The questions in the second section will focus specifically on expectations that participants from different backgrounds and areas (research/law enforcement/defence/government/ISP) have from FC. It is expected that the expectations of each group may be completely different as suggested in the literature review part of the research.

Section 3: Forensic computing problems and issues Section 3 questions will ask to explain the problems and issues that participants face in day-to-day life. The participants will be guided towards various technical, legal, organisational and other issues identified in this research as well as in previous sections of the interview.

Section 4: Solutions to identified problems Section 4 questions will be aimed at identifying possible solutions and/or at least improvements for the issues identified in section 3 of the interview. Specific questions will be given to identify critical opinions about who, when and how should provide solutions/tools/answers for the issues identified.

The aim of the questions will be to encourage participants to discuss issues related to the study without imposing limitations or constraints on how the participants answer these questions [20]. The main target is to explore with the experts in the spaces/paradigms:

- Their attitudes, experiences, insights in relation to their domain expertise and how they view the e-forensics space.
- The assumptions underpinning the way they navigate, move forward in their domains and how they identify problems, generate responses and evaluate what they do – their 'solutions'.
- Their perception of causes for the criminal on-line behaviours and other incidents involving FC.
- Recommendations for moving forward.

4 Conclusion

This paper has identified a series of issues addressing the realities of research work in the FC domain. From an academic perspective, it has reviewed current understandings and issues arising due to the lack of coherent approaches. It has also identified the implications of the current situation for methodologies used by academic researchers and suggested an additional step that may generate data that can be used to enhance the coherency of responses being developed.

This paper strongly demonstrates the need for developing a procedure to understand and model competing requirements for digital data investigations (FC). It proposes to use semi-structured interviews with experts from various organisations followed by grounded theory analysis of the interviews to:

- Better understand the needs of various groups.
- Find commonalities between these groups.
- Help researchers in the field of information systems to better understand needs and requirements for further research in this dynamically evolving field.

This paper is the first step in generating the necessary data and the authors look forward to implementing aspects of this methodological approach through frank and vigorous interaction with experts present at this

year's EICAR conference. The authors anticipate that this additional data collection and analysis will aid in the development of a framework to map the value propositions of, and interrelationships between the individual sets of responses within the dynamically evolving FC landscape. By exposing issues, responses, underlying assumptions and causalities it is anticipated that this will improve the possibility of calibrated responses that more effectively and coherently balance the interests for security, privacy and legal admissibility.

References

1. Baryamureeba, V., Tushabe, F.: The Enhanced Digital Investigation Process Model. Makerere University Institute of Computer Science, Uganda (2004)
2. Broucek, V., Frings, S., Turner, P.: The Federal Court, the Music Industry and the Universities: Lessons for forensic computing specialists. In: Valli, C., Warren M., (eds). 1st Australian Computer, Network and Information Forensics Conference, Perth, WA, Australia (2003)
3. Broucek, V., Turner, P.: Bridging the divide: rising awareness of forensic issues amongst systems administrators. In: 3rd International System Administration and Networking Conference, Maastricht, The Netherlands (2002)
4. Broucek, V., Turner, P.: Computer incident investigations: e-forensic insights on evidence acquisition. In: Gattiker, U.E. (ed.) EICAR Conference Best Paper Proceedings, EICAR, Luxembourg, Grand Duchy of Luxembourg (2004)
5. Broucek, V., Turner, P.: E-mail and WWW browsers: a forensic computing perspective on the need for improved user education for information systems security management. In: Khosrow-Pour, M. (ed.) 2002 Information Resources Management Association International Conference, pp. 931–932. IDEA Group, Seattle, Washington, USA (2002)
6. Broucek, V., Turner, P.: A forensic computing perspective on the need for improved user education for information systems security management. In: Azari, R., (ed.) Current Security Management Ethical Issues of Information Technology, IGP/INFOSCI/IRM Press, Hershey, PA, USA (2003)
7. Broucek, V., Turner, P.: Forensic computing: developing a conceptual approach for an emerging academic discipline. In: Armstrong, H. (ed.). 5th Australian Security Research Symposium, pp. 55–68 School of Computer and Information Sciences, Faculty of Communications, Health and Science, Edith Cowan University, Western Australia, Perth, Australia (2001)
8. Broucek, V., Turner, P.: forensic computing: developing a conceptual approach in the era of information warfare, J. Inf. Warf. **1**, 95–108 (2001)
9. Broucek, V., Turner, P.: intrusion detection systems: issues and challenges in evidence acquisition. In: CTOSE Conference, Facultés Universitaires Notre-Dame De la Paix, Namur, Belgium (2003)
10. Broucek, V., Turner, P.: intrusion detection: forensic computing insights arising from a case study on SNORT. In: Gattiker, U.E. (ed.) EICAR Conference Best Paper Proceedings, EICAR, Copenhagen, Denmark (2003)
11. Broucek, V., Turner, P.: intrusion detection: issues and challenges in evidence acquisition. Int. Rev. Law, Comput. Technol. **18**, 149–164 (2004)
12. Broucek, V., Turner, P.:Riding furiously in all directions implications of uncoordinated technical, organisational and legal responses to illegal or inappropriate on-line behaviours. In: Turner, P., Broucek, V., (eds). EICAR 2005 Conference Best Paper Proceedings, pp. 190–203 EICAR, Saint Julians, Malta, (2005)
13. Broucek, V., Turner, P.: risks and solutions to problems arising from illegal or inappropriate on-line behaviours: two core debates within forensic computing. In: Gattiker, U. E. (ed.) EICAR Conference Best Paper Proceedings, pp. 206–219. EICAR, Berlin, Germany, (2002)
14. Broucek, V., Turner, P., Frings, S.: Music piracy, universities and the Australian Federal Court: issues for forensic computing specialists, Comput. Security Rep. **21**, 30–37 (2005)
15. Carrier, B. D., Spafford, E. H.: Getting physical with the digital investigation Process, Int. J. Digit. Evidence **2**, (2003)
16. Ciardhuáin, S. Ó.: An extended model of cybercrime investigation. Int. J. Digit. Evidence **3**, (2004)
17. CTOSE: CTOSE Project Final Results (2003)
18. Denning, D. E.: Description of Key Escrow System (1997)
19. Denning, D. E.; Branstad, D. K.: A taxonomy for key escrow encryption systems. Commun. ACM **39**, (1996)
20. Doolin, B.: Alternative views of case research in information systems. Aust. J. Inf. Syst. **3**, 21–29 (1996)
21. Farmer, D., Venema, W.: Murder on the Internet Express (1999)
22. Filiol, E.: Personal communication (2006)
23. Glaser, B. G., Strauss, A.: The Discovery of Grounded Theory: Strategies for Qualitative Research. Aldine Pub. Co., Chicago (1967)
24. Hanks, P. (ed.) : The Collins Australian Pocket Dictionary of the English Language, HarperCollins Publishers (1991)
25. Hannan, M., Frings, S., Broucek, V., Turner, P.: Forensic computing theory and practice: towards developing a methodology for a standardised approach to computer misuse. In: Kinght, S.-A. (ed.). 1st Australian Computer, Network and Information Forensics Conference, Perth, WA, Australia (2003)
26. Hannan, M., Turner, P., Broucek, V.: Refining the taxonomy of forensic computing in the era of E-crime: insights from a survey of Australian Forensic Computing Investigation (FCI) Teams. 4th Australian Information Warfare and IT Security Conference, Adelaide, SA, Australia, 151–158 (2003)
27. Leroux, O., Pérez Asinari, M. V.: Collecting and producing electronic evidence in cybercrime cases. In: CTOSE Conference, Facultés Universitaires Notre-Dame De la Paix, Namur, Belgium (2003)
28. McKemmish, R.: What is forensic computing. Trends and issues in crime and criminal justice (1999)
29. Palmer, G.: A Road Map for Digital Forensic Research: Report from the First Digital Forensic Research Workshop (DFRWS), Utica, New York (2001)
30. Reith, M., Carr, C., Gunsch, G.: An examination of digital forensic models; Int. J. Digit. Evidence **1**, (2002)
31. Reno, J.: Law enforcement in cyberspace address. In: Denning, D. E., Denning, P. J. (eds). Internet Besieged: Countering Cyberspace Scofflaws, pp. 439–447. ACM Press (1996)
32. Sato, O., Broucek, V., Turner, P.: Electronic evidence management for computer incident investigations: a prospect of CTOSE. Security Manage. **18**, 11–18 (2005)
33. Strauss, A., Corbin, J. M.: Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory. Sage Publications, Thousand Oaks (1998)
34. Urry, R., Mitchison, N.: CTOSE Project. Electronic evidence: gathering, securing, integrating, presenting. In: CTOSE

Conference. Facultés Universitaires Notre-Dame De la Paix, Namur, Belgium (2003)
35. Venema, W., Farmer, D.: SATAN (Security Administrator Tool for Analyzing Networks) (1995)
36. Verreck, P.: Case study – vindictive e-mail. Int. J. Forensic Comput. (2000) http://www.forensic-computing.com/archives/vind.html
37. Verreck, P.: Presenting the evidence. Int. J. Forensic Comput. (2000) http://www.forensic-computing.com/archives/present.html
38. Zimmerman, P.: A note to PGP users (2001)
39. Zimmerman, P.: Testimony of Philip R. Zimmerman to the Subcommittee on Science, Technology, and Space of the US Senate Committee on Commerce, Science, and Transportation (1996)