

Refining the Taxonomy of Forensic Computing in the Era of E-crime: Insights from a Survey of Australian Forensic Computing Investigation (FCI) Teams.

M.B.Hannan¹, P.Turner² and V.Broucek²

¹School of Accounting and Information Systems
University of South Australia, Australia.
Email: mathew.hannan@unisa.edu.au

²School of Information Systems
University of Tasmania, Australia.
Email: vlasti.broucek@utas.edu.au; paul.turner@utas.edu.au

ABSTRACT

The incidence of criminal, illegal and inappropriate computer behaviours has focused attention on the need for enhanced digital evidence acquisition and presentation competences. However, the dynamic and multi-disciplinary nature of the forensic computing domain has made difficult the identification of the nature, level and type of competences required. Building on the forensic computing taxonomy of Broucek and Turner (2001) this paper reports on a survey of competences amongst 21 Australian FCI teams within Australia. This survey provides insights into the current practice of forensic computing investigation, identifies anticipated key future competence requirements and enables a refinement of the taxonomy of forensic computing.

Key words: Forensic Computing, E-crime, Forensic Computing Investigation, Taxonomy, Computer Misuse.

INTRODUCTION

At the broadest level within the private and public employment sectors, the increased risk and incidence of criminal, illegal or inappropriate computer behaviours has heightened awareness of the need to develop defensive and offensive responses to e-crime and computer misuse (McKemmish 1999; ACPR 2000; ACPR 2001; Broucek & Turner 2001).

Although traditional methods for addressing conventional social transgressions (including deterrence, security and education) still have a significant role to play, computer misuse and e-crime present unique challenges in that, when this behaviour is detected, there is also a need to:

- Formally investigate and assess the extent and effect of the behaviour; and
- Gather evidence and proof for future actions that may include criminal or civil prosecution, organizational censure or dismissal.

Concurrent with the technical difficulties of detecting, identifying and recording these behaviours, there exists a number of legal considerations regarding types of evidence acquisition ('forensic') activities and the legal admissibility of the digital evidence that these forensic activities produce. As a result, a multi-disciplinary mix of specialised human skills is required to ensure the successful conduct of computer forensic investigations. However, the identification and relevancy of these skills, their nature, type and level of the competence, is complicated by the dynamic nature of the forensic computing domain.

At the practical level, a significant number of publications written technical, legal and organisational issues pertaining to computer misuse and e-crime have been produced by computer security experts, legal professionals and information systems specialists. However, an exploration of the

interrelationships between these issues has until recently been limited by the lack of a conceptual framework within which to position these different approaches. This has also inhibited the development of the specialised skill sets required to advance the theory and practice of forensic computing research and investigation (Broucek & Turner, 2001).

In the Australian context, the paper describing the forensic computing taxonomy developed by Broucek & Turner (2001) provides a summary of results from a survey of 21 forensic computing investigation teams aimed at establishing a body of knowledge relating to FCI team competence. This survey provides insights into the current practice of FCI and the existing competences contained within current Australian FCI teams. Significantly, the survey also provided insights into how these human skill sets were evolving in anticipation of the new challenges of computer misuse and e-crime facing FCI teams. Finally, the results of the survey enabled a validation and further refinement of Broucek & Turner's (2001) taxonomy of forensic computing.

The remainder of this paper is in five sections. Section One provides a brief overview of assessments of the current levels of computer misuse and in particular e-crime in Australia. Section Two provides background on the taxonomy of forensic computing (Broucek & Turner, 2001) and illustrates how it was deployed as a basis for the survey of Australian FCI team competence. Section Three outlines the survey and summarises its key findings. Section Four considers the development of offensive forensic computing techniques in the era of e-crime and information warfare. Section Five provides a conclusion and looks to the future.

SECTION ONE: LEVELS OF COMPUTER MISUSE

The diffusion of information and communication technologies (ICT) throughout Australian government, business and society has led to new opportunities, new challenges and new risks. By the end of 2002 surveys of ICT connectivity revealed that in Australia:

- 67% of households own or lease a computer;
- 52% of households were connected to the Internet;
- 72% of Australians aged 16 years and over have Internet access from any location;
- 73% of Australian males and 72% of females aged 16 years and over have Internet access; and
- 80% of people aged 16-34 and 68% of people aged 35 years and over in Australia have Internet access.

Given these figures it is not surprising that the propensity of individuals and/or groups utilizing ICT to engage in computer misuse and e-crime (McKemmish, 1999; ACPR, 2000, 2001; Broucek & Turner, 2001) has increased over the last ten years. However, obtaining accurate figures on the levels of computer misuse are fraught with difficulties.

In the United States, approximately 70% of corporations reported e-crime incidents during 2000, up from 30% in 1999. It is estimated that these e-crime incidents cost corporations approximately \$US265,589,940 in 2000 (AFP, 2001).

In Australia a similar trend has been observed. The Australian Computer Emergency Response Team (AUScert) recorded similar increases in e-crime response requests from Australian organisations over the period 1998 to 2000 and AUScert's most recent Computer Crime and Security Survey reported that 42% of respondents had experienced one or more significant attacks that had harmed the integrity, confidentiality or availability of network data or systems and that 38% of respondents were dissatisfied with the level of IT security qualifications in their organisations.

Other trends observed by AUScert were:

- Greater occurrence of externally-sourced harmful attacks
- Financial losses due to computer attacks which harmed the confidentiality, integrity or availability of network data or systems had doubled over the last year (\$12 million in 2003, compared with \$6 million in 2002)
- Financial fraud, laptop theft and virus, worm and Trojan infections are the largest source of computer crime losses
- 22% of organizations surveyed experienced more than ten computer security incidents.

(Source: AUScert, 2003)

The nature and extent of the problem of computer crime within Australia is not known. There is a lack of comprehensive data that clearly identifies the level and incidence of electronic crime within Australia that is compounded by non-reporting and non-detection of e-crime (ACPR 2000; Etter 2001b).

The last ten years have seen the development of specialist Forensic Computing teams to conduct investigations into criminal, illegal or inappropriate behaviour committed or facilitated through the use of computers or other digital devices. In the absence of specific training courses these teams have been required to draw on knowledge, skills and experience from a range of disciplines in order to meet the challenges of conducting an investigation in a digital environment.

SECTION TWO: A TAXONOMY OF FORENSIC COMPUTING

The last decade Forensic Computing teams has seen the emergence of Forensic Computing teams in government and non-government organisations. These teams have evolved from a variety of backgrounds and draw on the multi-disciplined backgrounds of the team members in order to provide the knowledge, skills and experience necessary to undertake Forensic Computing.

The increased uptake of technology within Australian society, coupled with rapid developments in digital technology, has occurred more quickly than the development of a legal framework to address aspects of criminal, illegal or inappropriate conduct occurring within this medium (Drucker & Gumpert 2000; Broucek & Turner 2001; Etter 2001a). This has vast implications for Forensic Computing teams operating within Australia that are constantly required to gain new legal and technical knowledge in addition to maintaining their existing skills necessary to conduct Forensic Computing operations.

The lack of an overarching conceptual framework was identified by Broucek and Turner (2001) as a source of both confusion and frustration for researchers wishing to explore aspects of the emerging discipline of Forensic Computing. Conversely FCI teams rely on individual members contributing a variety of knowledge, skills and experience in order to provide all the necessary human resources to undertake Forensic Computing investigations. The proposed taxonomy by Broucek and Turner (2001) provided both the academic community and practitioners within the field of Forensic Computing with a basis for examining existing research and skills and upon which to direct research for the future development of practitioner knowledge, skills and experience.

Broucek and Turner (2001) further developed the concept of Forensic Computing as a multi-disciplinary academic by building on previous work by authors including Farmer (2001) and Venema (2000) and expanding on the definition of Forensic Computing as provided by McKemmish (1999).

McKemmish (1999:1) proposes the following definition for Forensic Computing:

‘the process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally acceptable’

Through the examination of previous research, Broucek and Turner (2001) argue that in the absence of an overarching taxonomy, Forensic Computing research has failed to combine and leverage the strengths of individual disciplinary investigations of particular forensic issues. To overcome this, they proposed a taxonomy for the discipline that includes multiple dimensions and sub-categories upon which to frame the future development of the discipline. Table 1 provides the expanded dimensions within the proposed taxonomy.

COMPUTER SCIENCE <ul style="list-style-type: none">• Operating Systems and Application Software• Computer Security• Systems Programming and Programming Languages
LAW <ul style="list-style-type: none">• Computer Law• Criminal, Civil and Technology Law (CCT Law)
INFORMATION SYSTEMS <ul style="list-style-type: none">• Systems Management and Policies• User Education
SOCIAL SCIENCE

(Adapted from: Broucek & Turner 2001)

Table 1 *Proposed Taxonomy: Forensic Computing*

Broucek and Turner (2001) recognised that the proposed taxonomy may be incomplete; however they suggested that it served as a starting point for the development of a more comprehensive conceptual framework to support research in Forensic Computing Investigation.

SECTION THREE: A SURVEY OF COMPETENCE IN AUSTRALIAN FCI TEAMS

This research sought to examine practicing FCI teams currently operating within Australia. The existing taxonomy was used as the basis for the development of the instrument for the measurement of FCI team competence within this research study.

In addition to the disciplines included in the existing taxonomy, Forensic Computing team leaders were asked to provide information on any additional areas that they believed were essential to undertake Forensic Computing Investigation.

This study collected data through the use of a questionnaire completed by 21 FCI team leaders in organisations currently conducting Forensic Computing Investigation in Australia. The questionnaire was developed to include questions suitable for administration to a team leader, Sergeant or Inspector (or equivalent rank or being the sole Investigator within an organisation) leading a Forensic Computing Investigation Team.

The questionnaire comprised 22 questions divided over three parts, all relevant and specifically related to the objectives of the research and designed to gather information that would enable analysis relating to the operations of the team (location, industry and number of investigations), and the knowledge, skills and experiences held by the team and desired by the team leaders in the future.

In addition, a section of the questionnaire sought to gather information relating to the method of competence development and the level of experience that each FCI team held within each area of competence.

The outcome of the research was that the taxonomy provided by Broucek and Turner (2001) was able to be used to describe many of the areas of knowledge, skills and experience that FCI teams employ to undertake Forensic Computing. However, the taxonomy fell short of the inclusion of investigation as a distinct discipline whereas investigation was observed as being one of the most common and most desired disciplines within practicing Forensic Computing teams.

- **Investigation skills**

The discipline of investigation skills was observed as the most common experience held by FCI teams operating within Australia. This was further supported by the team leaders rating investigation skills as the most important skill for Forensic Computing both presently and into the future.

The term “investigative skills” within the sample of forensic computing team leaders was taken to mean law enforcement investigation related skill sets. The distinction is different from an academic meaning of the terms investigation or investigative where in normal (academic) context would be used to describe a study to examine a specific phenomenon.

Within the context of Forensic Computing Investigation, skills may include (but not be limited to):

- Methodological approach to the investigation
- Case management
- Communication
- Interview technique
- Preparation of court documentation
- Preservation of physical aspects of evidence and investigation
- Documentation of process
- Appropriate use of resources
- Critical thinking

Investigation skills are necessary to ensure that the investigation process complies with the legal or organisational requirements governing the investigation whereas investigative practice is determined by the experience of the team based upon training, legal requirements and organisational policy.

In conducting this study the researchers observed that the majority of FCI team members operating within Australia, even when currently employed by agencies outside state and federal police organizations, had some law enforcement background. This reflects the concerns raised by the Australasian Centre for Policing Research in its 2000 scoping paper “The Virtual Horizon: Meeting the Law Enforcement Challenges” which identified that a major concern of policing jurisdictions operating FCI teams will be the retention of highly trained staff members.

The confirmation of these fears reinforces the need for law enforcement agencies to find new methods to encourage the retention of the highly trained FCI team members. To meet this challenge, traditional policing management practice within Australia may need to be confronted and new innovative ideas employed in order to encourage staff to remain within the organisation when incentives to leave are often considerable.

Further Observations from Practicing Australian Forensic Computing Investigation Teams

The email survey was distributed to a sample of 30 Forensic Computing team leaders currently practicing in Australia. From the 30 surveys distributed, 21 were returned as completed by the

respondents. The sample was developed through extensive investigation on the part of the researchers in the absence of previous research in the area. The sample represented a cross section of industries including:

- Property and Business Services
- Finance and Insurance
- Government Administration and Defence
- Education
- Law Enforcement
- Transport and Storage

(Industry categories based upon Australian Bureau of Statistics (1997) categories)

The researchers recognised that other organisations may have been conducting Forensic Computing Investigation within Australia however, in the absence of previous comprehensive research in the area and despite exhaustive enquiries undertaken as a component of this research, no further organisations engaged in Forensic Computing Investigation were identified.

Accounting was also recognised by some team leaders as an additional discipline of knowledge, skill or experience required to undertake Forensic Computing. Unlike, investigation skills, accounting was not unanimously supported by the team leaders as an additional discipline. The researchers accept the legitimacy of accounting in some Forensic Computing investigations and indeed in some teams, knowledge of this area may be crucial to the investigation. However, the researchers believe that inclusion of accountancy may be a legacy of the evolution of some of the FCI teams from former fraud investigation teams or because the organisation within which the team operated was essentially an accountancy firm.

SECTION FOUR: FORENSIC COMPUTING AND INFORMATION WARFARE

In the age of information warfare, Forensic Computing offers government and private organisations the ability to detect, identify and record legally admissible evidence that may form the foundation to prosecute attackers. Further, proactive Forensic Computing can provide the basis upon which to devise defensive strategy, gather intelligence or initiate counter operations.

While this paper presents a suggestion for an expansion of the existing taxonomy of Forensic Computing in the context of Information Warfare, the knowledge, skills and experience held by Forensic Computing teams can provide a valuable resource. The ability of a Forensic Computing team to detect, identify and record legally admissible evidence upon which prosecution of attackers may be based is a central function. However, the knowledge, skills and experience possessed by the team to undertake this function can also be mobilised and deployed for the gathering of intelligence and counter intelligence. The versatility of these teams can provide a wealth of information and deterrence against attack in an age of information warfare.

Information warfare, as with Forensic Computing, is not longer the sole domain of government and military organisations. The expansion of Information Warfare into private corporations and society at large presents a growing need within Information Warfare operations (Warren & Hutchinson, 2001) to incorporate the knowledge, skills and experience held within Forensic Computing teams. Further the mobilisation and deployment of such knowledge, skill and experience in both offensive and defensive roles may bring with it a distinct strategic advantage for an organisation engaged in an Information based conflict.

SECTION FIVE: CONCLUSIONS AND LOOKING TO THE FUTURE

The survey conducted with FCI teams in Australia is now being used as the base for a similar study to be conducted by a University in the United Kingdom by the end of 2003. It is anticipated that an international comparative study of applied practice among FCI teams will result.

The taxonomy of Forensic Computing continues to be refined as this paper is contributing to potential international comparisons of work within this field and is the first step in the development of a matrix of computer behaviour requiring Forensic Computing Investigation.

Within the Australian context, the incidence of criminal, illegal and inappropriate computer behaviours has become so serious that Forensic Computing teams have developed across all industries and this research can be utilised as an initial framework for the future examination of this growth.

- **The future**

Broucek and Turner (2001) identified the need to develop specialised training in Forensic Computing and identify what such training might cover. Etter (2001b) states "the challenge of e-crime is real and immediate" and supports Broucek and Turner's call for specialised training, and specifically the need to identify training needs at all levels within Australian law enforcement, government and private organisations to address the unique challenges of Forensic Computing. Loper (2001) and May (2002) go further in identifying a knowledge gap between the technical knowledge of computer hackers and Forensic Computing Investigators.

Hannan and Turner (2003) state that the key to superior performance within this environment is in the development of knowledge. This taxonomy provides the strategic framework for the development of this knowledge, skills and experience by both practitioners and academics in order to address many of the risks faced in an era that is now requiring Forensic Computing Investigation.

The taxonomy, with amendments, may serve as the basis upon which more formalised training and acceptable standards of practice may be developed in order to address the needs identified by Broucek and Turner (2001); Etter (2001a); Loper (2001); and May (2002).

REFERENCES

- ABS (1997). Take-up rate for modem and internet use low. Canberra, Australian Bureau of Statistics. 2002.
- ACPR (2000). The Virtual Horizon: Meeting the Law Enforcement Challenges - Developing an Australasian law enforcement strategy for dealing with electronic crime. Adelaide, Australasian Centre for Policing Research: 1-132.
- ACPR (2001). Electronic Crime Strategy of the Police Commissioners' Conference. Adelaide, Australasian Centre for Policing Research.
- AUScert (2003). Computer Crime & Security Survey. AUScert.
- Broucek, V. & Turner, P. (2001). "Forensic Computing: Developing a Conceptual Approach in the Era of Information Warfare." Journal of Information Warfare 1(2): 95-108.
- Drucker, S. J. & Gumpert, G. (2000). "CyberCrime and punishment." Critical Studies in Media Communication 17(2): 133-158.
- Etter, B. (2001a). Computer Crime. AIC 4th National Outlook Symposium on Crime in Australia -
- Etter, B. (2001b). The forensic challenges of e-crime. Adelaide, Australasian Centre for Policing Research: 1-8.

Farmer, D. (2001). "Bring Out Your Dead. The Ins and Outs of Data Recovery." Dr Dobb's Journal 30(1).

Hannan, M. & Turner, P. (2003). "Beyond the Matrix: Research on Competence among Australian Forensic Computing Investigation Teams" Proceedings of the 2nd European Conference on Information Warfare and Security, June 30 – July 1, 2003. Reading:U.K.

Loper, D.K. (2001). "A case study in the forensics of computer crime: E-mail address spoofing." Journal of Security Administration 24(2): 45-68.

May, M. (2002). "A wide web of attack." American Scientist 90(1): 29-31.

McKemmish, R. (1999). What is Forensic Computing? Canberra, Australian Institute of Criminology: 1-6.

NOIE (2000). E-commerce beyond 2000, National Office for the Information Economy. 2002.

Venema, W. (2000). "File Recovery Techniques. Files Wanted, Dead or Alive." Dr Dobb's Journal 29(12).

Warren, M., & Hutchinson, W. (2001). Information Warfare and Hacking. Paper presented at the 5th Australian Security Research Symposium, Perth, WA, Australia. 11 July, 2001.