

## **Computer Incident Investigations: e-forensic Insights on Evidence Acquisition**

*Vlasti Broucek, Paul Turner*

*School of Information Systems, University of Tasmania*

### **About the authors**

*Vlasti Broucek, MSc has been working in the computer industry since 1985, currently, he is a researcher in the School of Information Systems and a network administrator in the School of Psychology, both at the University of Tasmania, Australia. Vlasti's research focus is on Legal and Technical Issues of forensic computing. Vlasti has an MSc degree from the Czech Technical University in Prague and currently is pursuing a PhD at the University of Tasmania under leadership of Dr Paul Turner. Vlasti recently received an award for his work in forensic computing from the Australian National Institute of Forensic Sciences. (<http://www.nifs.com.au>)*

*Mailing address: School of Information Systems, Private Bag 87, Hobart TAS 7001, Australia; Phone: +61-3-62262346; Fax: +61-3-62262883; E-mail: [Vlasti.Broucek@utas.edu.au](mailto:Vlasti.Broucek@utas.edu.au)*

*Continued on page 2...*

### **Descriptors**

*computer misuse; criminal, illegal or inappropriate on-line behaviours; CTOSE; e-forensics; evidence acquisition; forensic readiness; MP3 piracy*

**Reference to, or Citation** of this paper should be made as follows:

Broucek, V. & Turner, P. (2004). Computer Incident Investigations: e-forensic Insights on Evidence Acquisition. In U.E. Gattiker (Ed.), EICAR 2004 Conference CD-rom: Best Paper Proceedings (ISBN: 87-987271-6-8) 18 pages. Copenhagen: EICAR e.V.

*Prior to joining the School of Information Systems as a senior research fellow Dr. Paul Turner was a research fellow at CRID (Computer, Telecommunications and Law Research Institute) in Belgium. Paul has also worked as an independent ICT consultant in Europe and was for 3 years editor of the London-based Telecommunications Regulation Review. Paul's strong research focus has continued at the University of Tasmania, where for 2 years Paul was concurrently Research Manager for the Tasmanian Electronic Commerce Centre (<http://www.tecc.com.au>). Paul is currently the University's research coordinator for the Smart Internet CRC (<http://www.smartinternet.com.au>) and was instrumental in the recent establishment of the forensic computing institute (<http://www.forensiccomputing.org>).*

Mailing address: School of Information Systems, Private Bag 87, Hobart TAS 7001, Australia; Phone: +61-3-62266240; Fax: +61-3-62266211; E-mail: Paul.Turner@utas.edu.au

## Computer Incident Investigations: e-forensic Insights on Evidence Acquisition

### Abstract

*The growing incidence and risk of inappropriate, illegal and/or criminal computer behaviours has increased the need to build bridges between technical and legal areas of expertise in order to produce more effective defensive and offensive responses. Although there is already a large volume of literature on organizational, technical and legal issues pertaining to computer misuse and e-crime there have until recently been only limited explorations of the interrelationships between these issues. This has been partly because of the lack of a conceptual framework within which to position these different approaches and partly because of the complexity of the specific sets of legal and technical challenges faced (Broucek & Turner, 2001a, 2001b; Hannan, Frings, Broucek, & Turner, 2003; Hannan, Turner, & Broucek, 2003).*

*While at one level conventional approaches to social misconduct (including deterrence, security and education) retain their relevance in cyber-space, the variety of ways that individuals and/or groups can now use digital technologies to engage in computer misuse and e-crime does present unique challenges. As with other types of investigation when an incident occurs or behaviour is detected there is need to formally investigate and assess its extent and effect. There is also a need to gather evidence and proof that may be used as the basis for responses. Significantly, in the case of computer misuse and e-crime, it is these evidence acquisition activities that from an e-forensics perspective present the most difficult technical and legal challenges.*

*On the technical side, problems remain in relation to the processes for detecting, identifying and logging these behaviours. On the legal side, numerous challenging legal considerations exist regarding types of evidence acquisition (“forensic”) activity and the legal admissibility of the digital evidence that these activities produce. To address these challenges is particularly difficult because most technical e-security solutions are not currently designed to support such e-forensic data acquisition and most organisations are unfamiliar with the admissibility requirements for digital evidence collection, collation and presentation (Broucek & Turner, 2002a, 2003c; Sommer, 1998).*

*This research paper provides a forensic computing perspective on these issues through a discussion of a recent legal case against three Australian Universities involving MP3 piracy. The paper also explores the recently developed European CTOSE (Cyber Tools On-line Search for Evidence) methodology (Frings, Stanistic-Petrovic, & Urry, 2003; Leroux & Pérez Asinari, 2003; Urry & Mitchison, 2003) and presents some basic key principles for approaching digital evidence handling. Key findings of the paper include:*

- *“Best” practice for digital evidence handling involves deploying 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;*

- *Opportunities exist for the further refinement of e-forensic methodologies and processes such as those developed by CTOSE;*
- *Enhancing e-forensic professionalism through the rapid development of processes for e-forensic computing competences and certification will lead to improved outcomes in the investigation and prosecution of computer misuse and e-crime.*

## Introduction

The recent “MP3 piracy” case in the Federal Court of Australia ([Aust unis in court over file-swapping](#), 2003; Broucek, Frings, & Turner, 2003; Lamont, 2003; Morgan, 2003; Rose, 2003) raises serious concerns about the understanding amongst all participants (including the federal court judge) of the nature and admissibility of digital evidence and appropriate investigative procedures for its identification, collection, storage, analysis and presentation. Not surprisingly, this case involving Sony Music Entertainment (Australia) Limited, Universal Music Australia Pty Limited and EMI Music Australia Pty Limited (the applicants) and three Australian Universities – the University of Tasmania, University of Melbourne and University of Sydney (the respondents) has generated considerable public debate.

This research paper examines the case from a forensic computing perspective and presents the approaches of the three parties involved – applicants, respondents and federal court judge. More specifically, this examination highlights a series of problems in dealing with digital evidence that have been the focus of the European Union funded Cyber Tools On-line Search for Evidence (CTOSE) (CTOSE, 2003; Frings et al., 2003; Leroux & Pérez Asinari, 2003; Urry & Mitchison, 2003) project funded by European Union in 2003. This paper explores the outcomes of the CTOSE project and presents some basic key principles for approaching digital evidence handling. By leveraging these insights from theory and practice the paper concludes by presenting four key findings that point to enhancing “best practice” for digital evidence handling and for improving forensic computing knowledge amongst practitioners and in the broader community.

## The MP3 Piracy Case

In late January 2003, during a period when the Australian Record Industry Association (ARIA) was publicising the damage on-line piracy was doing to the music industry and the actions that the industry was determined to take to combat these activities (*Online piracy hurts 2002 music sales: ARIA*, 2003) three Australian Universities<sup>1</sup> (University of Tasmania, University of Melbourne and University of Sydney) were approached by members of the Australian music industry (Sony Music Entertainment (Australia) Limited, Universal Music Australia Pty Limited and EMI Music Australia Pty Limited) and requested to preserve digital evidence on their systems of the distribution of MP3s by students and

---

<sup>1</sup> It is widely believed that more Universities were involved, in fact only the three Universities offered any resistance to initial request by the music industry to preserve and hand in evidence about these alleged activities

staff. These requests came because the music industry was concerned that MP3s and these distribution activities were potentially in breach of Australian copyright laws.

Subsequent to this request to the Universities, these members of the music industry further requested access to this digital evidence for discovery purposes that might subsequently lead to the prosecution of individuals. In response the three Universities concerned refused to provide this access<sup>2</sup>.

### History of the case<sup>3</sup>

As a result of Universities refusal to provide access to this digital data, on February 18, 2003 these music industry members (applicants) launched legal proceedings against the Universities (respondents) in order to gain access to this data preserved data by the respondents at their request. The basis of the legal proceedings were procedural with applicants seeking a right of access to the preserved potential evidence in order to conduct discovery investigations that could possibly lead to identification of person(s) involved in copyright infringements who would then be acted against in subsequent litigation. The case clearly demonstrates lack of preparedness by all the involved parties – Universities, music industry and legal profession

On February 18, 2003 at the initial hearing the case was adjourned with orders made to the respondents to preserve the digital data. The case and initial ruling raised serious concerns amongst academics, students and civil liberty groups who viewed this as the beginnings of a major assault by copyright owners to infringe the privacy of individuals.

On May 30, 2003 after a number of further court sessions and out-of-court attempts to find a mutually acceptable solution, the presiding judge, Justice Tamberlin, made his decision in favour of the applicants ("Sony Music Entertainment (Australia) Limited v University of Tasmania [2003] FCA 532 (30 May 2003)," 2003). Subsequently on July 18, 2003 he ordered the respondents to hand over their digital data records to the applicants and their forensic expert for further investigation ("Sony Music Entertainment (Australia) Limited v University of Tasmania [2003] FCA 724 (18 July 2003)," 2003).

On July 29, 2003 ("Sony Music Entertainment (Australia) Limited v University of Tasmania [2003] FCA 805 (29 July 2003)," 2003) Justice Tamberlin further ordered the respondents to bear the cost of the discovery process, and, in determining the data to be handed over argued that "deleted files are equal to overwritten files"<sup>4</sup> (Pearce, 2003). Again, this

---

<sup>2</sup> At the University of Tasmania, this occurred in the context of on-going concerns about privacy in contracts with external research collaboration projects.

<sup>3</sup> For a more in-depth discussion of this case – refer to: Broucek, V., Frings, S., & Turner, P. (2003). The Federal Court, the Music Industry and the Universities: Lessons for Forensic Computing Specialists. In Proceedings of 1st Australian Computer, Network & Information Forensics Conference. Perth, WA, Australia.

<sup>4</sup> This statement from Justice Tamberlin was made when one of the respondents reported that the backup tapes in question had accidentally been overwritten and therefore did not have any forensic value for the applicants.

reveals a worrying lack of comprehension of the technical nature of digital logs and data storage, as from a technical perspective it is clearly inappropriate to consider overwritten backup tapes as admissible evidence. Subsequently, this ruling was used by the recording industry in mounting “a possible contempt of court” challenge against the University of Sydney. This challenge resulted in a small but significant victory for the respondents, as it was dismissed and the applicants ordered to pay cost. (“Sony Music Entertainment (Australia) Limited v University of Tasmania [2003] FCA 929 (4 September 2003),” 2003).

The case has not been resolved at the time of writing this paper and appears to be stalled. In the authors’ opinion, this is largely because of the anomalies highlighted above.

While the subject of this case is only procedural – discovery, it is interesting to note how the arguments of the respondents have evolved from their initial refusal to provide access. This initial opposition was primarily based on the premise that excessive access to this data could lead to breaches of privacy and intellectual property law covering aspects of the data held. It is however important to note that respondents were from the outset willing to provide some digital data to the applicants, providing that this data was collected by the respondents and then handed onto the applicants. Several offers of this kind were made, however the applicants were dissatisfied with the amount of data and discovery offered. The applicants demanded the rights to conduct full computer forensic investigation of the preserved data, despite the fact that the overwhelming majority of the data in question contains (or contained) information on the on-line activities of thousands of “presumably innocent” users and not just data on users that were alleged to be guilty of illegal practices.

What emerges is the fact that this data highlights activities pertaining to personal, confidential and commercial activities of the Universities’ staff and students as part of their research, teaching and commercial activities. In this context, the judgement in this case has provided unprecedented access to huge amounts of potentially highly sensitive data because of a suspicion that some of it contains evidence of illegal practices. Unfortunately, the judgement has not provided this data access to an independent third party (for example, an external forensic investigation team) but rather to the very same groups who have “pointed the finger” in the first place. Although the judgment puts in place certain safeguards, these applicants are then allowed to “mine” this data in search of what they themselves deem “illegal practices”. Aside from the intrusion into the data of thousands of “presumably innocent” users, issues of data tampering/manipulation (except where MD5 check-sums are calculated and stored by respondents), breaches of privacy, commercial dealings, intellectual property are all only protected by confidentiality provisions placed on the applicants.

### **e-Forensic Issues identified**

From a forensic computing perspective, this case and the responses of its participants highlight a number of significant issues. Firstly, the approach of the three Universities in preserving the “evidence” after the initial request reveals a lack of e-forensics knowledge and/or preparedness. The initial data collection and storage was conducted by network administrators with little or no training in forensic computing procedures. For example, file

level copies of file systems were made to CD-ROMs or standard backup procedures were used to preserve the evidence. In the case of University of Tasmania, music industry legal representatives sent an e-mail regarding one particular www site that was allegedly hosting copyright MP3 files. Subsequently, the machines involved were copied/backed up as requested and backup tapes were stored in the fire proof safe in late January 2003. Only file level backups using standard backup software were collected.

In the opinion of the authors, although these tapes might contain evidence of files being stored on particular computers it would be of limited value in any subsequent legal prosecutions because it was not collected using binary copies and neither the chain of custody or rules of evidence were followed (Broucek & Turner, 2001a, 2002a, 2002b, 2003b). While such evidence might be sufficient in a case of dispute resolution it would be unlikely to stand-up to examination in a criminal or a civil case. This suggests a lack of "forensic readiness" on the part of participants and the need for set procedures, covering all possible variants of investigations involving digital evidence to reveal any criminal, illegal or other inappropriate behaviours.

Another interesting issue was highlighted by the repeated requests by the applicants' forensic computing expert for the use of the specialised forensic software tool EnCase (the tool most widely used by law enforcement agencies). Such software enables detailed investigation of digital evidence, in particular recovery of deleted files, recovery of slack spaces etc., however, it requires appropriate input data. The repeated requests to use this tool on evidence collected by using file level backups where there would not be the possibility of doing such data recovery certainly reduces the authors confidence in the abilities and knowledge of the e-forensics expert employed by the applicants.

Subsequently during the case it was revealed that this e-forensics expert was actually not able to investigate the digital data provided by the respondents due to a lack of and/or inappropriate hardware and software available to him. Subsequently a request was made that the digital "evidence" collected be copied into a format suitable for the applicants' e-forensic expert. This procedure was undertaken at great expense by at least one of the respondents but clearly raises further questions about whether the chain of the custody was broken during these processes.

More broadly, these incidents provide some support for a perception presented in some media coverage of cases involving digital evidence that many so called e-forensic experts lack the appropriate skills. It has been suggested that a number of cases of this type have collapsed due to mistakes made by e-forensic experts. This points up a growing awareness of the need for some type of registration and certification of e-forensic experts. Particularly as currently in the UK and Australia, anyone with degree in computer science can act as an expert witness/forensic computing expert. In contrast, while conventional forensic experts in Australia have to be registered with the National Institute of Forensic Science and are subject to annual certification, no such requirement exists for forensic computing experts. Indeed, most Australian forensic computing teams in both the public and private sectors contain many staff without any formal technical or legal training in forensic computing.

Finally, returning to the MP3 piracy case, during the process requested by the applicants' e-forensic expert, backup data from magnetic tapes were restored to hard disks. While the data originated from UNIX machines, it is believed that the data were subsequently restored to hard disks formatted with either FAT or NTFS. During this process vital information could have been lost or changed. It should also be noted from an e-forensics perspective that in at least one of the Universities the disks were not physically handled in a completely safe way for evidence acquisition purposes. For example, the disks were not immediately put into static electricity proof containers and sometimes they were stacked on top of each other. All these processes could potentially lead to significant damage or even alteration of the evidence and contribute to a subsequent loss of the admissibility and/or validity of any data produced from them in the court.

The above discussion highlights a series of problems in dealing with digital evidence. The next section of this paper briefly examines the European Union funded Cyber Tools On-line Search for Evidence (CTOSE) project which has made a significant contribution to the development of a generic process model and advisory tools for conducting forensic investigations (CTOSE, 2003; Frings et al., 2003; Leroux & Pérez Asinari, 2003; Urry & Mitchison, 2003).

## **Cyber Tools On-Line Search for Evidence**

The project Cyber Tools On-Line Search for Evidence (CTOSE) was initiated to:

*“develop a methodology architecture, processes, a common set of tools and procedures for an electronic investigation. This standard methodology was deemed to be necessary for investigators (internal staff, external consultants, law enforcement), lawyers and judiciary, to have a common understanding about the difficulties of gathering, analysing, securing, storing and presenting electronic based evidence in a court or any form of commercial, civil investigation or legal prosecution” (CTOSE, 2003)*

From the outset, the CTOSE project began developing a reference process model resembling organisational, technical and legal guidelines on how a company should proceed when a computer incident occurs. The focus of this model is on the acquisition of digital evidence and on how it should best be collected, stored, secured and analysed in a manner that will be legally admissible should court proceedings be instigated. Figure 1 illustrates how this reference model links to a detailed examination of technical, legal and presentational requirements. The project also linked this model to the development of its own project software demonstrator.

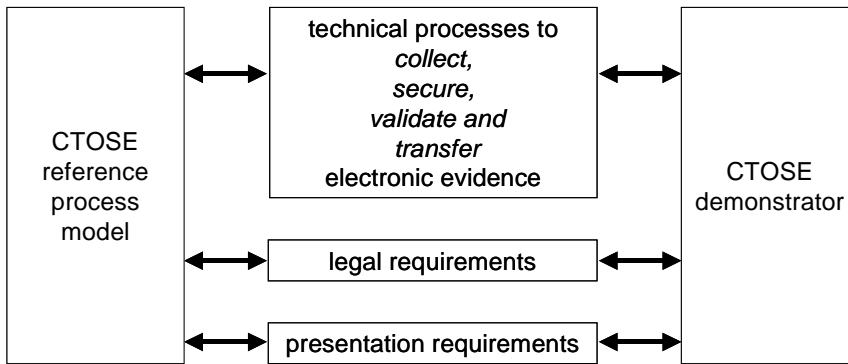


Figure 1: CTOSE Project

The reference process model involves five linked phases: preparation, running, assessment, investigation and learning phases. This process model describes the actions and decisions that have to be conducted as part of an investigation of computer misuse. Additional information including specific roles and responsibilities, the required skill sets, checklists and further guides to reference documents, tools and legal advice are also provided to support actions and/or decision in each phase (see Figure 2). The CTOSE approach prioritises the preparation phase (also called “Forensic Readiness”) because IT security measures critical to the whole process are defined and implemented in this phase, for example, implementing an intrusion detection system.

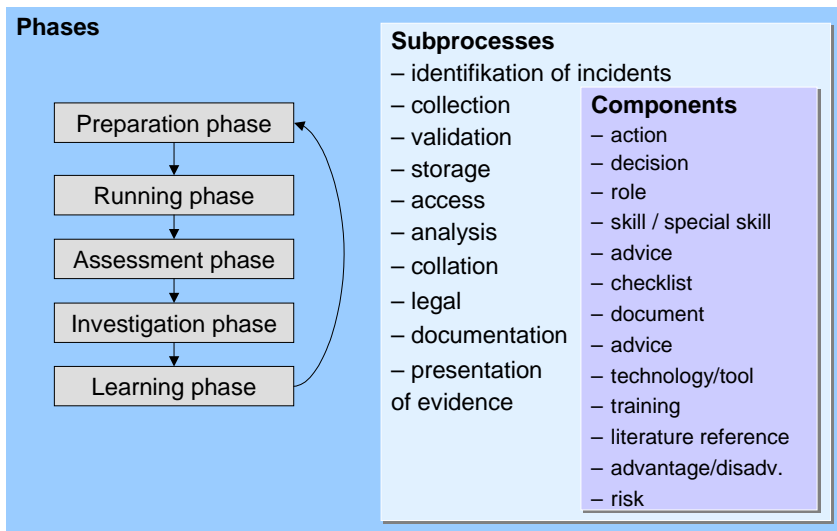


Figure 2: CTOSE Phases of response.

As a result of the complexity of the process reference model the CTOSE project developed an electronic version. This version is called the Cyber Crime Advisory Tool (C\*CAT) and involves a database connected to a database administration tool containing all actions, decisions, relationships (sequence of flow charts) and all additional information. The

architecture of C\*CAT is presented in Figure 3. Figure 4 presents a fragment of the CTOSE process model to highlight its depth and detail.

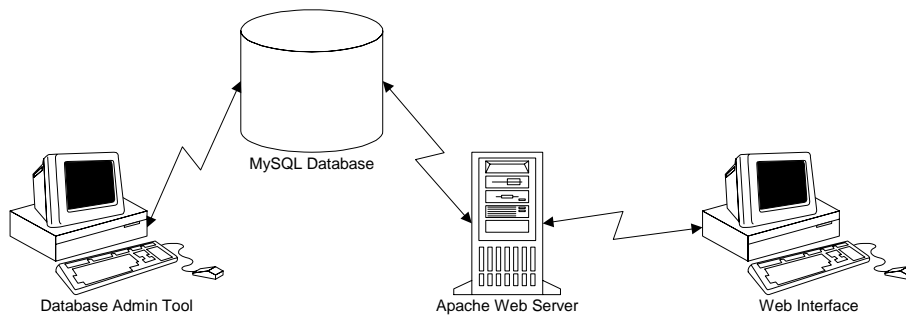


Figure 3: C\*CAT Architecture

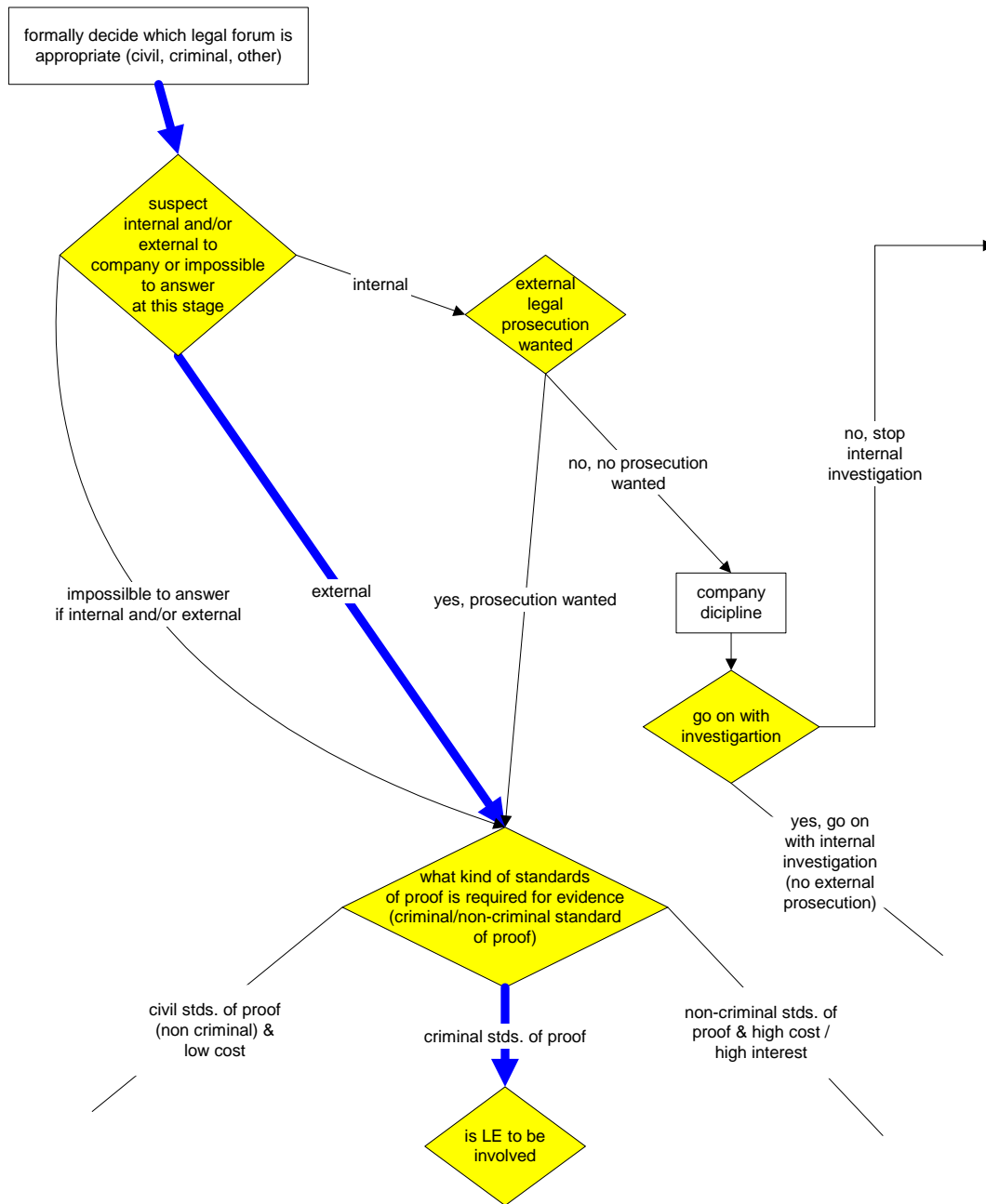


Figure 4: Fragment of the process model

The Web based front end of C\*CAT (see Figure 5) connected via an Apache Web server to the database is the interface between the information to be processed and the people involved in investigating a computer misuse incident.

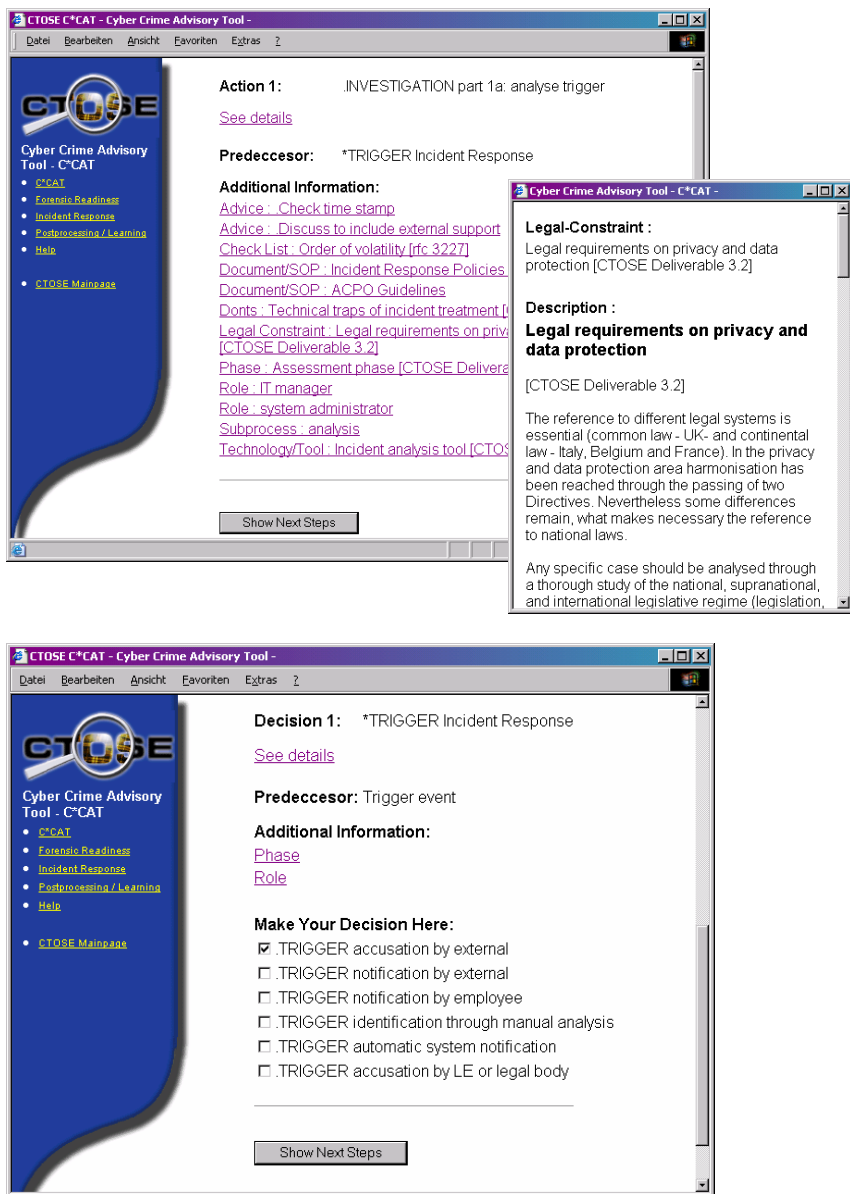


Figure 5: C\*CAT’s web based interface

C\*CAT is easy to use and enable users to define their situation (by selection among different choices and to present the appropriate actions and/or decisions to be followed. Through C\*CAT the user can also obtain further information, guidance and advice. Given the paramount importance of the chain of custody it is essential that the correct procedures are followed.

To further refine and improve the methodology and facilitate its adoption as widely as possible, the CTOSE project has developed a simulation environment (CTOSE Demonstrator) as an educational awareness and validation tool. This demonstrator “walks

through” a variety of scenarios using the process model and providing users with insight into do’s and don’ts when handling digital evidence during each phase (CTOSE, 2003; Frings et al., 2003; Urry & Mitchison, 2003). Clearly the CTOSE project has made a very significant contribution to developing a methodology for a standardized approach to computer misuse.

## Conclusion

This research paper has deployed a forensic computing perspective to examine a recent Australian federal court case involving the acquisition and use of digital evidence. This examination has revealed several serious issues relating to the level of understanding and knowledge displayed by all three parties involved in the case concerning digital evidence handling. More specifically, this examination has explored the issues and their implications for the legal admissibility of any digital evidence produced.

The paper has also presented details of recent attempts by the European Union funded Cyber Tools On-line Search for Evidence (CTOSE) project to address these digital evidence handling issues in a structured and coherent manner. Both the case and the work of CTOSE highlight the critical need for greater “forensic readiness” for dealing with criminal, illegal or inappropriate on-line behaviours. By leveraging these insights from theory and practice it is also possible to identify four key findings that highlight the need for on-going enhancement of “best practice” for digital evidence handling and for improving forensic computing knowledge amongst practitioners and in the broader community more generally.

These key findings are as follows:

- *“Best” practice for digital evidence handling involves deploying the highest investigative standards at all stages in the identification, analysis and presentation of digital data;*

When a computer incident occurs that requires an e-forensic response it is often not immediately evident as to the behaviours being investigated are criminal. Illegal or inappropriate and/or in what environment the digital evidence collected will subsequently be presented. For example, in an Australian context, the evidential requirements of criminal courts, civil courts and industrial tribunals display variation in relation to digital evidence admissibility, validity and weight. It is however safe to presume that digital evidence handling techniques that are good enough for the presentation of evidence in a criminal court will also be good enough for industrial tribunal dealing. For organisations, however it is clear that technical and training costs are likely to be incurred to ensure that these procedures can be followed.

- *Targeted training and education of network administrators and end-users in the key principles of digital evidence handling is urgently required;*

In many cases computer incidents and any associated digital evidence handling is dealt with by front-line network administrators. Many of these individuals have limited

experience of the most appropriate methods for digital evidence handling. While the ideal case would be that organisations would either have their own trained experts or would acquire services of suitable qualified experts from outside of the organisation it is necessary to provide suitable training to key stakeholders in principles of evidence handling. More generally, by raising the general awareness of these issues amongst end-users it is much more likely that computer incidents will be handled more quickly, more effectively and with a reduction in overall costs.

- *Opportunities exist for the further refinement of e-forensic methodologies and processes such as those developed by CTOSE;*

While the CTOSE approach is to be applauded, it has already been acknowledged that continued project refinement and development is required. Specifically, there is a need to evaluate the approach in the context of different jurisdictional systems. For example, not all actions that are appropriate digital evidence handling in one jurisdiction are suitable in another. These more legal issues of applicable law and cross-jurisdiction implications of digital evidence handling are one of the main driving forces behind the establishment of the not-for profit CTOSE Foundation. This foundation will aim to provide “constant updates of cyber attacks, modus operandi, new technologies and legislative changes” (CTOSE, 2003).

- *Enhancing e-forensic professionalism through the rapid development of processes for e-forensic computing competences and certification will lead to improved outcomes in the investigation and prosecution of computer misuse and e-crime.*

This research paper has highlighted the lack of formal professional accreditation within the field of forensic computing. The ease with which one can currently be deemed a forensic computing expert or act as an expert witness has also been mentioned. It has also been shown how easy it is to damage potentially crucial digital evidence. In this context, it is the opinion of the authors' that there is a need for the rapid development of processes and procedures to assess forensic computing expertise. It can be assumed that by enhancing the professionalism of forensic computing investigators the investigation and prosecution of computer misuse and e-crime will be enhanced.

More broadly, by enhancing forensic computing professionalism, it can be anticipated that this will lead to an increased awareness of these issues amongst the general public. From the users' perspective, education about appropriate behaviour in digital environments is remains a major issue (Broucek & Turner, 2003a). The majority of people are unaware of the legality of creating MP3 copies from their CDs and are unaware that “state-swapping” is illegal in Australia (Nelson, 2003). This is perhaps partly because the market is flooded with MP3 players and that some operating systems now come with “ripping software”. There is clearly an urgent need for improved user education in this regard (Broucek & Turner, 2003a).

More significantly, it can be argued that the approach adopted by the applicants and the Australian Federal Court in the MP3 piracy case is short-sighted and may back-fire on the

music industry's desire to crack-down on piracy. This is because it is probable that many users will now proceed to encrypt all of their communications to impede subsequent "snooping"<sup>5</sup>. Additionally, this case and the responses of all Australian Universities have resulted in making many network administrators in Universities reticent about reporting on suspected computer misuse of their systems. This is because they are either afraid that they will be held responsible or that they will have to conduct or be involved in e-forensic investigations for which they feel unqualified or for which they have inadequate time or resources.

---

<sup>5</sup> i.e. PGP or SSL with keys 1024 or greater. Of course, it can be argued that pushing the introduction of encryption will inhibit the availability of illegal material because with most current P2P Networking is hampered by this technique.

## References

- Aust unis in court over file-swapping (2003). [On-line]. Available: <http://www.zdnet.com.au/newstech/communications/story/0,2000048620,20272193,00.htm>. Last access: 2003, February 18.
- Broucek, V., Frings, S., & Turner, P. (2003). The Federal Court, the Music Industry and the Universities: Lessons for Forensic Computing Specialists. In S.-A. Kinght (Ed.), 1st Australian Computer, Network & Information Forensics Conference. Perth, WA, Australia.
- Broucek, V., & Turner, P. (2001a). Forensic Computing: Developing a Conceptual Approach for an Emerging Academic Discipline. In H. Armstrong (Ed.), 5th Australian Security Research Symposium (pp. 55-68). Perth, Australia: School of Computer and Information Sciences, Faculty of Communications, Health and Science, Edith Cowan University, Western Australia.
- Broucek, V., & Turner, P. (2001b). Forensic Computing: Developing a Conceptual Approach in the Era of Information Warfare. Journal of Information Warfare, 1(2), 95-108.
- Broucek, V., & Turner, P. (2002a). Bridging the Divide: Rising Awareness of Forensic Issues amongst Systems Administrators, 3rd International System Administration and Networking Conference. Maastricht, The Netherlands.
- Broucek, V., & Turner, P. (2002b). Risks and Solutions to problems arising from illegal or Inappropriate On-line Behaviours: Two Core Debates within Forensic Computing. In U. E. Gattiker (Ed.), EICAR Conference Best Paper Proceedings (pp. 206-219). Berlin, Germany.
- Broucek, V., & Turner, P. (2003a). A Forensic Computing perspective on the need for improved user education for information systems security management. In R. Azari (Ed.), Current Security Management & Ethical Issues of Information Technology. Hershey, PA 17033-1117, USA: IGP/INFOSCI/IRM Press.
- Broucek, V., & Turner, P. (2003b, May 8-9). Intrusion Detection Systems: Issues and Challenges in Evidence Acquisition. Paper presented at the CTOSE Conference, Facultés Universitaires Notre-Dame De la Paix, Namur, Belgium.
- Broucek, V., & Turner, P. (2003c). Intrusion Detection: Forensic Computing Insights arising from a Case Study on SNORT. In U. E. Gattiker (Ed.), EICAR Conference Best Paper Proceedings. Copenhagen, Denmark.
- CTOSE. (2003). CTOSE Project Final Results.
- Frings, S., Stanisic-Petrovic, M., & Urry, R. (2003). Holistic Approach for Processing Electronic Evidence Related to High-Tech Crime and Severe Disputed Electronic Transactions: Cyber Crime Advisory Tool - C\*CAT. In U. E. Gattiker (Ed.), EICAR 2003 Conference Best Paper Proceedings. Copenhagen, Denmark: EICAR.

- Hannan, M., Frings, S., Broucek, V., & Turner, P. (2003). Forensic Computing Theory & Practice: Towards developing a methodology for a standardised approach to Computer misuse. Paper presented at the 1st Australian Computer, Network & Information Forensics Conference, Perth, WA, Australia.
- Hannan, M., Turner, P., & Broucek, V. (2003). Refining the Taxonomy of Forensic Computing in the Era of E-crime: Insights from a Survey of Australian Forensic Computing Investigation (FCI) Teams. Paper presented at the 4th Australian Information Warfare and IT Security Conference, Adelaide, SA, Australia.
- Lamount, L. (2003). Recording firms ask to scan university computers [On-line]. Available: <http://www.smh.com.au/articles/2003/02/18/105330603596.html>. Last access: 2003, February 19.
- Leroux, O., & Pérez Asinari, M. V. (2003, May 8-9). Collecting and Producing Electronic Evidence in Cybercrime Cases. Paper presented at the CTOSE Conference, Facultés Universitaires Notre-Dame De la Paix, Namur, Belgium.
- Morgan, A. (2003). It's war on a generation of cyber pirates [On-line]. Available: <http://www.smh.com.au/articles/2003/02/17/105330539310.html>. Last access: 2003, February 18.
- Nelson, D. (2003, August 5). Student piracy row may leave IT to face the music. The Age, pp. Next 3.
- Online piracy hurts 2002 music sales: ARIA (2003). [On-line]. Available: <http://www.zdnet.com.au/newstech/communications/story/0,2000048620,20271487,00.htm>. Last access: 2003, January 24.
- Pearce, J. (2003). Evidence of piracy allegedly destroyed [On-line]. Available: <http://news.zdnet.co.uk/business/0,39020645,2138165,00.htm>. Last access: 2003, July 25.
- Rose, D. (2003, August 2). Uni hit by Net piracy action. The Saturday Mercury, pp. 13.
- Sommer, P. (1998). Intrusion Detection Systems as Evidence, Recent Advances in Intrusion Detection - RAID'98. Louvain-la-Neuve, Belgium.
- Sony Music Entertainment (Australia) Limited v University of Tasmania [2003] FCA 532 (30 May 2003). (2003). Federal Court of Australia.
- Sony Music Entertainment (Australia) Limited v University of Tasmania [2003] FCA 724 (18 July 2003). (2003). Federal Court of Australia.
- Sony Music Entertainment (Australia) Limited v University of Tasmania [2003] FCA 805 (29 July 2003). (2003). Federal Court of Australia.
- Sony Music Entertainment (Australia) Limited v University of Tasmania [2003] FCA 929 (4 September 2003). (2003). Federal Court of Australia.
- Urry, R., & Mitchison, N. (2003, May 8-9). CTOSE Project. Electronic Evidence: gathering, securing, integrating, presenting. Paper presented at the CTOSE

Conference, Facultés Universitaires Notre-Dame De la Paix, Namur,  
Belgium.