

The Federal Court, the Music Industry and the Universities: Lessons for Forensic Computing Specialists

Vlasti Broucek¹
Sandra Frings²
Paul Turner¹

¹School of Information Systems,
University of Tasmania,
e-mail: Vlasti.Broucek@utas.edu.au
Paul.Turner@utas.edu.au

²Fraunhofer Institut fuer Arbeitswirtschaft und Organisation,
Competence Center Software-Management,
Stuttgart, Germany
e-mail: Sandra.Frings@iao.fhg.de

Abstract

The recent judgement in the Australian Federal Court case involving the Music Industry and three Australian Universities is disturbing in a number of ways. Aside from the worrying implications of the judgement for individual privacy and data protection, the case has revealed serious flaws in understanding amongst all participants over the nature of digital evidence and how it should best be collected, analysed and presented. In this context, this paper reviews the case from a forensic computing perspective and considers the approaches of the three parties involved – applicants, respondents and federal court judge. The paper also recommends the development of standard framework for forensic investigations and briefly presents the framework proposed by European CTOSE project. The paper concludes by considering the implications of this case for the forensic computing domain.

Keywords

MP3, computer forensics, process model, CTOSE, C*CAT, legal, privacy, cyber crime, federal court

INTRODUCTION

The recent case in the Federal Court of Australia 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 interest and debate. Unfortunately, much of the debate and conjecture around the case has been misplaced due to incorrect reporting in many media reports that suggested the case was about the Universities being sued for copyright infringement. There were also other media reports suggesting eleven Australian Universities were involved in the “MP3 Piracy Case” as it has alternatively been called (Aust unis in court over file-swapping, 2003; Lamount, 2003; Morgan, 2003; Rose, 2003). If this is the situation, it is indeed noting that of all the Australian Universities approached only these three offered any resistance to initial requests by the Music Industry for access to their digital files and networks.

In reality this Federal court case was procedural in nature and involved the Music Industry applicants seeking a “discovery ruling” against the three Universities involved. This paper reviews the case, identifies issues and challenges and draws out lessons for forensic computing specialists. The paper also presents details of the European “Cyber Tools On-line Search for Evidence” (CTOSE) project and its reference process model that has made a major contribution to the development of a standardised approach to the conduct of forensic computing investigations (Frings, Stanicic-Petrovic, & Urry, 2003; Urry & Mitchison, 2003).

THE CASE SO FAR

On January 23, 2003 the Australian Record Industry Association (ARIA) released information suggesting that the industry was suffering significant losses in earnings due to on-line piracy and that the industry was determined to combat these activities (Online piracy hurts 2002 music sales: ARIA, 2003). While peer-to-peer (P2P) networks were not specifically targeted in this case, ARIA also cited its US counterpart, the Record Industry Association of America (RIAA), ongoing war with peer-to-peer networks and their users. At around

the same time three Australian Universities (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 these Universities systems of the distribution of MP3s by students and staff at these Universities.¹ These MP3s and distribution activities were being categorised by the music industry as potentially constituting breaches of copyright laws. Subsequent to this request to the Universities, the members of the music industry further requested access to this evidence for discovery. In response the three Universities concerned refused to provide this access².

On February 18, 2003 these music industry members (applicants) launched legal proceedings against the respondents in order to gain access to the evidence preserved by the respondents at their request. The basis of the legal proceedings were procedural with applicants seeking a right of access to the preserved 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.

At the initial hearing on February 18, 2003 the case was adjourned and orders made to the respondents to preserve the data. Immediately, the case and initial ruling created outrage amongst academics, students and civil liberty groups who viewed this as the beginnings of a major assault on the privacy of individuals. Indeed, the demands made by the applicants at the initial hearing were labelled as "witch-hunting" and using students and Australian universities as "scapegoats". A series of questions were raised, including as to whether Universities should be forced into the role of policing and/or taking responsibility for the on-line activities of their staff and students (Morgan, 2003).

Subsequently, 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 applicants ("Sony Music Entertainment (Australia) Limited v University of Tasmania [2003] FCA 532 (30 May 2003)," 2003) and on July 18, 2003 ordered the respondents to hand over the evidence 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). While the legal right of the court to make this ruling cannot be doubted, it raises serious questions about the courts understanding of the nature of the digital evidence in question. Significantly, on July 29, 2003 ("Sony Music Entertainment (Australia) Limited v University of Tasmania [2003] FCA 805 (29 July 2003)," 2003) Justice Tamberlin also 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" when one of the respondents pointed out that the backup tapes in question had accidentally been overwritten and therefore did not have any forensic value for the applicants (Pearce, 2003). Again, this reveals a worrying lack of understanding of the technical nature of digital logs and data storage. While there may have been a "suspicion over the accidental overwriting", from a technical perspective it was inappropriate to consider overwritten backup tapes as part of the 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)

Subject of dispute

Initially, the three Universities involved did not agree with the request for the discovery at all. However, as the case has evolved these respondents have been forced to find additional arguments to oppose the arguments used as the basis for the requests made by the applicants. The respondents' 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. They had however been willing from the outset to provide some digital evidence to the applicants, providing that this evidence was collected by 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.

¹ In the case of the University of Tasmania, music industry legal representatives sent an e-mail regarding one particular www site that was hosting copyright MP3 files. These were found using a Google™ search. Subsequently, these machines were copied as requested (using ufsdump not dd) and stored in the fire proof safe in late January 2003.

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

From the beginning the applicants demanded the rights to conduct full forensic investigation of the preserved data. It should be noted that the vast 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. However, what is certain is that the much of 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 however, 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. These applicants are then allowed to “mine” this data in search of what they themselves deem “illegal practices”. Quite apart from the intrusion into the data of thousands of “presumably innocent” users, issues of data tampering/manipulation (except where MD5 checksums are calculated and stored by respondents), breaches of privacy, commercial dealings, intellectual property are all only protected by confidentiality provisions placed on the applicants.

As a result of this case and concerns over the issues at stake in such “data hand-overs”, the majority of Australian Universities have now started to conduct their own forensic investigations. Numerous Universities have embarked on “scare campaigns”, reminding staff and students about importance of copyright protection and possible outcomes for breaches. They have also engaged in network traffic monitoring and scanning computers for mp3 files often without knowledge of the users (Nelson, 2003a). Many of these searches are being conducted in a manner that further creates dangerous precedents and fears over violations of privacy and academic freedoms. In many instances the techniques employed were very amateur. For example, in one instance computers and servers were searched using the find command with *.mp* mask . Searches of this type clearly produce numerous false positives and identify files that do not have anything to do with audio or video recordings (e.g. files with extension *.mpp that belong to Microsoft Project program). Furthermore, many audio card drivers and software themselves contain sample mp3 format files (e.g. the Microsoft Software Development Kit (MSDK) contains mp3 and mpg samples). As a consequence, many users were harassed by overly active and poorly instructed network and computer administrators and forced to delete legitimate files in a fear of possible copyright law breaches.

Combined, this case and the responses of Australian Universities have resulted in making many network administrators at the Universities afraid to report 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 forensic investigation for which they feel unqualified.³

ISSUES IDENTIFIED

From a forensic computing perspective, this case and the responses of its participants highlight a number of issues worthy of consideration. Firstly, from the users’ perspective, education about appropriate behaviour in digital environments is still a major issue (Broucek & Turner, 2003a). The majority of people are not aware of the legality of creating mp3 copies from their CDs and are not aware that “state-swapping” is illegal in Australia (Nelson, 2003b). This is perhaps partly because the market is flooded with MP3 players and that some operating systems now come with “ripping software”. There is therefore an urgent need for improved user education (Broucek & Turner, 2003a).

Secondly, it is noticeable that none of the Universities involved in the case were prepared for the initial request for the preservation of the evidence. The initial collection was conducted by the Universities network and systems administrators, without any training in forensic procedures as is evidenced by the nature of the evidence collection and storage processes used. File level copies of file systems were made to CD-ROMs or standard backup procedures were used to preserve the evidence .For example, in the case of University of Tasmania, the standard backup tapes created were subject to the discovery and the evidence from one particular computer where allegedly illegal MP3 files were held was collected by standard UNIX backup command, ufsdump.

While these tapes may contain the necessary evidence of files being stored on the computers, in the opinion of the authors, this evidence will be of very low value in a subsequent legal proceedings as it was not collected using binary copies and neither the chain of custody or rules of evidence were followed (Broucek & Turner, 2001, 2002a, 2002b, 2003b).

Thirdly, the approach adopted in the case is potentially short-sighted in that it is probable that many University users will now proceed to encrypt all of their communications to impede subsequent “snooping” Overall this highlights a lack of “forensic readiness” on the part of all participants and the need for set procedures, covering

³ Also resource requirements in SW, HW and HR.

all possible variants of investigations involving digital evidence to reveal any criminal, illegal or other inappropriate behaviours. Forensic procedures should be in place to protect organisations and in this context the next section briefly examines the CTOSE framework that has made a significant contribution to the development of a generic process model and advisory tools for conducting forensic investigations (Frings et al., 2003; Urry & Mitchison, 2003).

THE CTOSE PROJECT

The European Union (EU) funded project “Cyber Tools On-Line Search for Evidence (CTOSE)” has developed a methodology that aims to provide a consistent approach for identifying, preserving, analysing and presenting digital evidence. The primary motivation behind the establishment of the CTOSE project was to improve the ability of companies to respond to computer misuse incidents. In this regard, the CTOSE project began by developing a reference process model resembling organisational, technical and legal guidelines on how a company should proceed when computer misuse occurs. The focus of the model is on the acquisition of digital evidence and on how it is to be collected, conserved 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, which in-turn link to the project software demonstrator.

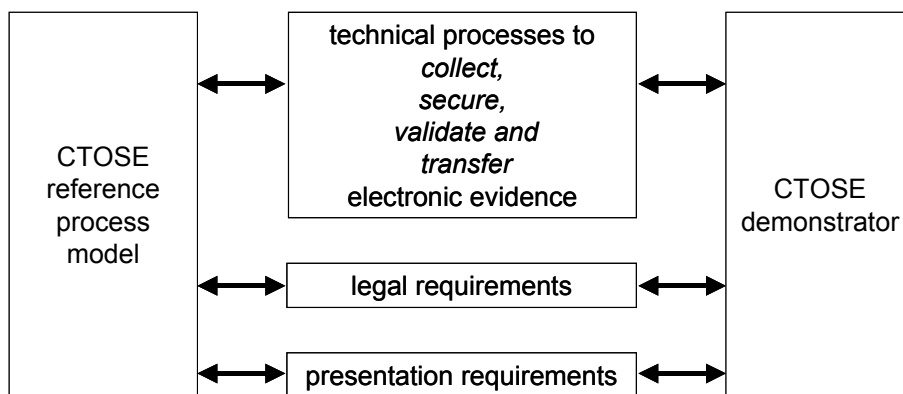


Figure 1: CTOSE Project

The reference process model is composed of five phases: preparation, running, assessment, investigation and learning phases. It articulates the flow of actions and decisions that have to be considered or executed in the case of an investigation of computer misuse. Moreover, additional information, (including: roles and their necessary skills, checklists, references to documents and tools, and legal advice) to support the action or decision in each step (see Figure 2). In this way a user can consult a checklist, prior to reporting an IT incident, which covers what technical information about the incident law enforcement agencies may require from the person involved. This should result in optimising communication between the two parties.

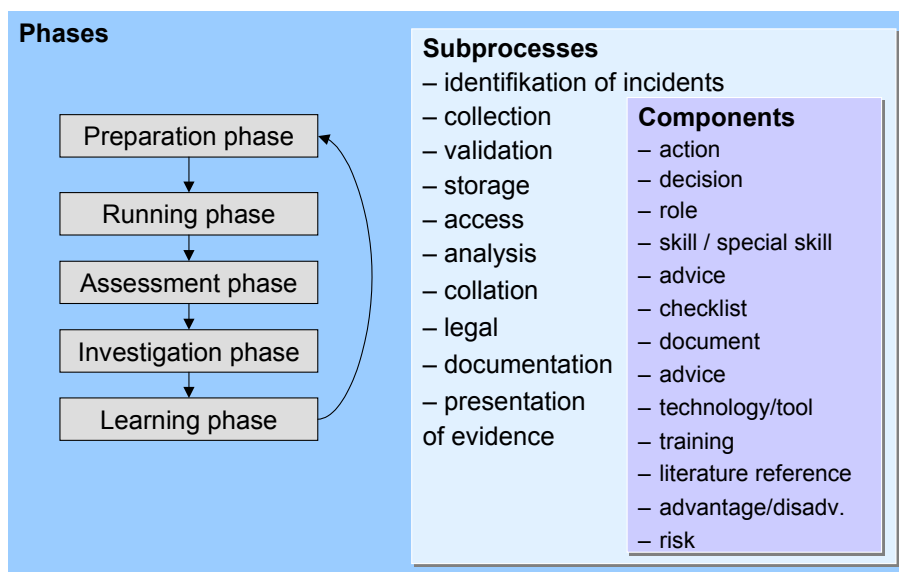


Figure 2: CTOSE Phases of response.

Significantly, the CTOSE project emphasizes the preparation phase, also referred to as “Forensic Readiness”, because IT security measures critical to the whole process are defined and implemented in this phase. For example, this phase includes the implementation of a firewall and/or an intrusion detection system.

The Software Prototypes:

As a consequence of the complexity of the process reference model (see Figure 3 for a fragment of it) it was decided that the CTOSE project would develop 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 4.

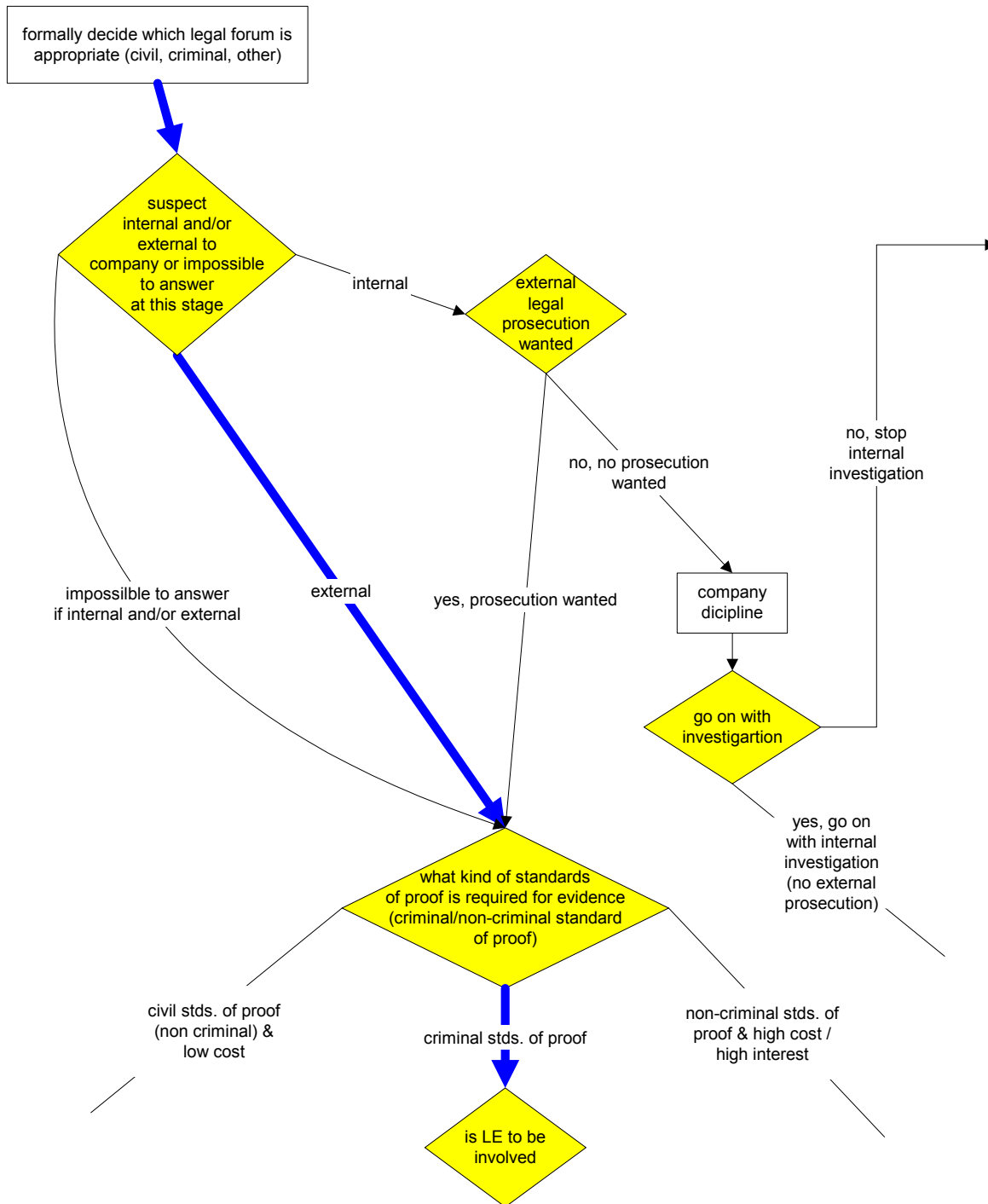


Figure 3: Fragment of the process model

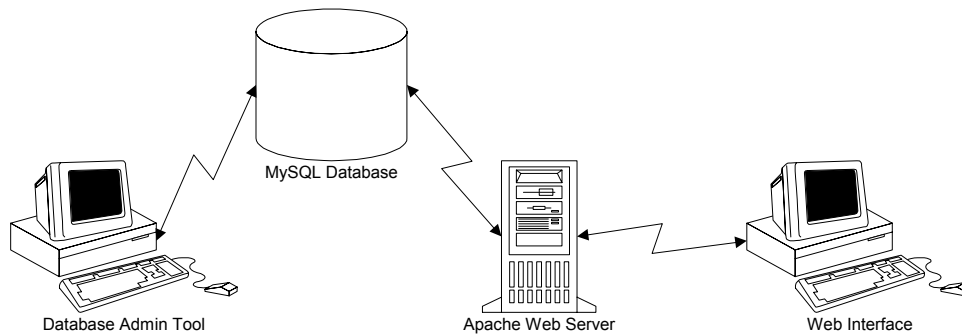


Figure 4: C*CAT Architecture

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.

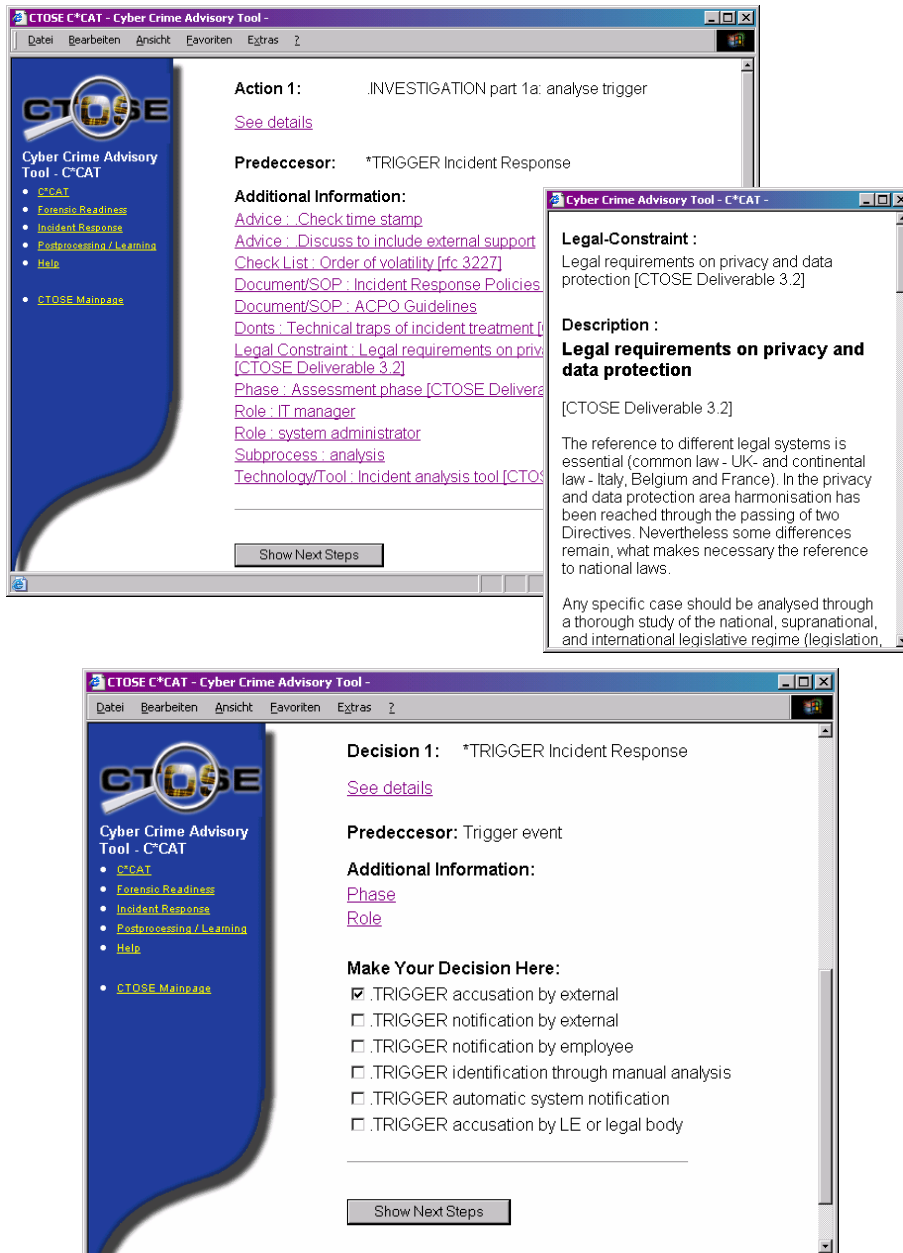


Figure 5: C*CAT's web based interface

From evaluation of C*CAT it is clear that it is easy to use, and allows users to define the situation (by selection among different choices). Following this phase C*CAT presents the necessary actions and decisions that should be taken. In each case the user is able to ask for more advice and guidance. Since the integrity of the chain of custody is critical, following correct procedures is of vital importance. At the end of the process, the user will be able to give feedback concerning the usage of the model to further improve its operation and utility.

The future aim of CTOSE is to refine and improve the methodology and distribute it as widely as possible. As part of these activities the CTOSE project has developed a simulation environment (CTOSE Demonstrator) as an educational awareness and validation tool. The demonstrator describes the process model using several different scenarios. Each scenario provides the user with a clear and understandable way to proceed with do's and don'ts when handling digital evidence for each phase. The project anticipates that the widespread utilization of the CTOSE methodology will assist companies in being able to recover more rapidly from computer misuse incidents and improve their ability to conduct computer forensic investigations (Frings et al., 2003; Urry & Mitchison, 2003). CTOSE project has made a very significant contribution to developing a methodology for a standardized approach to computer misuse.

CONCLUSION

This paper has reviewed and examined the recent Australian Federal Court case between the music industry and three Australian Universities. From a forensic computing perspective the case reveals the strong and urgent need for development of standard procedures for collecting and preserving the digital evidence and the need for greater "forensic readiness" whether dealing with criminal, civil or inappropriate on-line behaviour. While it remains unclear what the end result of the "discovery" activities of the music industry will be, it is evident that the case also has a number of worrying implications for individual users' privacy and the confidentiality of data held within institutions. In responding to the need for a standard approach, the CTOSE project has made a significant contribution in this regard, however it is clear that further refinement and development is required.

REFERENCES

- Aust unis in court over file-swapping. (2003). Retrieved February 18, 2003, from <http://www.zdnet.com.au/newstech/communications/story/0,2000048620,20272193,00.htm>
- Broucek, V., & Turner, P. (2001). 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. (2002a). Bridging the Divide: Rising Awareness of Forensic Issues amongst Systems Administrators. In 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.
- 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.
- Lamont, L. (2003). Recording firms ask to scan university computers. Retrieved February 19, 2003, from <http://www.smh.com.au/articles/2003/02/18/105330603596.html>
- Morgan, A. (2003). It's war on a generation of cyber pirates. Retrieved February 18, 2003, from <http://www.smh.com.au/articles/2003/02/17/105330539310.html>
- Nelson, D. (2003a, August 5). Protecting intellectual property. *The Age*, p. Next 3.

- Nelson, D. (2003b, August 5). Student piracy row may leave IT to face the music. *The Age*, p. Next 3.
- Online piracy hurts 2002 music sales: ARIA. (2003). Retrieved January 24, 2003, from <http://www.zdnet.com.au/newstech/communications/story/0,2000048620,20271487,00.htm>
- Pearce, J. (2003). Evidence of piracy allegedly destroyed. Retrieved July 25, 2003, from <http://news.zdnet.co.uk/business/0,39020645,2138165,00.htm>
- Rose, D. (2003, August 2). Uni hit by Net piracy action. *The Saturday Mercury*, p. 13.
- Sony Music Entertainment (Australia) Limited v University of Tasmania [2003] FCA 532 (30 May 2003) (Federal Court of Australia 2003).
- Sony Music Entertainment (Australia) Limited v University of Tasmania [2003] FCA 724 (18 July 2003) (Federal Court of Australia 2003).
- Sony Music Entertainment (Australia) Limited v University of Tasmania [2003] FCA 805 (29 July 2003) (Federal Court of Australia 2003).
- Sony Music Entertainment (Australia) Limited v University of Tasmania [2003] FCA 929 (4 September 2003) (Federal Court of Australia 2003).
- 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.

ACKNOWLEDGEMENTS

This paper is sponsored by European Institute for Computer Anti-Virus Research (EICAR).

COPYRIGHT

Vlasti Broucek, Sandra Frings, Paul Turner © 2003. The author/s assign the We-B Centre & Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to the We-B Centre & ECU to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors.