Proceedings of the 8th Colloquium for
Information Systems Security Education
West Point, NY June 2004

Teaching Computer Forensics: Uniting Practice with Intellect

Colin Armstrong and Nimal Jayaratna

Abstract

The demand for skills and knowledge in computer forensics has risen over the past decade in response to the increased use of computers and the Internet to commit crime. Computer forensics requires specialist technical skills. However, computer forensics is also cross-discipline, encompassing the areas of, criminology, psychology and criminal profiling, investigative techniques together with aspects relating to the law, expert witness and testimony.

This paper introduces the nature and content of the computer forensics module at Curtin University and discusses the underpinning philosophy of the module and how it fits within a wider framework of the masters programs.

Index terms – Information Assurance, Infrastructure Assurance, Forensics

I. Introduction

The increasing use of computers and the Internet to commit crimes and to record criminal activities has lead to a corresponding demand for skills and knowledge in how best to recognize the occurrence of a computer crime, and how best to investigate, apprehend and where practical prosecute perpetrators. It is this digital world that is the domain of the computer forensics practitioner.

Computer crime is of such a nature that it is often difficult for the general public to perceive or to understand that a crime has actually occurred. Computer technology is used as a tool to perpetrate crimes (e.g. computer intrusion, stalking, harassment, and fraud), and they can contain evidence related to a crime [1]. Criminals are using computers to store records regarding drug deals, money laundering, embezzlement, mail fraud, telemarketing fraud, prostitution, pornography, gambling matters, extortion, and a myriad of other criminal activities [2].

Forensic is defined as belonging to, used in, or suitable to courts of judicature or to public discussion and debate [3]. Computer forensics is, the coherent application of methodical investigatory techniques to solve crime cases [4]. They continue this definition with; "preservation, identification, extraction, documentation and interpretation of computer data." Computer forensics involves the "preservation, identification, extraction, and documentation of computer evidence stored as data or magnetically encoded information" and is about evidence from computer systems that is sufficiently reliable to stand up in a court of law [5]. Vacca goes on to suggest that evidence is transparently created by the computer system's operating system without the knowledge of the user. Computer forensics is currently making an important transition from a 'black art', relegated to a select few, to a requisite component of the information security enterprise [6].

While, computer forensics requires practitioners to possess specialist technical knowledge and skills in computer architecture, operating systems, network and communications hardware and software, encryption and data hiding, computer forensics is also cross-discipline, encompassing the areas of criminology, psychology and criminal profiling, together with legal aspects relating to the law, expert witness and testimony.

During recent times, the coherent application of methodical investigation techniques to solve crime cases has increased, as has public interest in crime investigation. Patricia Cornwell's novels provided a relatively sophisticated understanding of forensic pathology. This interest led to documentaries and TV series covering the activities of police forensic technicians designed for those with a morbid fascination seeking entertainment. Everyone likes a mystery in life, but interest in crime scene investigation strikes a deeper chord. The application of skills, high-tech tools, and precise methodology in the fight for justice is a compelling story that is hard to resist [4]. This perception both assists and hinders computer forensics practitioners. It is the role of universities to capture this induced enthusiasm and through diligent application of three essential key knowledge areas, computing technology, investigative techniques and jurisprudence, to lead the enquiring mind to develop the knowledge and skills

Colin Armstrong, School of Information Systems, Curtin University of Technology, Perth WA 6845 Australia
Professor Nimal Jayaratna, Graduate School Business, Curtin University of Technology, Perth WA 6845 Australia

ISBN 0-87145-192-1/04/$15.00

demanded of a computer forensics practitioner. See Figure 1.

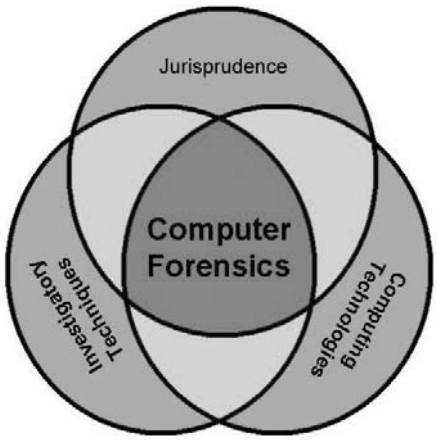

Figure 1.
Multi-Disciplinary Nature of Computer Forensics

II. The Three Essential Knowledge Areas

At the technical level, an investigator must understand how these systems work including basics such as the binary system and the ordered sequences of addressing. While the binary system utilizes interpretive rules for numbering systems, little endian and big endian, hexadecimal, floating point and binary coded decimal, other considerations include file types, signatures and various formats within a myriad of structures, architectures and platforms. The investigator's knowledge must be such that when confronted with a 'box' they know the most appropriate action to take to avoid damaging or destroying potential evidence. Being familiar with the physical bits and pieces is only a part of the technical skills required. It is important that the practitioner understands the implications of a set of given actions. For example, removing the supply of electrical power will result in a computer acting differently to being turned off or being powered down in an orderly fashion. Likewise knowing and understanding boot sequencing, the Power On Self Test - POST, BIOS, CMOS and bootstrap loader, the Master Boot Record and information about partitioning can be critical. With rotating magnetic media, the practitioner should understand not only the physical construction and manner of workings but also its encoding methods and formatting.

Having an understanding of what is happening, how, where, when and why enables a computer forensics practitioner to focus on discovering evidence that may be well hidden and to know what data is on the disk, and how that data is normally accessed. This understanding will assist in being able to identify unknown programs, run the program on a sacrificial machine in case the program turns out to be destructive.

A practitioner may be required to undertake other specialized tasks depending upon their individual skills and abilities. These may include, but are not restricted to; data duplication or preservation, data recovery, cleaning or removing data from rotating magnetic media prior to disposal through public sale, document searches, media conversion as with old media (5¼" and 8" floppy) to current readable formats, training, advice and planning. These services may complement corporate responsibilities of due diligence, duty of care, and being able to maintain a forensically sound record not dissimilar to a data backup so as to protect critical information or protect information at a critical point during a project.

In addition to this technical knowledge, a court of law will also require the investigator to employ well-defined procedures within their methodology. Both prosecution and defence experts will carry out tests on the evidence so the results must be repeatable, and produce consistent results. With this knowledge it is possible to discover and make sense of digital evidence collected in an investigation.

There are two primary reasons for instigating an investigation; prevention (being able to combat, prevent or lessen impacts of future occurrences by knowing what and how an occurrence happened) and to determine responsibility (to be able to punish perpetrators, victims have a responsibility to the community to permit gathering and analysis of evidence which may lead to prosecution).

To be valid, evidence is required to be admissible, authentic, complete, reliable, and believable. A practitioner must understand the significance between real evidence, ie any evidence that speaks for itself, and testimonial evidence supplied by a witness and hearsay. The main principles for evidence are authenticity, reliability, completeness and freedom from interference and contamination [5]. In this context, authenticity ensures the source of the materials is actually where it claims to come from. Reliability ensures consistency of the material and the 'correct working order of the computer'. Completeness refers to the entirety of the story and questions whether other stories can be drawn from the same material; and freedom from interference and contamination ensures that evidence has not been altered or corrupted in any way.

Edward Locard (1877-1966) was responsible for presenting one of the first recorded forensic principles. This became known as Locard's Exchange Principle:

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

> "Anyone or anything entering a crime scene both takes something of the scene with them, and leaves something of themselves behind when they leave" [1]

Due to the risk of damage to potential evidentiary materials arising from Locard's Exchange Principle certain safeguards must be implemented to ensure actions by investigating personnel do not contaminate digital evidence and thereby jeopardizing a case. Just as perpetrators leave traces of electronic evidence in numerous locations, i.e. logs and files, during normal computer usage, so too does an investigator. Locard's Exchange Principle applies in any criminal situation, including electronic and computer-based crimes. An investigator must ensure that opportunities for contamination to occur are either removed or diminished to a minimum and that these remaining contaminations are accounted for.

In addition, the investigation must be faithfully recorded, complete, without distortion, bias, nor breaks in the sequence of events. In creating the reconstruction of the chain of events account, the timeline should show the sequence of events accounting for any clock drift, delayed reporting, and different time zones. To maintain the integrity of the Chain of Evidence and protect it from contamination or alteration, it must be possible to account for all that has happened to the exhibit between its original collection and its presentation, uncontaminated, in court. All procedures used in examination should be auditable. Experienced practitioners should work from isolated computing equipment and never work on the originally collected data. During the crime to court journey, see Figure 2, and beyond, it is imperative that evidence is managed in an appropriate manner. As with accepted and fairly standard practices of law enforcement agencies, there should be a standard operational procedure that secures the integrity of data collected as evidence by clearly showing when where who why and how evidence was collected, transported and stored. These issues may become critical to a successful prosecution if as shown in Figure 2, there is an extended period between the time that a crime is suspected, the time that an investigation commences and subsequently to a hearing.

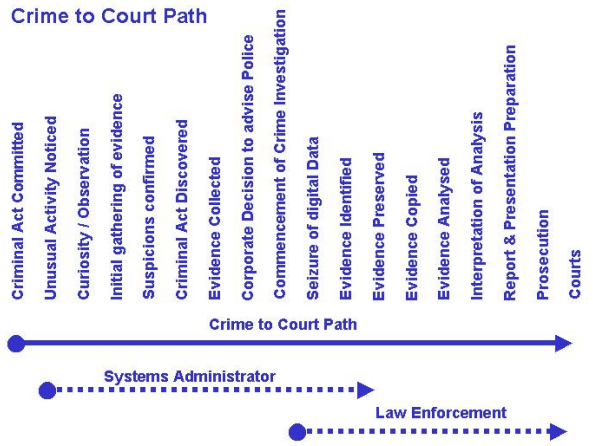

Figure 2: The Crime-to-Court Path

To uphold the chain of custody, evidence must be proven to be accounted for at all times, its passage from one party to the next, and from one location to the next fully documented. Casey's *Empirical Law of Digital Evidence Collection and Preservation* states that if you only make one copy of digital evidence, that evidence will be damaged or completely lost [1]. The results of an investigation may become evidence in a court of law, leading to the third area of skills and knowledge.

Finally, an investigator needs to develop a sense for discovering the important the facts at the heart of a case that prove or disprove the need for prosecution. This requires the practitioner possess a comfortable familiarity with criminology practices, crime scene investigation techniques, psychology and criminal profiling, as well as a working knowledge of criminal and civil law, and being able to present expert witness testimony.

Evidence gathered and analyzed during an investigation is of little value unless able to withstand the rigors of adversarial examination, be it at a disciplinary hearing or any of the courts in the hierarchy of the court system. In each country there will be legislation relevant to computer forensics practitioners. Practitioners should become familiar with any legislation likely to impact or apply to a case in hand including audit, banking, corporations, crime and cyber-crime, evidence, health services, taxation, telecommunications, archives and privacy legislation.

One could argue that law is the most challenging aspect of computer forensics simply because there are so many jurisdictions in the world. While a computer forensics specialist practicing in the jurisdiction of Australia must understand the three main sources of Australian law: common law, equity; and statute law, they must also be prepared to act in accordance with legal requirements of other jurisdictions when required.

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

For investigative findings to be accepted in a court of law they must be recognized by other experts within the field and conform to national and international standards of practice. The risks facing a computer forensics investigator include loss of credibility if another expert witness can demonstrate that proper or appropriate courses of action were mismanaged. The expert is required to explain technical terms and concepts in layman's terms to the judge and members of the jury. This ensures all those involved understand the evidence presented, upon which they are making a decision regarding the innocence or guilt of the accused.

In an effort to explain technical concepts in layman's terms, the approach used in the Kevin Mitnick case was 're-creation of the link between the defendant, a physical node, an IP address, an account and user name, the various conduits through which the criminal activity took place and the initial and related computer crimes' [7]. In order to enhance the judge and jury's understanding of the technological aspects of the case before them, the prosecution's case specifically detailed the forensic activities carried out on the specific switching or networks hacked by Mitnick (ie The Well, Netcom, Raleigh and Cell Switches) in the form of a diagram [7]. Expertise in the presentation of technical concepts in a court of law will be advantageous to the computer forensics practitioner. 'Regardless of the relative sophistication of the judge or jurors, results can vary, but far more often than not they come down to the story the expert chooses to tell and how well he or she tells it' [7]. Investigators and prosecutors will be influenced by their own view of the world emanating from their personal experiences and restrictive specialist practices. Jayaratna [8] refers to this as the practitioner's 'mental construct'. Values, ethics, motives, prejudices, experiences, reasoning ability, knowledge and skills, structuring processes, roles, and framework and models all interact in a dynamic way to form this mental construct. Some legal professionals are constrained in their decision-making by their own deep traditions and narrow local influences [7].

All aspects of preparing a case covered to this point become of little value if the credibility of the expert witness, or the witness with expertise, is discredited and there follows a loss of credibility. The credibility of an expert witness may be crucial to the outcome of a case and where the volume of work and the increasing number of investigations demand quick results there may be a tendency to select new automated examination and analysis tools. Government agencies within the USA have approximately 1400 active cases of cyber crime being investigated and this number does not include the myriad of cases where computers have been seized and evidence gathered and analyzed to support other crime cases [9]. Under these circumstances there is the potential to discredit an expert witness because as point and click wizards they may be perceived to have insufficient depth of expertise [6]. Use of point and click computer forensics application software, although allowing non-specialists to analyze evidence, is thus limited in its application. For example, a Windows based tool is limited to the functions offered by the Microsoft operating system on which the application sits. The admissibility of evidence processed by such applications in a court of law is sometimes questionable, as the investigator may not be able to explain how the software analyzed the data or images or arrived at the given findings. Automated based tools may also miss potential evidence due to the limited nature of the design, execution of code, and presentation of potential evidence found. The implications are that computer forensics practitioners appearing in a court of law (either for the prosecution or defence) need to understand not only legal and judicial matters, but also be able to present a convincing case for the admissibility of evidence.

Before discussing the education issues related to computer forensics, it is indisputable that we live and work in a digital age and world. That there are both corporate and government assets controlled and managed via the conduits of the digital world is indisputable. Without suggesting that digital crime is limited to corporate and government assets, it must be accepted that international banking, international air traffic control, inter-nation diplomacy, and the day to-day operational management of multinational corporations is simply not viable in today's world without this digital benefit and that there are elements within our society that will for what ever reason attack these assets. Indeed one could argue that there are not many facets of society or institutions and other essential services that are not exposed to digital risk. That digital crime is occurring in the digital world is indisputable. That this is not a desirable situation is also indisputable. From this one can conclude that it is necessary to protect these digital assets and to capture and punish unacceptable activities committed against these assets. This conclusion may therefore represent the line drawn in the sands of universal knowledge and provide the basis of current understanding of computer forensics from which research leading to improved education may commence.

III. Computer Forensics Education

Given the importance of computer forensics to the proper functioning of organization and society, it is essential that universities take on the responsibility for educating and preparing specialists in addressing these computer forensics issues.

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

At Curtin University, computer forensics is an essential module of the Masters Program in Internet Security Management. All Masters Programs in the School of Information Systems have been re-designed based on a common philosophy and an intellectual rationale. This paper will now address the common philosophy and the common framework of the programs before discussing the specific details of the computer forensics module.

IV. Philosophy of the Master Programs at Curtin University

All undergraduate and post graduate programs have undergone radical redesign to help them to be aligned to the School mission and the University vision. The latter is to be a World Class University while the School mission to achieve this through student development at intellectual, practical, professional and personal levels, i.e. holistic.

All Masters Programs have an underlying philosophy that should produce a graduate with a set of essential generic skills irrespective of any specialization. These generic skills are to help the graduate become a "problem solver" first, and a specialist domain expert second. Most Masters programs educate graduates with specialist skills to operate in the market place e.g. software engineer, computer scientist, data base administrator, security specialist. Whilst they help the person to become engaged immediately, they also create three kinds of problems. The graduates are locked into solution based skills and therefore have difficulties of understanding the 'real' problems of the end-users. Methodologies they learn have solutions and solution notions embedded in them that make it difficult to consider the real nature of problems. Jayaratna [8] defined these as "solution driven opportunity seeking methodologies." The second problem is that most specialists find it difficult to recognize the changes taking place in their own specialist field (e.g. languages, tools, technology, and roles) because they have mastered a set of skills which they are reluctant to sacrifice or master a new set of skills because of the time investment required. Thirdly, because of the changes in customer expectations and methods of transactions, products, etc., businesses require their employees to adapt to changes but more so become innovative in their approach to problem solving. Most specialists are reluctant to venture out of their specialist domain to tackle problems for which they have no answers. The aim of the Masters Programs of the School is therefore to produce a "problem solver" in the first instance that will be free to reach out to any tools, techniques, models, methods because they would be expected to perform as experts within a specialist field of operations. Thus the major philosophical shift for all Masters programs is to focus on the "problem-solving processes" which invariably means on the "problem solver" (knowledge and skills). To support this philosophy, all program structures have been changed to include generic skills modules as well as specialist skills modules and practical application of theory in the specialist area.

V. Generic Modules

These are modules that prepare a graduate to develop a set of generic knowledge and skills with which to undertake problem solving. The first module addresses advanced problem solving which is focused on the development of students' conceptual abilities, understanding of problem solving in conceptual terms, learning about the role of methodology in problem solving, learning to evaluate methodology practice and action research. For this undertaking, the module uses epistemological notions of systems, "Soft" Systems Methodology, and NIMSAD framework [8] [10] [11]. The second module addresses risk and project management. The aim of this module is to develop students' skills for managing projects, learning techniques and tools, understanding the role of the people in projects, learning how to evaluate cost/benefits and risks. The third module focuses on change management. The aim of the module is to develop interpersonal and behavioral skills of students to manage people and the effects of change including management of client-consultant relationships. The final generic module is research methods. Learning how to research a topic is to develop one's enquiring mind. Through this module a graduate learns how to conduct research into emerging and new topics and to integrate new knowledge with other specific knowledge areas. The four modules collectively develop the generic knowledge and skills in the graduate to undertake problem solving and the specialist skills are then developed using the generic skills as the foundation for learning. All modules are constructed using a standard template which is discussed below.

VI. Common Framework

The design of new curriculum in the School of Information Systems is aimed at achieving the University vision of becoming "World Class." Therefore the philosophy of education aims to shift focus of academic staff away from teaching to the development of the students. In order to integrate both teaching and learning strategies and to align the School mission and the University vision, a generic framework for a module was developed. As shown in Table 1, this Module Framework identifies several key components:

1. Module Objectives
2. Student Learning Outcomes

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

3. Syllabus in terms of knowledge, skills and competence
4. Assessment strategy

A. Framework Module Objectives

Module objectives help to understand the connection of each module to all other modules within a thematic subject area. They explain the academic rationale as to why a particular module is being taught within the curriculum. They also help to discuss why that module is included in a particular program, e.g. computer forensics in the Masters Program in Internet Security Management, The module objectives can be written in technical terms and focus on teaching perspective.

B. Framework Students Learning Outcomes

Student learning outcomes answer the students' questions as to "Why am I learning this module? What can I do with the acquired knowledge and skills?" Student learning outcomes of the module help students to make sense of the program and the role of the module in their learning. Since graduates have not yet undertaken the study of the module at this stage, the language in which the learning outcomes are expressed should be non-technical as far as possible to help them understand the rationale.

The curriculum model is based on the epistemological notions of "Systems" and therefore logically thought through. As a result, we have been able to reduce duplication or overlap of material, improve consistency and integrate the knowledge and skill areas learned. Both the module objectives and students learning outcomes are tightly connected to the School mission and the University vision.

C. Framework Syllabus

Syllabus content must demonstrate how the module objectives and the student learning outcomes can be realized. Equally, the syllabus content has to be organized under knowledge, skills and competence. All teaching should focus on a set of knowledge topics although only some of them will be taken to skills level. Skills are simply the demonstration of knowledge in practice while competence is measured by the depth/level of skills acquired. This partitioning helps to design topics that students should know, develop skills in, and the level to which they should demonstrate these skills.

D. Framework Assessment Strategy

The assessment strategies are based on the module objectives and the student learning outcomes and should show how knowledge, skills and competence can be measured to achieve the module objectives and the student learning outcomes. The assessment strategies can take many forms, e.g. examinations, written assignments, laboratory sessions, poster presentations, laboratory, classroom or external projects. The strategy should demonstrate the best way of measuring the module objectives and the student learning outcomes but at the same time be fun and challenging for the students. They should also focus on student's abstraction of lessons. In projects where the NIMSAD framework is used [8] [12] students must focus on lessons: from the situation; about the use of concepts, models, methods, techniques and methodology; as well as about themselves at three time periods – before, during and after intervention.

VII. Curtin University Computer Forensics Module

The rest of this paper will discuss the computer forensics module of the Master Program of Internet Security Management using the framework discussed above. In order to ensure the practicality of the module extensive consultations have been conducted with law enforcement, government and other academic bodies providing input to the design and delivery of the computer forensics module.

VIII. Computer Forensics Module Objectives and Syllabus

The purpose of this unit is to provide students with an introductory understanding of the principles of computer forensic techniques. It covers topics such as the identification, preservation, extraction and documentation of computer evidence using forensic techniques applied to computer related crime. The Unit is designed to develop students' awareness in each of these areas (as illustrated in Table 1).

A. Computer Forensics Module Objectives

At the end of this Module students should be able to:

- Understand the role of computer forensics examination and analysis principles as they apply to supporting crime investigations and prosecutions;
- Understand the impacts and implications to business of applying basic computer techniques and forensic principles;
- Have skills in the appropriate use of computer forensics software tools;
- Install and operate various operating systems
- Present Expert witness testimony

B. Student Learning Outcomes of the Module

At the end of this Module students should be able to –

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

- Become a contributing member of a computer forensics investigation team
- Assist in the formulation and implementation of a policy to accommodate corporate computer forensics requirements
- Significantly contribute to corporate due diligence and governance processes
- Instigate an investigation and know at which point in time to invite and pass investigation to law enforcement agency personnel
- Use the computer forensics tools and techniques to capture an image, find and analyze and maintain the integrity of the chain of evidence, and report finding in an adversarial environment

IX. Pedagogical Process

The pedagogical process is aligned with the School Mission of student development. In according to the new curriculum framework, see Table 1, the intellectual level of development consists of knowledge, skills, and competence. It is very important that the lectures do not become simply information providing sessions. Lectures therefore are focused on engaging the students and thereby form the knowledge component. Skills are simply the demonstration of knowledge in practice. Tutorial and laboratory sessions are focused on student's skills development. Competence is defined here as attainment of skills as determined by industry requirements in a selected set of skill areas. While topics listed under skills ensure students are able to demonstrate knowledge in practice, the topics under the competence column, see Table 1, demonstrate the syllabus content in which students have to reach a high level of skills. Using Sprenger's [13] multiple tracks to the brain and memory, action learning and reflection, students engage in practical exercises where computer forensics tools are used to capture, copy and analyze digital data so that the students gain an appreciation of the physical requirements of undertaking a computer forensics investigation.

Professional development of students is achieved by student's verbal and written presentation of their practical work in a simulated adversarial environment. Currently, Curtin University academic staff are working closely with a number of law enforcement agencies on joint research projects and teaching programs. Students will investigate criminal cases taken from the public domain supported by evidence from enforcement agencies. They are required to work as members of a team (learning to handle conflicts to achieve collaboration) as well as compete as teams in adversarial environment or context. In both they are expected to develop their professional skills.

Personal development is achieved by setting students topic areas and practical work where they have to use their own initiative and mental structuring of activities. They are required to demonstrate why they followed a particular line of reasoning thus helping both their personal as well as intellectual development.

A. Syllabus

The content material of the course is an extension of the syllabus as shown in Table 1. To form a foundation for this module, students examine and discuss forensic principles and methods to gain an understanding of the relationships with international guidelines, practices and ethics of forensic computing. Students are presented with the technical environment early in the module and are guided into the behind-the-scene activities deep within a computer system. Students understand the need for a comprehensive understanding of how a computer system functions but not always appreciate that there are considerable differences between being a competent computer user and being able to explain such concepts as binary, addressing, numbering systems and file types, formats, and structures to a formal hearing.

The adopted teaching approach focuses on assisting students develop their skills and knowledge to maintain credibility as an expert, especially in regard to addressing a formal hearing. While students in this module may have considered themselves well versed in technical aspects of computing, none had previously disassembled a hard disk drive to examine its inner workings before doing so in class.

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

Knowledge [α]	Skills [β]	Competence [δ]
Seminar	Laboratory Tutorial	Laboratory Tutorial
Computing Technology		
Introduction to Computer Forensics Principles and Methods	Computing basics, binary system, addressing and numbering systems	
International Guidelines, Practices and Ethics	*International Guidelines, Practices and Ethics* [δ] Installing Operating Systems; Linux, M/S	Installing Operating Systems; Linux, M/S
Computing Technologies Hardware and Software	File types, signatures and formats, structures, architectures, platforms and Hexadecimal	File types, signatures and formats, structures, architectures, platforms and Hexadecimal
Op Sys and File Structures and Tools and Concepts	Linux Forensics tools	
Investigative Techniques		
Investigation Techniques	*Investigation Techniques* [δ] Visit - W.A. Police	
Evidence Principles and Dynamics	Computer Investigation	
Principles and Tools for Data recovery, evidence, image	Data recovery, evidence	
Data recovery, evidence, image	Computer image verification and authentication	Computer image verification and authentication
Jurisprudence		
Jurisprudence	*Jurisprudence* [δ] Evidence Integrity	Evidence Integrity
Legal Perspectives and Court Proceedings	Report Preparation	Report Preparation
Law and Role of Expert Witness	Submitting to Court Examination	
Review Unit and Exam preparation	Mock Court	Mock Court

Symbol index for the above table;
- [α] Intellectual development
- [β] Practical development
- [θ] Professional development
- [δ] Personal development

Table 1: Knowledge, Skills and Competencies

From this technical foundation, students next engaged in the techniques that would enable them to actively contribute to an investigation. The teaching approach adopted encouraged team efforts and instilled the realization that while individual expertise is essential, team work will provide better chances of a successful prosecution should an investigation warrant so. The module concludes addressing jurisprudence issues where the focus once again concentrates on the ability of the individual to communicate their findings in a manner that retains their credibility, integrity and lead to successfully prosecuting a case.

Securing a law enforcement computer forensic practitioner to assist in presenting class exercises proved beneficial to teaching this module. As a Detective Senior Constable, this practitioner provided first hand knowledge and experience of all aspects covered in the module. Finally, students were invited to visit University of Western Australia moot court sessions where Forensic Science students were assessed on their Courtroom expert testimony presentations.

B. Assessment Strategy

A range of assessment strategies are adopted to ensure the achievement of module objectives and the student learning outcomes. These are intended to measure intellectual, practical, professional, and personal aspects of development. In order to achieve this objective, continuous assessment testing is combined with time for students to reflect on their individual learning and is culminated with an end of semester examination. Interesting and realistic performance evaluations are conducted on scenario case studies based on past criminal cases taken from the public domain. In addition, mock court sessions are used to bring the intellectual, practical, professional and personal components together. By engaging practicing law enforcement and judiciary officials, students are afforded and opportunity to perform and learn within a safe but realistic environment.

Time limitations prohibit opportunities for students to conduct a comprehensive computer crime investigation and then to present their findings in a formal, adversarial setting. As this is seen as a highly desirable component of the module, students undertake snapshot tasks of this holistic endeavor. Future development of the module will address this issue and the intended assessment will not focus on how well a student presents expert testimony, but rather on their personal reflections gained from the experience.

X. CONCLUSION

Computer systems are increasingly being exploited and linked to digital crime. As a consequence there is a corresponding increase in demand for computer forensics practitioners and digital forensics skills.

The cross-disciplinary nature of computer forensics is significant, requiring the linkage between investigatory techniques, computing technologies and jurisprudence. Britz [14] suggests that “it is essential that the potentiality of computer-related crime and the insidious nature of the phenomenon be recognized and addressed by all sectors of the community”. There is an important role for academia in both research to assist computer forensics practitioners, and in educating and preparing future computer forensics specialists.

Computer forensics is an emerging area and the currency of the subject will be dependant on involving industry and government agency’s practitioners, and collegial cooperation in research across universities, departments and jurisdictions.

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

XI. REFERENCES

[1] Casey, E., 2000, *Digital Evidence and Computer Crime: Forensic Science and the Internet*, Academic Press, London, UK

[2] Icove, D., Seger, D. and VonStorch, W., 1995, *Computer Crime: A Crimefighter's Handbook*, O'Reilly and Associates, CA, USA

[3] Bologna, G. J. and Lindquist, R. J., 1995, *Fraud Auditing and Forensic Accounting* (Second Edition). New York, John Wiley and Sons, Inc.

[4] Kruse, W. G. and Heiser, J. G. , 2001, *Computer Forensics. Incident Response Essentials*. Boston, Addison-Wesley.

[5] Vacca, J.R., 2002, *Computer Forensics: Computer Crime Scene Investigation*, Charles River Media, Hingham, Massachusetts, USA

[6] Barbin, D. and Patzakis, J., 2002, Computer Forensics Emerges as an Integral Component of an Enterprise Information Assurance Program, *Information Systems Control Journal*, Volume 3.

[7] Smith, F. C. and Bace, R. G. 2003, *A Guide to Forensic Testimony. The Art and Practice of Presenting Testimony as an Expert Technical Witness*, Addison-Wesley, Boston.

[8] Jayaratna, N. 1999, *Understanding and Evaluating Methodologies. NIMSAD : A Systemic Framework*, McGraw-Hill Book Company, Maidenhead.

[9] Hatcher, T., 2001, *Survey: Costs of Computer Security Breaches Soar*, CNN.com, Available on-line at : http://www.cnn.com/2001/TECH/internet/-3/12/csi.fbi.hacking.report/index.html . (12 03 2001)

[10] Checkland, P. B. 1999. *Systems Thinking, Systems Practice*, Wiley and Sons, London

[11] Checkland and Scholes, 1999, *Soft Systems Methodology in Action*, Wiley and Sons, London

[12] Kawalek, J.P. and Jayaratna, N. , 2003, *Evaluating 'Interpretive' Information Systems Research*, in Benchmarking an International Journal, 10, 4, p.400-413.

[13] Sprenger, M. 1999. *Learning and Memory: the Brain in Action*. ASCD, VA, USA.

[14] Britz, M.T., 2004, *Computer Forensics and Cyber Crime*, Pearson Prentice Hall, New Jersey

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE