Proceedings of the 10th Colloquium for Information Systems Security Education
University of Maryland, University College
Adelphi, MD June 5-8, 2006

Forensic Computing: Developing Specialist Expertise within the CS Curriculum

Jason Beckett[1, 2], Jill Slay[2] and Benjamin Turnbull[2]

Abstract — This paper responds to the need to understand the nature of forensic computing and the roles that are involved in the discipline. It defines the nature of the field and the roles and qualifications of the forensic computing practitioners who serve in the filed. It emphasizes the role of the specialist and the need for the development a tertiary curriculum which produces graduates who are able to take up entry-level graduate positions in Law Enforcement and government.

Index Terms— Forensic Computing, Digital evidence, certification, expert evidence, CS Curriculum

I. INTRODUCTION: WHAT IS FORENSIC COMPUTING?

Forensic computing has mostly developed out of a demand for service from the law enforcement community [2] and has since developed into a discipline that crosses the corporate, academic, scientific as well as the law enforcement domains. The establishment of the field of forensic computing as a true science (in the sphere of the forensic sciences) is a process that is still in development and still lacks a cohesive set of standards and competencies.

There have been numerous papers that have tried to define forensic computing or digital forensics (McKemmish 1999, Kruse & Heiser 2002, Casey 2004, Civie & Civie 1998, Hannan 2004) and without discussing the merits or deficiencies of each definition (each is worthy of a treatise of their own) it is suffice to say that each ultimately discuss the need to preserve, process and present evidence for the courts. The commonality between each definition is the use of the word forensic.

The word forensic has been well defined and its origins go back to ancient times, but in more recent times it has been used to describe any professional practice that provides scientific knowledge to the 'trier of fact'. The following definition is commonly used;

> *"forensic comes from the Latin word forensis: public; to the forum or public discussion; argumentative, rhetorical, belonging to debate or discussion. From there it is a small step to the modern definition of forensic as belonging to, used in or suitable to courts of judicature, or to public discussion or debate. Forensic science is science used in public, in a court or in the justice system. Any science, used for the purposes of the law, is a forensic science."[3]*

Examples of disciplines that have been classed as 'forensic' include Medicine, Biology, Chemistry, Pathology, Psychology, Firearms-Ballistics, Handwriting, Accountancy and Photography to just name a few.

This established definition of forensic and forensic science and the examples of forensic disciplines demonstrate that the forensic computing discipline is more than just examining data and electronic devices, it has a purpose and that purpose is the pursuit of judicial process. In the forensic computing world the use of the word forensic is predominantly used to describe some of the processes, for example forensic copy and forensic examination when really it should be used to describe the goal for the process. Each of the attempts at defining forensic computing or digital forensics only briefly describe a need to present or produce for the court, that is, providing the results of examinations and analysis to this judicial process. This requirement for judicial process sets the scene for the need to define what is required to give evidence and in particular expert evidence. All the forensic computing definitions discuss this presentation phase but few apply the appropriateness of qualifications and experience to this need and the validity of practitioners providing the evidence.

II. EXPERTS & EXPERT EVIDENCE

One of the main characteristics of the law relating to expert evidence has been "the preparedness on the part of judges to refuse witnesses the right to give evidence as experts if their qualifications are not relevant and sufficient" [4] and in many countries specific case law and binding decisions have been made that effect the need for relevant qualifications in expert evidence. For example

[1] *Director of Electronic Evidence, New South Wales Police, Sydney Australia. Beck1jas@police.nsw.gov.au*
[2] *Enterprise Security Management Lab, School of Computer and Information Science, University of South Australia, MAWSON LAKES, SA5095. AUSTRALIA*
Phone: +61 8 83023840. jill.slay@unisa.edu.au

Frye v United States (1923) called the Frye Test and the Daubert v Merrell Dow Pharmaceuticals (1993) in the United States commonly called the Daubert Test have dictated how novel scientific evidence is presented to courts. More recently Rule 702 of the Federal Rules of Evidence in the United States were amended on 17th April, 2000 and which came into force on the 1st December 2000 stated that *"If scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise, if (1) the testimony is based upon sufficient facts or data, (2) the testimony is the product of reliable principles and methods, and (3) the witness has applied the principles and methods reliably to the facts of the case."*.

There are many examples throughout the world where similar stances are now being taken and in Australia Justice Dixon stated in Clark v Ryan (1960) that "experts could not testify in areas which were not part of a formal sphere of knowledge". These examples have been called the 'expertise test'. Without going into too much depth in discussing the merits of the expertise test as it has been discussed and debated widely [4] it is suffice to say there is an established need to ensure the expert giving evidence is qualified to express an opinion and can present articulated and valid evidence to a court of law.

With this understanding of expert evidence a number of questions then arise ;

- Is a certification in forensic computing evidence of "knowledge, skills, training, education or experience"? And,
- Does the preponderance of "point and click" forensic courses constitute the same "knowledge, skills, training, education or experience" and therefore class a practitioner as an expert?

Meyers and Rogers [6] raise a number of issues in relation to this, stating:

"In order for the field of computer forensics to mature, there must be a national system for certifying individuals who claim to be professionals. The continued lack of a professional certification, investigative standards, and peer reviewed method, may ultimately result in computer forensics being relegated to a "junk science," as opposed to a recognized scientific discipline." [6]

In order for the Forensic Computing discipline to address this issue there is a need to classify the various roles involved in any forensic computing investigation and then methods need to be constructed whereby professional certifications can be established and career pathways developed within the industry

III. Categorization Of ROLES

A model for the distinction of specific skills, qualifications and capabilities for Forensic Computing roles was proposed in draft format by the International Organization on Computer Evidence [5], but no public evidence could be found that this has been further developed nor finalized by this organization.

The IOCE identified 2 levels of competence, that of technician and analyst. The Scientific Working Group on Digital Evidence [6] details a similar breakdown but further introduces the role of incident responder.

The model being proposed here and in previous work [1], puts the role of the specialist into its own category, but still allows the analyst or technician level to have a depth of capability that will allow work to progress and offer "evidence of fact" as opposed to "expert evidence".

The reason for choosing this alteration of the models is to reflect the growth in the need for forensic examinations and specifically clarify the role of practitioners. Although anecdotal (a formal study is in progress), the experience of the first author's laboratory is that a majority of evidence only requires basic triage, that is, investigators looking for a specific item, such as a single document or file or the production of a file level copy and does not require specific forensic analysis such as a temporal analysis or data recovery that may require far greater specialist skills.

To investigate further a suitable model a look at the more established profession of medicine may allow certain comparisons to be formed between these two fields. Both require triage, diagnosis and management and expert opinion of cases bought before them. In medicine there are a complete range of broad job categorizations:

- first aid responder,
    - providing initial triage of a victim, they generally have completed a certification or authorized course and usually attend to the initial response of any incident and offer very basic management of an injury.
- nurse,
    - provides a greater initial triage and is able to apply more skills and experience in the management of a victim and is typically educated through some level of tertiary education and undergoes a registration process for them to operation in hospitals and certifications in the different functions they perform.
- doctor (general practitioner)

  - provides diagnosis beyond triage and a broad range of tests, and is always degree qualified and is also required to be registered to perform work.

- specialist (expert).
  - Work is always referred on by doctor and he/she provides expert opinions through knowledge, experience and testing based on extensive qualification and deep specialization in one area of medicine.

The forensic computing discipline has functional similarities, those of initial response, triage, diagnosis and specialist expert. To keep in line with current models such as SWGDE and IOCE the following categorizations and terminology for forensic computing are proposed;

- Initial Responder
- Technician
- Analyst
- Specialist

A. Initial Responder

This level of the framework is designed for street level investigators in law enforcement or investigators in corporate organizations, that is, the initial responders or staff who routinely investigate any incident that may have a computer or electronic component. This level would look at sources of electronic evidence, electronic evidence identification, basic evidence collection and use of electronic evidence in investigations. This level of development exactly aligns with the skill level proposed by the SWGDE.

The incident responder stage would not allow an investigator to process evidence of data in motion, but more data at rest. It would allow the investigator to understand that evidence may exist and that there are practitioners and specialists that can process the evidence. This stage could potentially allow minimal certification in evidentiary identification and collection of electronic evidence.

B. Technician

The technician stage of development is the initial processing of evidence and basic examination of the evidence, including preservation. Technician level capabilities would allow an examiner to give "evidence of fact" to a judicial process. This stage differs from the SWGDE model in that basic examination beyond just collection and preservation to basic examination, such as keyword searching, file copying.

This development phase would allow for triage of the data to the extent that evidence could be presented by the technician at court of the existence of data, the verification of chain of custody (preservation of data) and the lay description of files found (it is a word document, it is a JPEG image, etc).

The qualifications being proposed include certifications, and vendor specific course, but the underpinning knowledge and skill coming from a diploma level qualification. The experience level would range from 1 to 2 years, for practical autonomous operations in addition to the qualifications.

C. Analyst

The analyst stage of development is the most broadly trained and skilled level of practitioner. This stage of the model includes staff trained to move from the basic evidence of fact to that of opinion and validation evidence. The Analyst would also be able to handle the bulk of the diagnosis work in an examination. It includes the complete examination, analysis and recovery of digital evidence and the offering of evidence beyond that of fact, including the results of testing, observations, and opinions within the scope of their expertise. This does not mean a person deemed an Analyst would essentially be able to offer opinions on all areas of the field, but specific evidence on their area of specialization or training, making this the broadest area of the development phase.

The analyst would be the examiner with the broadest level of skills across the discipline, while the specialist would be the expert in the true essence of the word, that is, the expert in a specific aspect of the discipline. The qualifications for this level of practitioner would require a bachelors degree, heavy vendor training and industry certification but a depth of experience greater than 4 years.

D. Specialist

The specialist would typically be drawn from academia, vendors, researchers, and not necessarily the forensic laboratory that initially conducted the examination. The specialist expert would typically be a person with specific skills, knowledge on a specific topic and may not necessarily be an analyst. The specialist's role would be to offer in depth perspectives and opinions on a particular component of an investigation or examination. The specialist would not normally be specialized in all areas of the forensic process, but concentrated on a particular skill, piece of equipment or sphere of knowledge. The specialist may be a particular vendor familiar with their software, or an academic with a particular research background or even an analyst with extensive experience with a particular examination.

The typical specialist may have numerous formal qualifications and extensive research experience. It is possible for an expert to just have extensive knowledge

about a particular subject domain but a judicial decision would be the determinant for this exception.

IV. Developing Specialist forensic Computing Expertise in the CS Curriculum: case Study

The role of the university in the development of forensic computing specialists is a very new one and those who are being to work in this area are starting by developing coursework at Masters or Honours level which builds on to an undergraduate major in computer science or engineering.

At the University of South Australia we have had strong support from 2 Australian State Police Forces and have developed a course which will produce foundational knowledge. By encouraging students to take a major thesis (or major project dependent on their program) we are then able to support the graduate student in the development of higher level knowledge and skills in forensic computing. This does not automatically produce the specialist expertise described above but does lay the foundational knowledge in 'what is forensic computing?".

A. Course Content

The aim of our course ***Forensic Computing: Tools and Techniques*** is to:

- understand the role of the investigator in the investigation of criminal, illegal and inappropriate digital behaviour,
- understand the principles of responding to incidents and computer crime,
- identify types of inappropriate use of computer systems,
- show an understanding of investigation and evidence collection,
- demonstrate the principles of evidence handling,
- understand and demonstrate basic Forensic Computing Investigative procedure,
- understand legislative, case law and additional guidelines governing the Forensic Computing Investigation process,
- identify inappropriate use of computer systems ,
- demonstrate the principles of data collection from Windows and Unix based systems ,
- appreciate basic issues in collecting network based evidence,
- understand and demonstrate use of components of basic computer forensics toolkit and
- understand and demonstrate the use of components of basic network forensic tool kit.

Our syllabus includes

- Forensic Computing Investigations.
- Legal issues of investigation.
- Crime scene management.
- Case management.
- Evidence presentation.
- Data storage and media;
- Data acquisition;
- Data collection from Windows systems.
- Data collection from Unix systems.
- Collecting network based evidence.
- Tools: Encase, @Stake Sleuth Kit, Coroners Tool Kit, Autopsy
- Forensic Computing research

The course was developed with the assistance of members of the South Australian E-Crime lab and New South Wales Electronic Evidence Branch and draws on some guest lecturing form forensic computing practitioners

Coupled with substantial honours and Masters theses and projects such as:

- examination of the use of ontologies to speed up the search of electronic evidence,
- a standard operating procedure for iPod forensics
- evaluation of mobile phone 'forensic' software to determine if truly forensic in nature
- development of 'zero-skills' forensic software for law enforcement

which are researched with the support of our Law Enforcement partners who act as 'client' and mentor, we can then begin to produce skills and expertise which are of use to Law Enforcement, as training which will eventually produce experts and expert witnesses and skills which also are very applicable to the wider ICT industry.

B. Defining graduateness

The aim of our course development process is one which is intrinsic to the University of South Australia and we teach in a manner so as to develop 'graduateness' which underpins any claims to expertise.

In seeking to provide a high quality learning environment that will prepare its students for life long learning, the University of South Australia [7], among others working in this field, has defined a series of generic learning outcomes that it desires to produce in its graduates. These can then act as measures of graduateness.

These include:

1. the ability to operate with and upon a body of knowledge of sufficient depth to begin professional practice

2. preparation for lifelong learning in pursuit of ongoing personal development and excellence in their professional practice
3. effective problem solvers, capable of applying logical, critical and creative thinking to a range of problems
4. commitment to ethical action and social responsibility as a professional and a citizen
5. the ability to work autonomously and collaboratively
6. effective communication skills
7. demonstration of an international perspective as a professional and as a citizen.

These infer that while the first graduate quality, the body of knowledge, is of primary importance, the method in which this knowledge is gained and applied is of equal importance and in fact to some degree defines graduateness. All assessment pieces define which graduate qualities are being developed; if group skills are desired then group assignments which develop research skills in an Forensic Computing context are used. If individual report writing and information literacy skills are required then individual reports are requested. Students have to be taught, or are asked to review, report writing, information literacy or group skills simultaneously with the development of the body of knowledge in the required area.

In ***Forensic Computing: Tools and Techniques*** we have chosen to focus on the third and fourth graduate qualities so that we teach ethical problem solving in the context of forensic computing investigations

C. Challenges to Academia

The second and third authors must first state that in our own professional development we are indebted to Australian Law Enforcement, particularly to the South Australian E-Crime lab and New South Wales Electronic Evidence Branch.

We have found it fairly routine to teach computer architecture and operating systems in a forensic computing context

The challenges to us as academics with personal strengths in IT Security and IA teaching and research are basically those of constructing realistic crime scenarios and in producing electronic evidence for the large numbers of students who do wish to develop expertise in this field

The second and third authors have found that the following is a helpful guide in teaching and also in developing realistic assessment in Forensic Computing which challenges and extends a good student and prepares him or her for a graduate position in the forensic computing field (the first step on the path to 'specialist')

It is important for the student to understand that digital evidence can come from, amongst other things:

- Computers
- Laptops
- Skype handsets
- Ipods (etc etc)
- Mobile Phones

Digital evidence comes in three forms

- User-created information (emails, documents, spreadsheets, digital images) – anything made by the users themselves.
- Machine created information (log files, registry information, page files) – any file made by the machine of device automatically (usually without the user's knowledge)
- A combination of the two (chat logs, internet history, etc) – files automatically saved by the machine, but made up of both user input and machine information.

When searching for digital evidence, each of these provides different information and the focus depends on the case or what is intended.

- User-created documents are useful in fraud, child image abuse, forensic accounting and other investigations where you are trying to prove facts within these files.
- Machine-created information will allow investigators to understand a sequence of events (which user logged in at which time and for how long, what they did on their computers during this time, and what files were altered). This may give a timeline of events.

MAC Times – Modified, Altered, Created. These are based entirely on the PC clock, and are not infallible. MAC times are associated with every file on a PC.

1) Making Evidence for Teaching Purposes

You are now entering the shadowy world of Anti-Forensics, where you are actively making information that is not correct. Here we discuss changing some user-information and combination-information since changing log files is more difficult.

a) Timeline your events

Personal experience suggests making a timeline of events for each event, and then find out

- What files and information is created for each event

- Where each piece of information is stored
- The MAC for each file

b) Check the Time

The first stage is to ensure that your PC clock (Windows, Macintosh, whatever) is set to the time you wish to use it. If you are planning on making a file that was apparently created on a certain date and modified on another date, change your computer clock to the first time, make the file, and then move to the second time and edit it.

c) Making Evidence - text and word processing files

There are several text file formats you can use, and several ways of creating a text document (using Notepad, Wordpad, Microsoft Word, OpenOffice, PDF, to name a few).
Office files can be stored anywhere on a hard disk, but in a Windows XP environment are most likely stored in c:\Documents and Settings\<username>\My Documents (where <username> is a computer user on the system)
Be careful with Microsoft-formatted documents – these files will have the author's name embedded into them. To remove this, open the document, and then access **File > Properties > Summary** and delete the author information.

Adobe PDF files also embed author information. This is more difficult to remove, and it may be worth using a hex editor. OpenOffice files are actually zip files containing xml files, which can be edited by hand if desired. The easiest way to make these files is to install a package and make sure the author's name matches what you wish it to be.

d) Making Evidence - chat logs

This section will discuss the format of MSN Messenger logs and how to create and edit them. You may use other log files, but these are the simplest to manipulate.
MSN Messenger log files are stored in XML format. XML is actually two documents – one with the data and one to control the format.
Image 1 is what the formatted version of the chat log looks like and below this is two messages saying hi.

15/11/2005	2:07:24 PM	Ben	TT	see you at 5:10
15/11/2005	2:08:06 PM	TT	Ben	**hahaha**
15/11/2005	2:08:06 PM	TT	Ben	**we'll do**
15/11/2005	2:09:17 PM	Ben	TT	ok, see you then
2/12/2005	2:44:47 PM	TT	Ben	Hellooooooo
2/12/2005	2:45:19 PM	Ben	TT	ni how!
2/12/2005	2:45:50 PM	TT	Ben	:D
2/12/2005	2:46:32 PM	TT	Ben	how's it going?
2/12/2005	2:47:23 PM	Ben	TT	good good. yi chi is [illegible] how are you?
2/12/2005	2:47:55 PM	TT	Ben	tickety boo
2/12/2005	2:48:47 PM	TT	Ben	are you busy recently?
2/12/2005	2:49:15 PM	Ben	TT	i was, but I'm not [illegible]
2/12/2005	2:50:53 PM	TT	Ben	good to hear

Figure 1 – formatted MSN Messenger log

```
<Log FirstSessionID="1" LastSessionID="2">
<Message Date="15/11/2005" Time="2:00:45 PM"
DateTime="2005-11-15T03:30:45.888Z" SessionID="1">
<From><User FriendlyName="Ben"/></From>
<To><User FriendlyName="TT"/></To>
<Text Style="font-family:MS Shell Dlg; color:#000000;
">hi TT</Text>
</Message>
<Message Date="15/11/2005" Time="2:00:57 PM"
DateTime="2005-11-15T03:30:57.473Z" SessionID="1">
<From><User FriendlyName="TT"/></From>
<To><User FriendlyName="Ben"/></To><Text
Style="font-family:Microsoft Sans Serif; font-weight:bold;
color:#800000; ">hi Ben</Text>
</Message>
```

To create MSN Messenger logs, the easiest thing to do is read any existing ones you can find. MSN Logs are by default stored at C:\Documents and Settings\<username>\My Received Files\<MSN Login name and unique ID (for example plummy_plum1947392856)>\History each file is named after the user being conversed with (for example kitty_mel19822710761105.xml)

The session ID tags refer to the conversation. The first tag says how many conversations there are, and the tag within each message is which session the message is part of. The rest lf the format is self explanatory, except be sure to ensure that the times are correct in both sections, as otherwise the ordering will be incorrect.

To make an MSN message log, either set up MSN Messenger on two or more machines and have conversations, or manually edit these files.

e) Making Evidence - email

This section will discuss making emails that appear to have been sent.

The easiest method to forge an email that appears to have been sent, the simplest method is to actually send it! If you are fortunate enough to have a home ISP that allows you to make several email accounts, it is simple to set these up to email between each other. If not, there are methods to make it appear as if an email has been sent when it has been not. This will discuss the Microsoft Outlook Express email system, but if you use something else, this may still work.
Open outlook, set up the account, and write the email. Then, drag it into the sent items. You can also do this for received emails. All user-data will suggest that this email has been sent and received.

Please note that this is only forensically sound for user-data, and is not forensically sound

f) Making Evidence – digital images

If you intend to make digital photos created at a specific time and place, be sure to check your digital camera's internal data and time. Your digital camera stores more than just the photograph, including make and model of camera, date and time of camera image, exposure length, and whether a flash was used. If you use Photoshop or other programs to make or alter images, this too will be discovered.

g) Making Evidence – internet history

Internet history storage depends on the browser you use, but the only feasible method to make a history is by actually browsing.

Internet Explorer stores internet history at C:\Documents and Settings\<username>\Local Settings\History and C:\Documents and Settings\<username>\Local Settings\Temporary Internet Files

V. Conclusion

There is much work to be done in progressing the forensic computing discipline, it is maturing at an exponential rate. This paper presents one attempt at collaboration with Law Enforcement to develop specialist skills in Forensic Computing. Our context is one where ethics and problem solving within the domain provide a primary focus for the development of graduateness in the potential Forensic Computing specialist.

VI. References

[1] Beckett, J. (2005) *Forensic Computing: Experts, Certifications and the Categorization of Roles*, CISSE-AP, Adelaide, November 2005

[2] Noblett M, Pollitt M, & Presley L. (2000) *Recovering and examining computer forensic evidence,* Forensic Science Communications US Department of Justice Federal Bureau of Investigation Volume 2 Number 4.

[3] AAFS. (1996) "*What is Forensic Science?*", [online], American Academy of Forensic Sciences, http://www.aafs.org/.

[4] Freckelton I, Selby H. (2005), "*Expert Evidence Law, Practice, Procedure, and Advocacy"* Third Edition, Pg 44, Pg 85.

[5] International Organization on Computer Evidence (2002), *"Training and KSAs",* DRAFT V1.0 workshop proceedings www.ioce.org .

[6] Scientific Working Group on Digital Evidence and Imaging Technology, (2004) "*SWGDE/SWGIT Guidelines & Recommendations for Training in Digital & Multimedia Evidence"* Version 1.0

[7] University of South Australia. 1996. *Guide to implementing the qualities of a University of South Australia graduate in course and subject development*. Unpublished internal paper.

[8]