Digital Evidence 2008
26-27 June 2008

Certification, Registration and Education of Digital Forensic Experts

Peter Sommer
London School of Economics
peter@pmsommer.com
p.m.sommer@lse.ac.uk
Digital Evidence Expertise

- Computer Forensics has been a discipline since the late 1980s
- How do you select and assess potential experts?
Overview

- What sort of expert do you need?
- Confusion of Qualifications, Registration Schemes, Degrees and Courses
- What sort of qualifications?
- Trends in Education
- Registration / Assessment Schemes
The problem:

- The tests used to grant qualifications and certifications of various kind may not be closely related to the tests you need to apply to assess whether someone will fulfil your specific forensic needs.
How to Select an Expert

• What do want an expert for?
• How do you assess from the marketplace?

You don’t necessarily always need “the best” – you want someone appropriate to your needs
What do want an expert for?

• To carry out or assist in an investigation
  ➔ Locate digital evidence
  ➔ Preserve evidence
  ➔ Conduct a forensic examination
  ➔ Produce exhibits which are admissible
  ➔ Execute a civil search order / warrant
What do want an expert for?

• To provide litigation support
  ➔ Manage digital material so that lawyers can handle
  ➔ Prepare exhibits
  ➔ Manage disclosure
What do want an expert for?

- To provide expert testimony
  - Knowledge of legal procedures
  - Knowledge of role of expert witness
  - CV which supports claimed “expertise”
What do want an expert for?

- (Defence) To advise on expert evidence tendered by others
  - Manage technical evidence so that lawyers can manage
  - Verify and test exhibits
  - Manage disclosure / criticise inadequacy of disclosure
What do want an expert for?

To design, or evaluate a Forensic Readiness Program

➢ So that the organisation can, on demand, produce reliable evidence in a cost-effective and timely manner

➢ To minimise panic
What do want an expert for?

• (Judge) To ascertain the qualifications of a witness offering opinion and background evidence
  → To ensure that the court (and a lay jury) is assisted but not over-influenced
Scope of Expertise

• Technical Environments
  ➔ PCs    Macs, Linux
  ➔ Minis, Mainframes
  ➔ Small Business Systems - LANs
  ➔ Internet, Internet browsers, Web-servers
  ➔ Emails
  ➔ Email servers
Scope of Expertise

• Technical Environments
  ➔ E-Commerce
  ➔ Peer-to-Peer File Sharing Services
  ➔ Social Networking
  ➔ Instant Messaging, Chat Rooms etc
  ➔ Particular commercial environments
    • Banking, Travel, Manufacture, Retail etc etc
  ➔ PDAs, Cellphones,
  ➔ Particular hardware
    • Terminals, Swipe cards, RFID, weighing and counting machines, burglar alarms etc etc
Scope of Expertise

• Skills
  → Evidence Identification and Preservation
  → Data Recovery
  → (Instant Response)
  → Evidence Analysis
  → Systems Analysis
    • Relating computers and telecommunications to business processes
Scope of Expertise

• Skills
  ➔ Investigations
    • How creative / How much of a self-starter / How far to stray from instructions?
  ➔ Good inter-personal relations
  ➔ Lawyer- and Lay-orientated explanations
  ➔ Report writing
  ➔ Oral testimony (the witness box)
Finding Your Expert
Expert Witness Directories

• **Widely distributed to lawyers**
• **Who runs?**
  → Law Society
  → Specialist entity/society
  → Legal Publisher
  → Directory Publisher
• **What acceptance criteria?**
• **What vetting procedures?**
• **How frequent the renewal process?**
Qualifications

• A few years ago... no qualifications or certification schemes

• Now... a huge and confusing proliferation

• Still very difficult for those who wish to assess expertise....
Qualifications

- University degrees
- Membership of professional bodies
- Other post-nominals
- Training Schemes - commercial
- Certification Schemes
- Registration / Assessment Schemes
- Directories of Experts
- (Recommendations)
Post-nominals

- CISA
- CISSP
- CFCE and Certified Electronic Evidence Collection Specialist Certification (CEECS)
- Certified Information Systems Auditor (ISACA - Information Systems Audit and Control Association)
- Certified Information Systems Security Professional - ISC²
- Certified Forensic Computer Examiner – IACIS (International Association of Computer Investigative Specialists) – 2 weeks + correspondence course
Post-nominals

- CFC
  - Certified Forensic Consultant – American College of Forensic Examiners

- CCE
  - Certified Computer Examiner – International Society of Forensic Computer Examiners

- CIFI
  - Certified Information Forensics Investigator - International Information Systems Forensics Association

- CEE
  - Certified Computer Examiner (commercial)
Post-nominals

- **EnCE**
  - EnCase Certified Examiner – 64 days + written & practical exam
- **ACE**
  - Access Data Certified Examiner
- **CFIP / CFIA**
  - Certified Forensic Investigation Professional – 2 days from 7Safe. CFIP+: university assessed
- **GCFA**
  - Global Information Assurance Conference Certified Forensics Analyst
Post-nominals – Professional Bodies

These have charters, codes of ethics, vetted membership etc

But none specific to digital evidence.

• MBCS / FBCS: British Computer Society
• AAFS: American Academy of Forensic Sciences
Post-nominals – University Degrees

- BSc (Hons)
- MSc
- PhD
- DPhil
- MA (Oxon)
- PGCert

But in what subjects, on what syllabus, and how long ago? How “good” is the university?
University Degrees

• Measure student at time of course
• Measure according to academic criteria
  ➔ Notions of generally expected and accepted standards
• What award?
  ➔ Undergraduate, Master’s, Doctoral, Diploma, Certificate, Post Graduate Certificate
• What course?
University Degrees

What course?

• Syllabus?
  ➔ Relevance
  ➔ Teaching quality
  ➔ Up to date

• Practical experience for students / facilities

• Course Teachers and their experience
  ➔ How many are active practitioners?

• University courses and “bums on seats”
Registration / Assessment Schemes

- Aim is to assess against published criteria
- Usually an evaluation of relevant qualifications
- Case-work
- Codes of Ethics
- There are no courses directly linked
- UK CRFP and US DFCB
Registration / Assessment Schemes

- Who sponsors?
- Who assesses?
- What is being assessed?
  - Competence
  - Excellence
  - Specific areas or general abilities
- What precise criteria?
- Currency of assessed competence
- Frequency of re-assessment
- Who assesses the assessors?
Registration / Assessment
Schemes: Dangers

• Groups of friends who validate each other
• More limited in scope than is first apparent
• Registration is for life, but the subject area keeps changing
UK Scheme: CRFP

- Council for the Registration of Forensic Practitioners
- 1999: set up by UK Home Office after a number of concerns about the reliability of forensic science expertise
- Emphasis on crime and family/child issues
CRFP Computer Speciality

Three Grades

• **Data Capture**
  ➔ Correct preservation / imaging of data media

• **Data Examination**
  ➔ Examination of data media to find files, fragments etc, but without comment

• **Data Evaluation**
  ➔ Analysis and interpretation of discovered files, fragments etc; offering opinions
CRFP Computer Speciality

Application Process

• Qualifications, Memberships, evidence of Training
• Referees
• Agreement to Code of Practice
• Log of Recent Case-work
• Assessor selects from case-work and asks for full file (anonymised)
CRFP Computer Speciality

Application Process

• Assessor applies criteria against case-work, asks for clarifications, makes recommendation
• Reviewed by Lead Assessor
• Some assessment separately scrutinised for process
• Registered!
• Renewal after 3 years
Assessment Criteria (Data Examination)

- Understanding the nature of the case, their role within it and the requirements of the examination, selecting the proper resources, identifying the correct items for examination and getting priorities right.
- Ensuring there is a forensically sound working environment to prevent or detect the contamination or loss of potential evidence.
- Labelling and handling procedures.
- Contemporaneously logging and documenting the handling of items and the data examination process in a way that can be audited and permits the process to be repeated if appropriate.
Assessment Criteria (Data Examination)

• Determining the data examination strategy, identifying essential information and selecting appropriate tools and methods for the task.
• Examining data to identify anomalies and to identify, extract, preserve and exhibit material which is of potential evidential value.
• Reconsidering the work done in the light of new findings and information. Consulting other specialists and relevant reliable sources of information at an appropriate time and in an appropriate way to assist with the interpretation.
• Reporting methods, findings and results - orally, electronically and in writing - clearly and accurately to colleagues, others in the investigation and the court.
• Keeping up to date with technological and other developments in the field and taking active steps to maintain competence.
Assessment Criteria (Data Evaluation)

- Knowing the hypothesis or question to be tested
- Establishing that items submitted were suitable for the requirements of the case
- Confirming that the correct type of examination has been selected
- Confirming that the examination was carried out competently
- Recording, summarising and collating the results of the examination
- Interpreting the results in accordance with established scientific principles
- Considering alternative hypotheses
- Preparing a report based on the findings
- Presenting oral evidence to court and at case conferences
- Ensuring that all documentation is fit for purpose
CRFP Computer Speciality

Assessment Criteria

• Assessor must be able to establish evidence for all of these criteria across a range of cases
US DFCB

• Digital Forensics Certification Board
  ➔ National Institute of Justice hosted by University of Central Florida
  ➔ Certification based on “core competencies”
    • Quality Assurance, Legal and Ethics, Techniques, Process, Concepts
  ➔ Still very early days
Problems of Assessment Schemes

- Assessments have to be detailed to be credible
- The greater the detail, the greater the burden on the assessor in terms of skills and time required
- Assessors need to be practitioners – and will be earning quite highly
- Assessment fees rise correspondingly
- High assessment fees are a deterrent
Problems of Assessment Schemes

• Should non-registered “experts” be barred:
  ➔ From working at all?
  ➔ From giving any type of evidence in court?
  ➔ From giving opinion evidence in court?

• What happens when a court needs highly specialised advice which the professional “digital evidence expert” may not be able to supply?
Conclusions

- There will never be a simple, easy way to select a digital evidence expert
- Qualifications, training, education all help
- Assessment schemes help but have limitations
Conclusions

• There is no substitute for being clear what you want the expert for, and to do

• Probe your potential expert’s skills carefully!
Digital Evidence 2008
26-27 June 2008

Certification, Registration and Education of Digital Forensic Experts

Peter Sommer
London School of Economics
peter@pmsommer.com
p.m.sommer@lse.ac.uk