

Embargo Tuesday 29 October 2002
Spy vs Spy: the science of surveillance and security
Session 3: 11.20am Fraud squad

Presentation: Catching Computer Crooks
Chris Buttner
Computer Forensic Team
Australian Federal Police



The Science Forums

- *key words/terms/ applications: computer analysis, forensics*

Future of forensic computer analysis:

The driving force behind computer forensic analysis has for many years been the underlying technology of the PC.

More recently, other factors have emerged and appear likely to overshadow the future of forensic computer analysis.

I suggest that the next 5 years will see three factors significantly influencing the way organisations deal with forensic computer analysis.

Those factors are:

- an international drive for laboratory accreditation
- the increasing proliferation of embedded devices, and
- an examiner mindset change that sees value in what I describe as the 80/20 solution.

Laboratory accreditation

The drive for laboratory accreditation will put significant financial stress on smaller organisations presently involved in the field.

Some organisations wishing to develop a capacity will form cooperative ventures.

Once a 'critical mass' develops, judges and legal practitioners are likely to put increased pressure on the factual evidence and opinions of experts from non-accredited organisations.

Increasing proliferation of embedded devices

The increasing proliferation of embedded devices such as PDAs, mobile phones, on-board vehicle computers, GPS systems etc -- which are all potential sources of evidence -- will require forensic organisations to make substantial investments in research and development.

Without that investment, recovery of relevant data within an acceptable time frame will be impossible.

The 80 percent solution

Forensic science has traditionally espoused a 100% solution.

Modern business is now seeking solutions that are increasingly a shade of grey rather than pure black and white.

This is not to suggest a lowering of the legal standards of proof. It is more a reflection of managers' need for timely advice in a proactive sense and the role that forensic services can play in filling that need.

Embargo Tuesday 29 October 2002

Profile

Chris Buttner began his career with the Australian Federal Police in 1978.

In 1991, while working in major fraud investigations, he established the AFP Sydney Computer Crime Team and has worked in that team as its leader ever since.

Since 1998 he has been actively involved in the drafting of national competencies for computer forensic examinations.

In 1999 he was elected to the Board of the International Organisation on Computer Evidence (IOCE). He is currently the National Coordinator for the AFP Computer Forensic Teams; represents the AFP on the Australasian Computer Crime Managers Group (an activity of the Australasian Centre for Policing Research) and is the current Chair of IOCE.

The Science Forums

UTS Faculty of Science

Project Manager: Mary Mulcahy 0439 448 861

Consultant: Jenny Eather 0417 207156

mary.mulcahy@uts.edu.au, jenny.eather@uts.edu.au

phone 61 + 2 + 9514 2249, fax 61 + 2 + 9514 9968