Forensic Computing: Current Research Challenges and Directions

Dr Benjamin Turnbull

Forensic Computing Lab
Defence and Systems Institute
University of South Australia
Forensic Computing is multi-disciplinary. Research must reflect this and can come from several areas. I won’t discuss all of these.

Challenges discussed today:

• Increase in jobs, exhibits and what crimes are investigated
• Increase in data sizes and variation
• Breadth of data repositories and devices
• Accreditation and competency
• Dealing with existing and emerging technologies:
  • SCADA
  • Mobile phones
  • Wireless
  • Memory Forensics
  • Netbooks
  • Virtual Machines
  • Old technologies
SA Police E-Crime Lab Jobs and Exhibits
**Jobs – 2007/2008** by the type of offence investigated

This does not reflect the common perception that child abuse imagery is the most common crime investigated (although it is close).

It is interesting to note that drug-crime is the most commonly investigated type of crime from this data.
Exhibits – 2007/2008 by the type of offence investigated

Comparison between the jobs and the exhibit percentages provides an idea of job complexity.

This weighting does not provide for urgency and investigative priority.
Specific Crime Data

This component focuses on specific types of crime and how the investigations relate to electronic evidence.

Specifically, drug crime, fraud, pornography and assault and harassment.

Analysis of electronic items is influenced by:
• Crime type
• Investigator knowledge
• Seriousness of crime
Looks at all illicit drug enforcement.

Use in electronic crime has grown significantly over the recorded period and is now the largest.

Includes selling/trading drugs, production and manufacture of drugs, and other drug offences. Also includes importation.
**Devices analysed**

Primarily cheap, disposable items are connected with drug investigations, rather than computers themselves.
Includes all identity theft, accounting fraud and transaction fraud investigations.

The numbers and percentages of this type of investigation are dropping, but these do not include federal investigations.
The devices analysed reflect the type of crime. Primarily business devices (no or little GPS, games console, etc). Consumer equipment is lacking.

Computers, laptops, hard disks, and mobile phones comprise the bulk of work.

Anecdotally, much of this work is extraction of data that is then analysed offline by investigators.
Including all child abuse imagery and illegal pornography investigations.

Anecdotally this type of investigation is the ‘bread and butter’ of electronic analysis. However, the number of exhibits per job is low and the majority of work is not complex.
As expected, the devices analysed are data storage devices, or devices capable of producing pornography (camera phones, digital cameras). On occasion, online systems are analysed in regards to distribution of such imagery.
Increasing Data Size and Complexity
The estimated size of the digital universe in 2008 is 487 billion gigabytes. This is expected to double every 18 months.

At a more personal level, the storage capacity of a computer is subject to Kryder’s Law, but additionally there are more devices holding data.

This has changed forensic investigation:
- Data trawling
- Connectivity
Even small forensic analysis jobs now deal with amounts of data once considered extreme. Analysts can no longer look at every bit, let alone every file.

Even a basic job is likely to have tens-hundreds of thousands of files. A complex job can have orders of magnitude higher.

How can irrelevant files be filtered without potentially impairing an analyst?
The number and variety of electronic devices has increased. Beyond this, some data storage repositories are off-site:
Computers, laptops, mobile phones, USB keys, external hard drives, cameras, GPS’, iPods (or whatever), CDs, DVDs, Google Docs, Amazon S3, servers, car systems, routers, etc.
A decade ago this was not an issue.
Often, information of importance is spread through multiple devices, each providing some context.
FTK uses a Known File Filter – this removes known files from Windows.

Other areas of research look at data mining combined with visualisation techniques.

Vis gives us options on how we present data:
• View on different data or metadata.
• Filter, zoom and details on demand.
• Intuitively follow leads.
• Undo any filtering.

Must be driven by intelligence. Intelligence can assist, but not at the expense of freedom.
Increasing Data Size and Complexity
Increasing Data Size and Complexity
Increasing Data Size and Complexity
There is other research in the area:
• Intelligent searching beyond keywords.
• Better, more flexible file filtering.

This is an active area of research.
Validation and Verification
• Forensic computing has mostly developed out of a demand for service (collection of electronic evidence) from the law enforcement community
  – in an ad hoc manner not a scientific one.
  – as a discipline that crosses the corporate, academic, scientific as well as the law enforcement domains
  – as a forensic science.
• Compliance with ISO 17025 standard for laboratory accreditation is becoming the main method of achieving the goal of establishing the quality required from a forensic science.
Accreditation brings structure and organization with procedures, documentation and testing.

Implications
- validation and verification of test methods.

Problem
- forensic tools are modified regularly in order to keep up with change in technology
- not all tools used by specialists were designed originally with the forensic process in mind, instead developed to meet the needs of particular interest groups, such as file system drivers, operating systems, Indexing engines,
- Validation and verification in a dynamic environment
The connotation of ‘forensic’ infers a scientific approach. In order for the discipline to adopt a scientific framework there needs to be scientific method.

‘Need for speed’ from the increase in case load, from the increase in the amount of data requiring examination

Trustworthiness of evidence is an issue

Law enforcement has a way to go to meet minimum standards for a scientific discipline.

- 58% of Agencies in the United States still did not have digital evidence policies
- only 57% of agencies required specific training to duplicate, examine and analyze evidence and
- more than 70% of Practitioners had no or minimal training in this discipline.
One of the tenets of scientific method is the principle of reproducibility. This ability to test and accurately reproduce results is also of concern to the digital forensic community. In most cases reproducibility is achieved in the discipline either by using the same tool or by cross validation of forensic tools, that is, producing the same result with two different tools. These methods are sound methodologies in the context of judicial or scientific reproducibility but both have a major flaw inasmuch as they do not deal with what happens when the tools are incorrect. We have met the tenet of reproducibility of the process, that is we can reproduce the result of a tool or test, but not necessarily the principle of reliability.
• Supervisory Control And Data Acquisition.
• Systems were independently run, but are now attached to corporate internal networks.
• These systems are not capable of handling viruses, and have typically relied on security through obscurity.
• Forensic controls must exist to allow investigation, but these are real-time critical systems and cannot be offline for analysis.
Mobile Phones
Mobile phones are increasingly becoming important sources of information in electronic analysis. They comprise approximately 20% of all electronic exhibits analysed in SA.

4 new mobile phone models are being released daily to the UK.

There are tools to analyse mobile phones, but they do so through phone-request.

Different tools will provide different information, based on what the phone allows.

Phone interaction has limitations and issues.
JTAG is a system that is used for phone diagnostics, and does not operate through a phone’s operating system but self-powers into an accessible state.

JTAG allows for the direct dumping of a phone’s internal memory. However, this results in a single file that is a binary of the phone’s memory structures. These structures are proprietary and may not conform to specification.

Memory structures may differ per model or even OS revision.
Wireless
By their very nature, 802.11-based wireless systems provide connectivity between electronic devices without the need for a physical connection to exist, making a wireless network discreet and devices potentially far removed.

This is an issue when considering the evidence identification and collection phase of an area-of-interest within a forensic investigation that may involve electronic evidence.
• Whilst wired connections may be noticed, the lack of physical connections between communicating wireless devices may make the identification of such devices problematic, and this may lead to particular wireless devices, which should be seized, left undiscovered.

• Wireless (specifically 802.11 for the purposes of this research) also operates across physical boundaries, which is also of issue in the case of forensic evidence collection where there may be legal limits to the area searched.

• If the search area for an investigation is limited to an area given by a warrant or other restriction, investigators may not be certain that all relevant evidence lies within this area.
Wireless Cameras and Surveillance
Within the evidence seizure process:
A wireless device outside of normal search boundaries is still fully accessible, but may not be collected for analysis.

The only post-mortem evidence of this is within seized equipment in connection settings and log files.
Area of interest on the right
Potential evidence sources A, B
Access Points 1, 2
Neighbour C

There are two potential issues with the seizure process:

  Whilst Computer A and B are active, they may be accessed from Computer C
  Shutting down AP 1 will not effectively disable networking, as devices may connect to AP 2
The first conviction for wireless misuse occurred in North Carolina, in 2003. Clayton Dillard was arrested after using an insecure wireless network to break into the Wake Internal Medicine Clinic network. He copied 2,000 patient records, which he mailed to police, the media and the patients themselves. He did this to highlight the insecurity of the network, hoping to be awarded a security consultancy there to repair it.

He was traced as he used his own computer, which was named after his business. This was captured by the internal networking security systems the Clinic employed.
Criminal acts involving wireless technology

• 2 men, Brian Salcedo, Adam Botbyl, were arrested in North Carolina, after using a wireless network to break into Lowe’s Hardware stores, and installing software to harvest credit card numbers. They repeatedly connected to the networks of several stores to achieve this.

• The installation of software was noticed by system administrators, and the FBI arrested them in the carpark of the store. Botbyl and Salcedo sentenced to 26 and 108 months prison respectively, with Salcedo’s sentence being the longest computer crime sentenced imposed in the US.
• Myron Tereshchuk pleaded guilty to attempting extortion, in Maryland, in the US. He attempted to extort a pharmaceutical company, delivering threats via anonymous internet connections.

• He was discovered after asking the extortion cheque to be made out in his own name.
Analysing wireless traffic is possible, but Australia governs these interactions under the Telecommunications (Interception and Access) Act, which forbids the interception of networking traffic without a warrant. This governs wireless.

So Kismet (and similar tools) can never be used as evidence, as their use is illegal without a TI warrant.

However, frame headers are exempt from the Act, given that their analysis is required for network protocols to operate.

We are developing forensic software to detect wireless devices in forensically sound ways.
Netbook Forensics
One of the largest segments of computer sales growth in the last year has been from netbooks; low cost, low power laptops.

Designed for internet browsing, some office work and email use.

Developed by Asus, the EeePC was one of the first netbook systems to market. It now represents an entire sub-brand.
There are forensic implications related to these devices, for both extraction and analysis of data.

- **Extraction** – non-standard hardware, lack of optical drive, hard disk or extraction mechanism.
- **Analysis** – custom Linux system. What exists, where is it stored? There is also a lack of storage space available, and this poses greater forensic issues (let me explain…)

This work seeks to develop a means of extracting and forensically analysing the Asus EeePC, such that the lessons learned can be ported to other netbook and mobile computing platforms.
Where netbooks differ and why we care.

This work was conducted on an EeePC 701 (1\textsuperscript{st} generation).
Virtual Machine Forensics
Virtual Machines are becoming a new standard at an enterprise, personal and commercial level. They also have potential forensic issues and benefits.

Their RAM state can be saved, snapshots can be taken and in several implementations, the machine can be suspended, copied and forensic images taken without needing to be shut down.

However, there are also potential issues related to the fact that one system is running within another, and each is vulnerable. Exploits can attack one or both machines and the host OS may contaminate the guest OS.
Older Technologies
Older Technologies

Old technologies can pose issues for electronic analysts.

Computer Forensics has evolved, and there is little documentation for analysing older technologies.

Finding working equipment for correct extraction of old technologies is difficult, there is often no correct procedure and few ways of ensuring that evidence is not contaminated.

There have been both criminal and e-discovery cases where electronic analysis has been stalled through the use of once-common technologies.
Memory Forensics
Memory forensics is a controversial issue in the CF community.

There are benefits – instead of ‘pull the plug’ process, investigators load on an application that saves the contents of RAM to an external disk. The machine can then be shut down.

Analysis of RAM can provide additional information, but the process of acquisition can be seen to be against some of McKemmish’s laws (and also US equivalents) – specifically ‘minimal handling of the original’ and ‘account for any change’.
Memory stores all currently required information, but does not have the same time-stamp and metadata of filesystems. However, the information recoverable can be amazing. It includes:

- Passwords for open encrypted containers
- VOIP packets that can be reconstructed into conversations
- Information on open sessions, unlogged conversations

This is an emerging area, and the benefits are still being realised.

There are two areas of work; acquisition and analysis.

In analysis, Australia is quite advanced. PyFlag created and uses the Volatility framework to perform memory analysis.
Summary
There are challenges and opportunities to research in this area. Computer Forensics is such a varied and altering field that there are so many new technologies and devices to understand.

The capacity for the criminal misuse of any device is amazing and will provide new challenges.

There are also new areas of work in online intelligence and other similar fields.
Conclusion

Questions?
Benjamin.Turnbull@unisa.edu.au