Digital Forensics for the Corporation

Dr John Haggerty
J.Haggerty@salford.ac.uk
http://www.cse.salford.ac.uk/profiles/haggerty/

Presentation outline

- Digital forensics
- Digital forensics versus computer security
- Issues for an organisation
- Legal considerations
- Current practice
- Resolving technical and organisational issues
- Future challenges and directions

University of Salford
A Greater Manchester University

Why digital forensics ?

- Field has received great interest
  - The CSI effect ☹
- Pervasiveness of computing devices in home and work environments
  - Greater sources of potential evidence
  - Greater amounts of data
- Temporary nature of this evidence
  - The 'future historian' problem

University of Salford
A Greater Manchester University

Digital forensics – a definition(?)

- "*Digital forensics: the study of how people use computers to inflict mischief, hurt and even destruction*" (Mohay et al, 2003)
- "*The application of computer investigation and analysis techniques to determine potential evidence*" (Lin & Seberry, 2003)
- No accepted definition
  - However, generally focuses on investigation and analysis to determine culpability

University of Salford
A Greater Manchester University

Beyond law enforcement

- Wide range of digital forensics activities and tools being used today, e.g.
  - Legal compliance, data recovery, audit, security (Incident Response), etc.
- Increasingly being deployed in organisations
  - Without the robustness of law enforcement processes?
- Organisations understand security but not forensics

University of Salford
A Greater Manchester University

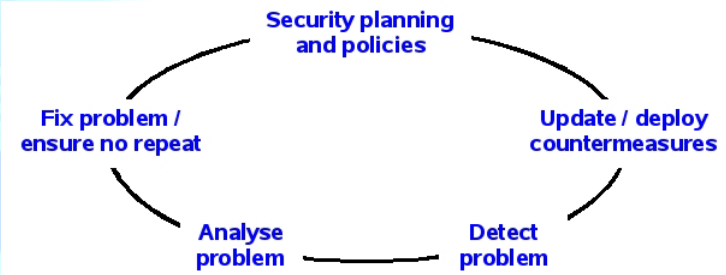
Forensics vs. security

DIGITAL FORENSICS	COMPUTER SECURITY
Attribute culpability	System protection
Multi-disciplinary	Discipline in own right
Emergent field	Established field
No national frameworks/ certification	International frameworks/ certification
Closed forums	Sharing information
Long-term viewpoint (computationally exhaustive)	Short-term viewpoint (reduce computational exhaustion)

University of Salford
A Greater Manchester University

Computer security timeline

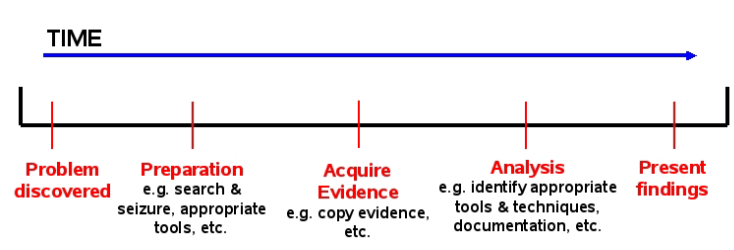
- Iterative process
- Focus on system integrity



University of Salford
A Greater Manchester University

Digital forensics timeline

- Linear process
- Focus on culpability/responsibility



University of Salford
A Greater Manchester University

Issues for an organisation

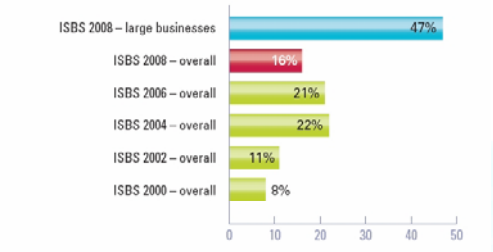
- No such thing as a typical investigation within an organisation
  - A demoted employee resigns from an organisation and leaves behind a date triggered time bomb program
  - Employees are discovered to be sending sexist or racist emails about a colleague
  - An employee with access to sensitive information offers this data for sale
  - A public company wishing to operate in the US must legally comply

University of Salford
A Greater Manchester University

Computer misuse

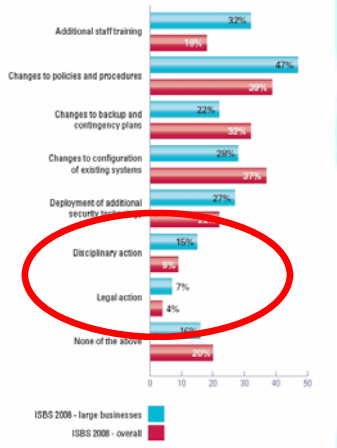
How many UK businesses suffered from staff misuse of information systems?

Figure 62



How did UK businesses address the weakness that caused their worst incident?

Figure 80



Source: BERR Information Security Breaches Survey 2008

University of Salford
A Greater Manchester University

Legal considerations

- Organisations must be aware of / comply with a variety of legislations
- Computer security and digital forensics differ in their relationship with the law
  - Computer security has limited legal implications
    - Focus on policy and integrity
  - Digital forensics requires greater understanding of the law
    - Both judicial law and corporate / employment legislation

University of Salford
A Greater Manchester University

Legal considerations

- Accessing personal data
- **Data Protection Act (1998)**
  - Who owns personal data in a corporate environment?
  - Personal data belonging to customers?
  - Appropriate security measures applied to personal data during investigation
  - DPA does provide some exemptions for detection/ prevention of criminal activities
    - Tax duties, national security, etc.

University of Salford
A Greater Manchester University

Legal considerations

- Monitoring computer networks
- **Regulation of Investigatory Powers Act (2000)**
  - Unlawful to intercept any communications in the course of transmission without consent or lawful authority
  - Differentiates communications / traffic data from content
  - Part III of RIPA – encryption keys

University of Salford
A Greater Manchester University

Legal considerations

- Procedures for corporate digital forensics investigations
- **Criminal Procedure and Investigations Act (1996) and Amendments to the Criminal Justice Act (2003) – Part 5**
  - Covers the legal requirements to provide evidence in support of a prosecution should the case end up in a court of law
  - 'Live investigation' – notes to be handed over

University of Salford
A Greater Manchester University

Legal considerations

- Offences that must be handed over to the Police
- **Money Laundering Regulations [MLR] (2003) and Sexual Offences Act [SOA] (2003)**
  - MLR concerned with falsifying of computer records
  - SOA is concerned with indecent images of children and evidence handling of such evidence

University of Salford
A Greater Manchester University

Legal considerations

- Relevant non-UK legislation
- **US Sarbanes-Oxley (2002)**
  - Came into being after Enron scandal
  - Any company wishing to do business with US must comply with this law
  - Section 802 imposes explicit penalties for the destruction of essential files
  - Forensic investigations should be performed so as to (where possible) ensure no alteration to corporate computer files

University of Salford
A Greater Manchester University

Legal considerations

- What about outcome of corporate case?
- **Employment Act (2002) and Employment Rights (Dispute Resolution) Act (1998) or Employment Tribunals Act (1996)**
  - Many forensics investigations will not come under judicial law
  - Employment Act covers disciplinary and dismissal procedures
  - Employment Rights Act covers dismissal and unfair dismissal

University of Salford
A Greater Manchester University

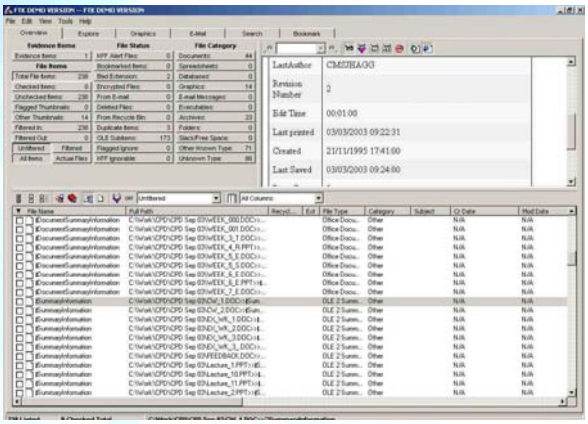
Current practice

- Time consuming and laborious!
- Collect evidence and copy taken
- Forensics tools to reconstruct logical structure of underlying OS
- View extant / deleted files
- Report relevant / suspicious data / files with supporting evidence
  - Time files were created/accessed/modified, etc.
- Present case

University of Salford
A Greater Manchester University

Current practice

- Forensics ToolKit (Access Data)



University of Salford
A Greater Manchester University

Issues with current practice

- **Technical issues:** current tools have some issues, e.g.
  - Not designed for current HDD capacities
  - File system reconstruction and MD5 reliance
  - Intangible versus tangible evidence
- **Organisational issues:** are organisations ready to conduct an investigation?
  - No existing frameworks
  - Lack of understanding
  - Lack of experience

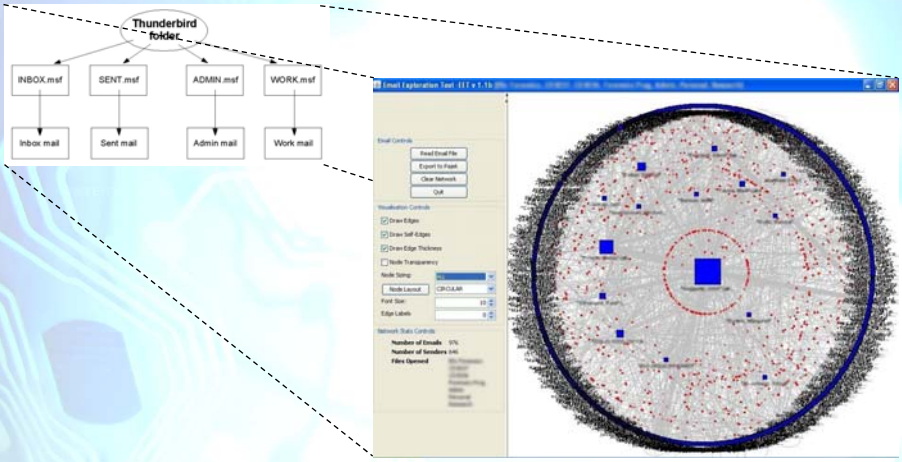
University of Salford
A Greater Manchester University

Resolving technical issues

- Development of new tools to meet today's requirements
- **FORSIGS** (and FORWEB)
  - Fast automated searches of storage media for malicious multimedia
    - Use signature analysis and searches HDD rather than OS
- **EET**
  - Email analysis to quantify and measure intangible evidence

University of Salford
A Greater Manchester University

EET



University of Salford
A Greater Manchester University

Resolving organisational issues

- Focus on technical issues not enough
  - Need to look at processes and procedures
- Requirement for robust framework
  - Law enforcement have ACPO Guide, but organisations have no framework
- Taylor, Haggerty & Gresty (2007) *Organisational Model for Computer Forensics Investigations*
  - High-level, 4-stage model, simplified procedures

University of Salford
A Greater Manchester University

OMCFI model

Stage 1 Investigation preparation	a. identify the purpose of investigation
	b. identify resources required
Stage 2 Evidence acquisition	a. identify sources of digital evidence
	b. preserve digital evidence
Stage 3 Analysis of evidence	a. identify tools and techniques to use
	b. process data
	c. interpret analysis results
Stage 4 Results dissemination	a. report findings
	b. present findings

University of Salford
A Greater Manchester University

Future challenges

- Academia well placed to address future issues (throw out goalposts?)
- To name a few
  - Move to mobile/pervasive networked devices
  - Expanding memory availability
  - User security
  - Secure networked applications (e.g. Skype)
  - Frameworks
  - Law and technology

University of Salford
A Greater Manchester University

Future directions

- Some future directions of the field
  - Process automation
  - Accepted applications used by all
  - Development of scalable tools and techniques
  - Development of standards outside law enforcement
  - Utilization of intangible evidence
  - Addressing geo-political constraints
  - Visual analytics for forensics

University of Salford
A Greater Manchester University

Summary

- Computer forensics and computer security are complementary but distinct fields
- Organisations require an understanding of investigation processes and relevant laws
- Current practice is fairly robust but improvements are required
- A number of challenges exist with the change in the digital landscape

University of Salford
A Greater Manchester University