Digital Forensics in the Organisation

Dr John Haggerty
School of Computing and Mathematical Sciences,
Liverpool John Moores University
J.Haggerty@ljmu.ac.uk
http://www.cms.livjm.ac.uk/cmpjhagg/

Outline of talk

• Digital forensics
• Digital forensics versus computer security
• Organisational considerations
• Current practice
• Resolving technical and organisational issues
• Future challenges and directions
Why digital forensics?

• The field has received great interest recently
  ▪ The ‘CSI Effect’

• Pervasiveness of computing devices in home and work environments
  ▪ Greater potential sources of evidence
  ▪ Greater amounts of evidence

• Temporary nature of this evidence
  ▪ The ‘Future Historian’ problem

• Digital forensics provides means by which crime (computer-based and ‘traditional’) can be detected, tracked over time and culpability for actions ascribed

What is digital forensics?

• “Computer 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” (Li & Seberry, 2003)

• No accepted definition

• Focus on investigation and analysis
  ▪ To determine responsibility for an event/set of events

• Legacy of law enforcement focus
  ▪ But is being adopted outside this domain
Digital forensics outside law enforcement

- Whilst there is the law enforcement legacy of the field, digital forensics tools and techniques are increasingly being used outside this role
  - Data recovery
  - Legal compliance
  - Audit
  - Security
  - Networks

- Increasingly being deployed in organisations
  - However, this is often without the robustness that law enforcement requires

- Organisations understand security but not forensics

Forensics vs. security

<table>
<thead>
<tr>
<th>DIGITAL FORENSICS</th>
<th>COMPUTER SECURITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute culpability</td>
<td>System protection</td>
</tr>
<tr>
<td>Multi-disciplinary</td>
<td>Discipline in own right</td>
</tr>
<tr>
<td>Emergent field</td>
<td>Established field</td>
</tr>
<tr>
<td>No national frameworks/ certification</td>
<td>International frameworks/ certification</td>
</tr>
<tr>
<td>Closed forums</td>
<td>Sharing information</td>
</tr>
<tr>
<td>Long-term viewpoint (computationally exhaustive)</td>
<td>Short-term viewpoint (reduce computational exhaustion)</td>
</tr>
</tbody>
</table>
Computer security timeline

- Iterative process
- Focus on system integrity

Digital forensics timeline

- Linear process
- Focus on culpability/responsibility
Issues for an organisation

- No such thing as a typical scenario for the organisation
  - A demoted employee leaves the organisation and leaves a date-triggered ‘time-bomb’ which deactivates handheld devices used by the sales force
  - An ex-employee sends threatening or malicious emails
  - An employee in a law firm steals a trial plan and offers it for sale to the opposing lawyer team
  - An employee with access to sensitive customer information offers this information for sale to criminals
  - A public company wishing to operate in the US having to demonstrate complicity with the Sarbanes-Oxley Act

Legal considerations

- Organisation must be aware of / comply with a variety of legislations
- Data Protection Act (1998)
  - Personal data accessed during a corporate computer forensic investigation
  - Monitoring of computer networks during a corporate investigation
  - Procedures used during an investigation
Legal considerations

- Offences that must be reported to the police:

- Relevant non-UK legislation:

- What about the outcome of a corporate case?

Current practice

- Time consuming and laborious!
- Collect evidence and copy taken
- Forensics tools to recreate logical structure of underlying operating system
- View files
  - Extant and deleted
- Report suspicious/malicious files data/files with supporting evidence
  - Time files were created/accessed/modified, by whom, etc.
- Present case and evidence (to management, legal team, court, etc.)
Example - FTK

Issues with current practice

• JMU working to resolve some of the following

  • **Technical issues:** current tools have some limitations
    ▪ Not designed for current hard drive capacities
    ▪ Time pressure from management to deliver results
    ▪ Filesystem reconstruction
    ▪ Reliance on MD5 file checksum searches

  • **Organisational issues:** are organisations ready to conduct an investigation?
    ▪ No existing frameworks
    ▪ Lack of understanding
    ▪ Contravention of policies rather than crime *per se*
    ▪ Lack of experience
Resolving technical issues

• Development of new tools to meet today’s requirements
  - International computer security and forensics company based in NW taking the following forward

• FORSIGS – automated, fast forensic searches of storage media for malicious multimedia
  - Produces file fingerprints from known files
  - Utilises underlying hard drive architecture (not filesystem) to achieve speed of search

• FORWEB – automated network forensics tool for searching Web servers for malicious multimedia
  - Uses file fingerprinting technique combined with Webbots

Resolving technical issues - FORSIGS

• FORSIGS automated searches for 100 file fingerprints within 5GB to 20GB evidence files
  - Suggests 30 minutes to search 100GB on 3GHz processor compared to 50 minutes on 2GHz processor
Resolving technical issues - FORWEB

- Searches for fingerprints across a network
- Network will have some impact
- Flickr (external) ACSF (internal)

- Additional EXIF picture data is also reported by the program such as camera make & model, date picture taken, settings, etc.

Resolving organisational issues

- Focus only on technical issues not enough
  - Need to look at processes/procedures
- Organisational requirement for robust framework for conducting investigations
  - Law enforcement have ACPO Guide, organisations have no such framework
  - Four-stage model
  - High-level view of the investigation process (outside law enforcement)
  - Simplified procedures irrespective of tools used
  - Breaks up a complex process (example demonstrates this)
The 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

---

The model – an example

- Example – unauthorised leak of commercially sensitive documents

- **Stage 1: Investigation preparation**
  - A) **purpose** – gain evidence and culpability for leak of information
  - B) **resources** – access to personnel, machines, servers, management, access to external resources

- **Stage 2: Evidence acquisition**
  - A) **sources** – network hosts, internal servers, network logs, hard drive data, personnel, etc.
  - B) **preserve evidence** – on-site analysis, host/server hard drive images, mail server, copy all relevant machine data to analysis machine, etc.
The model – an example

• Stage 3: evidence analysis
  • A) identify tools – forensics tools if available, file viewers (deleted and extant files), network logs, hex editors, etc.
  • B) process data – hard drive analysis, view documents, view registry, email logs, network logs, security logs, etc.
  • C) interpret evidence – timeline analysis, network analysis, record findings, etc.

• Stage 4: present evidence
  • A) report findings – demonstrate methodologies, findings, supporting evidence, submit to management/legal team, etc.
  • B) present findings – to management, possibly to industrial tribunal

Future challenges

• Academia well placed to meet future challenges to the field (throw out the goalposts?)

• To name a few:
  • Move to mobile/pervasive networked devices
  • Expanding memory availability
  • User security
  • Secure networked applications (e.g. Skype)
  • Investigatory procedures/frameworks in corporate environments
  • The law and technology (geo-political borders)
  • Multi-disciplinary nature of the field
Future directions

• Some future directions of the field:
  § Process automation
  § Development of scalable tools and techniques
  § Development of standards outside law enforcement
  § Understandable and applicable investigation frameworks
  § Security with accountability
  § Multi-disciplinary approaches encompassing law, technology and trust

Summary

• Digital forensics is currently receiving much attention
• Computer security and computer forensics are distinct but complementary fields
• Digital forensics in the organisation is not only about investigations
• Both technical and organisational issues require resolution
• Academia is well placed to address future challenges