
**Counter-Cybercrime Technology Investigation Symposium (CTINS)**

# Open Source Forensic Tools for Capacity Building

Dr. Joshua I. James
Joshua.i.james@hallym.ac.kr
Legal Informatics and Forensic Science Institute
College of International Studies
Hallym University

# Capacity Building

- **Irish case in 2009-2010**
  - Computer Crimes Unit had 14 investigators (population 4.6 million)
  - All based in Dublin – rural areas difficult to access
  - Case backlog of over 3 years
    - Several liability close calls
  - Recession / austerity measures hit police budgets very hard

# Capacity Building

- **Irish case in 2009-2010**
  - Need to reduce case backlog…
  - While reducing budget…
  - And maintain quality of investigation
- **First: Measure!**

# Capacity Building

- **What are the most important types of cases?**
  - Are priority areas actually priority?
- **Where do investigators spend the majority of their time?**
- **What slows down investigations?**
- **Are there any obvious time-wasters?**

# Capacity Building

- **Irish case in 2009-2010 [1]**

**Table 1**
Percentage of incoming investigation requests per crime group in 2009–2010.

| Crime group | Incoming investigation requests | Incoming investigation requests |
|---|---|---|
| Child exploitation material | 444 | 34% |
| Data retrieval, Internet investigations, email and fraud/counterfeiting | 601 | 46% |
| Murder, cell phones, telephone fraud, hacking, kidnappings, drug related | 65 | 5% |
| Other | 196 | 15% |
| **Total:** | **1306** | **100%** |

**Table 2**
Average estimated percentage of an investigator's time spent per crime group per week.

| Crime group | Average estimated % of investigator's time |
|---|---|
| Child exploitation material | 80% |
| Data retrieval, Internet investigations, email and fraud/counterfeiting | 15% |
| Murder, cell phones, telephone fraud, hacking, kidnappings, drug related | 5% |

# Capacity Building

- **Irish case in 2009-2010 [1]**

**Table 3**
Percentage of requests closed per crime group, per total closed requests, and per total incoming investigation requests in 2009–2010.

| Crime group | % of requests closed per crime group | % of total closed requests | % of total incoming investigation requests |
|---|---|---|---|
| Child exploitation material | 35% | 20% | 11% |
| Data retrieval, Internet investigations, email and fraud/counterfeiting | 65% | 52% | 29% |
| Murder, cell phones, telephone fraud, hacking, kidnappings, drug related | 67% | 6% | 4% |
| Other | 84% | 22% | 13% |
| **Total:** | | | **744** |

# Capacity Building

- **Solving the problem**
  - Organizational changes
  - Implemented custom open source tools
  - Biggest change: process flow (tools modified to support process)
- **Traditional Digital Forensic investigation process is usually not very optimized**

# Defining Open Source

# Open Source Tools

- **Software that provides the source code for review**
  - Usually able to modify the source code
  - Usually has a main developer or community
    - Main developer may be a company
- **Most liberal definition:**
  - “Open source software is software with source code that anyone can inspect, modify, and enhance.” [2]

# Open Source Tools

- **Open Source does not necessarily mean ‘Free’**
  - Many open source tools are provided at no cost
  - Some open source tools are commercial products that also provide the source for review / community expansion

# Open Source Tools

- **Paid tools tend to have support services similar commercial / closed source software**
  - Expert witness services sometimes provided
- **Free tools generally rely on the community or self-support**
  - Expert witness services not usually provided

# Open Source Tools

- **In most countries results from open source tools are admissible in court**
  - Sometimes more accepted than closed source: can see how the tool works (requires programming knowledge)
  - Most tools can be accepted if they are *properly tested*
  - Investigator must be the expert witness

# Why use open source tools for digital forensic investigation?

- **Open Source Digital Forensic tools have improved a lot in recent years**
  - All digital forensic tasks can be done in a similar time
- **(Usually) Reduced cost**
  - Many open source tools are provided for free
  - Charge for training / support
  - Important for *sustainable* capacity building

# Why use open source tools for digital forensic investigation?

- **Improved local support**
  - More support and control for local languages and data structures (Asian languages / file formats)
- **Greater flexibility and process automation**
  - Open source tools normally provide support for multiple platforms

# Why use open source tools for digital forensic investigation?

- **Improved feature expansion**
  - Open source tools often provide libraries that can be used as a basis for your own tools
- **(arguably) Improved security / correctness**
  - Open source tools have a potential to be more secure because

# Reasons to use commercial closed source tools for digital forensic investigation

- **Ease of use**
  - Expert witness describing the tool may be provided
  - Technical support almost aways provided
  - Closed/commercial products are generally easy to use (low learning curve)
    - Open source tools tend to be harder to use (requires technical ability)
  - Commercial tools are sometimes maintained longer

# LE Capacity Building with the UNODC

- **My experience:**
  - Some costs cannot be easily reduced: hardware – let's focus budgets on hardware
  - Can we make a fully-functional digital forensic laboratory using only open source tools?
    - YES! But…
  - Providing expensive closed-source software (that must be renewed) does not help countries
    - Buy & train this year – what happens next year?

# Interesting Open Source Tool (kits)

- **Autopsy**
  - http://www.sleuthkit.org/autopsy/
- **Volatility**
  - http://www.volatilityfoundation.org/
- **DEFT / Caine**
  - http://www.deftlinux.net/
  - http://www.caine-live.net/
- **DeepThought [3]**
- **Automated Network Triage (ANT) [4]**

# Open Source Tools

- **Education:**
  - Video game to train first responders on digital evidence handling [5]

# Open Source Tools

- **Hardware:**
  - FIREBrick [6] – acquisition system
  - Open source alternative to hardware write blockers and acquisition devices
  - Can be built for about $199
  - Uses open-source software
  - Allows custom programs

# Current Project

- **Open Source Infrastructure for Child Exploitation Investigation**
  - Machine learning for automatic classification of images and videos
  - Known-bad hash database compatible with C4All (Autopsy with C4All plugin for front-end)
  - Costs: Hardware, development, training
  - All results can be easily replicated in other countries

# References


1) James, J. I., & Gladyshev, P. (2013). A survey of digital forensic investigator decision processes and measurement of decisions based on enhanced preview. Digital Investigation, 10(2), 148–157. https://doi.org/10.1016/j.diin.2013.04.005

2) (n.d). What is open source?. OepnSoruce.com. https://opensource.com/resources/what-open-source

3) Shaw, A., & Browne, A. (2013). A practical and robust approach to coping with large volumes of data submitted for digital forensic examination. Digital Investigation, 10(2), 116–128. https://doi.org/10.1016/j.diin.2013.04.003

4) Koopmans, M. B., & James, J. I. (2013). Automated network triage. Digital Investigation, 10(2), 129–137. https://doi.org/10.1016/j.diin.2013.03.002

5) Conway, A., I. James, J., & Gladyshev, P. (2015). Development and initial user evaluation of a virtual crime scene simulator including digital evidence. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST (Vol. 157). https://doi.org/10.1007/978-3-319-25512-5_2

6) http://dfire.ucd.ie/?page_id=1011