Digital Forensics: Current and Future Needs

Katrin Franke
Norwegian Information Security Laboratory (NISlab)
Gjøvik University College
www.nislab.no
Crime in the Modern World

- **Massive amount of data:**
  - 247 billion email per day
  - 234 million websites
  - 5 billion mobile-phone users

- **ICT Infrastructures:**
  - Complex, rapidly growing
  - Dynamically changing
  - Hostile, adversary environment

- **Cybercrime:**
  - One million victims daily
  - Expected losses 297 billion Euro
  - Crowd sourcing -> Crime sourcing
  - Flash mobs -> Flash robs

- **Proactive, Ultra-large scale Forensic Investigations, Computational Forensics:**
  - Situation-aware methods
  - Quantified, measurable indicators
  - Adaptive, self-organizing models
  - Distributed, cooperative, autonomous

- **Rule-of-Law:**
  - Culture, social behaviours
  - Legal & privacy aspects
  - Cross-jurisdiction cooperation
  - European / International cyberlaw
  - Law as framework for ICT
  - Law as contents of ICT, Automation, programming of legal rules
Forensic Science

Forensic methods consist of multi-disciplinary approaches to perform the following tasks:

- **Investigate** and to **Reconstruct** a crime scene or a scene of an accident,
- **Collect** and **Analyze** trace evidence found,
- **Identify**, **Classify**, **Quantify**, **Individualize** persons, objects, processes,
- **Establish linkages**, associations and **reconstructions**, and
- Use those findings in the prosecution or the defense in a court of law.

So far, mostly dealt with previously committed crime, **greater focus is now to prevent future crime.**
Crime in the Modern World

cont.

- Digital devices are used everywhere: Computers, mobile phones, PDAs, cameras, copy machines, printers, videogame consoles
- Used to plan/conducted physical and cyber crimes

Digital evidence:
- System registry, Event logs, Print spool, Swap files, Recycle bin
- Mobile phone SMS messages, Contacts, Connections etc.
- Threatening emails or chats messages
- Documents (e.g., in places they shouldn’t be)
- Suicide notes
- Bomb-making diagrams
- Malicious Software, Viruses, Worms, Botnet ...
- Child pornography
Computer Crime Offences & Costs

Report of the Belgian Economic and Financial Crimes Division (DJF)

Online crime complaints and dollar loss in the United States (IC3, 2010)

German Annual Federal Criminal Police Office
Situation Report on Cybercrime 2009 and 2010
European Status

Strengthening Forensic Science in the United States: A Path Forward

Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council
This PDF is available from the National Academies Press at: http://www.nap.edu/catalog/12589.html
I. New collaborative approaches and partnerships with private and research sector

II. Active support and investment in cutting-edge research and development

III. Adoption of research results, development of investigative tools and methods, and further advancement of ICT in police work
Interpool –
Global-Complex Singapore

- **Mission**
  - Enhance capability to tackle the crime threats of the 21st century
  - Strengthen international policing worldwide

- **Strategic Initiatives**
  - *Innovative research and development* to enhance forensics and database capabilities (incl. identification of crimes and criminals, biometrics, database technologies)
  - Addressing the demand for technology and innovation-based *capacity building and training* (e.g. training in advanced investigation techniques)
  - Enhancing capacity to provide *24/7 operational support* to police across time zones and distances with greater mobility
Crime in the Modern World

- Massive amount of data:
  - 247 billion email per day
  - 234 million websites
  - 5 billion mobile-phone users

- ICT Infrastructures:
  - Complex, rapidly growing
  - Dynamically changing
  - Hostile, adversary environment

- Cybercrime:
  - One million victims daily
  - Expected losses 297 billion Euro
  - Crowd sourcing -> Crime sourcing
  - Flash mobs -> Flash robs

- Proactive, Ultra-large scale Forensic Investigations, Computational Forensics:
  - Situation-aware methods
  - Quantified, measurable indicators
  - Adaptive, self-organizing models
  - Distributed, cooperative, autonomous

- Rule-of-Law:
  - Culture, social behaviours
  - Legal & privacy aspects
  - Cross-jurisdiction cooperation
  - European / International cyberlaw
  - Law as framework for ICT
  - Law as contents of ICT, Automation, programming of legal rules
Challenges and Demands in Forensic Science

Challenges:

- **Tiny Pieces of Evidence** are hidden in a mostly **Chaotic Environment**,  
- Trace Study to reveal **Specific Properties**,  
- Traces found will be **Never Identical**,  
- Reasoning and Deduction have to be performed on the basis of - **Partial Knowledge**,  
  - **Approximations**,  
  - **Uncertainties** and  
  - **Conjectures**.

Demands:

- **Objective** Measurement and Classification,  
- **Robustness** and **Reproducibility** of the Results,  
- **Secure** against Falsifications.
Current Forensic Practice

- Evidence becoming increasingly **data intensive** and **widely distributed**
- Common practice to **seize all data carriers**; amounts to **many terabytes of data**
- Enrich with data available on the **Internet, Social networks**, etc.
- Huge amounts of **Paper Documents**
Testimon-Research Agenda

- Research in the area of large-scale investigations; automatic search through terabytes of electronic data storage within closed systems and the Internet,

- Research and development for the rapid acquisition, correlation and analysis of Internet-related evidence,

- Technologies for cross-media search and data integration to access diverse sources of information, in particular data enrichment from Internet sources,

- Algorithms for the analysis of encrypted evidence and cryptographic credentials,

- Design of advanced computing technologies to achieve more objective evidence analysis and final decision making by implementing computational intelligence,

- Develop of methods and tools for digital penetrator attribution and profiling, visualization of serious criminal relationships and associations, and geographical mapping of digital and physical evidence.
Computational Forensics

- Study and development of computational intelligence methods to
  - Assist in basic and applied research, e.g. to establish or prove the scientific basis of a particular investigative procedure,
  - Support the forensic examiner in their daily casework.

- Modern crime investigation shall profit from the hybrid-intelligence of humans and machines.
Computational Methods

- **Signal / Image Processing**: one-dimensional signals and two-dimensional images are transformed for better human or machine processing,
- **Computer Vision**: images are automatically recognized to identify objects,
- **Computer Graphics / Data Visualization**: two-dimensional images or three-dimensional scenes are synthesized from multi-dimensional data for better human understanding,
- **Statistical Pattern Recognition**: abstract measurements are classified as belonging to one or more classes, e.g., whether a sample belongs to a known class and with what probability,
- **Machine Learning**: a mathematical model is learnt from examples.
- **Data Mining**: large volumes of data are processed to discover nuggets of information, e.g., presence of associations, number of clusters, outliers, etc.
- **Robotics**: human movements are replicated by a machine.
Computational Forensics - Definition

It is understood as the hypothesis-driven investigation of a specific forensic problem using computers, with the primary goal of discovery and advancement of forensic knowledge.

CF works towards:

1) **In-depth Understanding** of a forensic discipline,
2) **Evaluation** of a particular scientific method basis and
3) **Systematic Approach** to forensic sciences by applying techniques of computer science, applied mathematics and statistics.

It involves **Modeling** and computer **Simulation (Synthesis)** and/or computer-based **Analysis** and **Recognition**
Example:
Ongoing Research – Malware and Botnet Detection

Nyugen, Franke, et all

www.nislab.no
Admission of Computational Forensics

1. Need of Automatization, Standardization, and Benchmarking

2. Need of Education, Joint Research, and Development by Forensic and Computer Scientist

3. Need of Legal Framework
Automatization, Standardization, and Benchmarking

- **Increase Efficiency** and **Effectiveness**
- **Perform Method / Tool Testing** regarding their Strengths/Weaknesses and their Likelihood Ratio (Error Rate)
- **Gather** data, manage and extrapolate data, and to synthesize new **Data Sets** on demand.
- **Establish** and implement **Standards** for data, work procedures and journal processes

**Fulfillment of Daubert Criteria**

Joint Research & Development: Forensic and Computer Scientist

- **Education and training,** Revealing the state-of-the-art in *each* domain
- **Sources of information** on events, activities and financing opportunities
- **International forum to peer-review and exchange,** e.g., IWCF workshops
- **Performance evaluation, benchmarking, proof and standardization** of algorithms
- **Resources in forms of data sets, software tools, and specifications** e.g. data formats
- **New Insights** on problem description and procedures
Legal Framework ?!

- Questions on methods for **dimensionality reduction** – loss of relevant information
- Questions on **extracted numerical parameters** – loss of information due to inappropriate features
- Questions on the reliability of **applied computational method / tool**
- Questions on the final conclusion due to “wrong” computational results
Crime in the Modern World

- Massive amount of data:
  - 247 billion email per day
  - 234 million websites
  - 5 billion mobile-phone users

- ICT Infrastructures:
  - Complex, rapidly growing
  - Dynamically changing
  - Hostile, adversary environment

- Cybercrime:
  - One million victims daily
  - Expected losses 297 billion Euro
  - Crowd sourcing -> Crime sourcing
  - Flash mobs -> Flash robs

- Proactive, Ultra-large scale
- Forensic Investigations, Computational Forensics:
  - Situation-aware methods
  - Quantified, measurable indicators
  - Adaptive, self-organizing models
  - Distributed, cooperative, autonomous

- Rule-of-Law:
  - Culture, social behaviours
  - Legal & privacy aspects
  - Cross-jurisdiction cooperation
  - European / International cyberlaw
  - Law as framework for ICT
  - Law as contents of ICT, Automation, programming of legal rules
Open Forensic Discussion

1. Need of Automatization, Standardization, and Benchmarking

2. Need of Education, Joint Research, and Development

3. Need of Legal Framework

4. Stakeholders & PP-Partnerships
Thank you for your consideration of comments!

Getting in touch
WWW: kyfranke.com
Email: kyfranke@ieee.org
Skype/gTalk: kyfranke
Katrin Franke, PhD, Professor

- Professor of Computer Science, 2010
  PhD in Artificial Intelligence, 2005
  MSc in Electrical Engineering, 1994
- Industrial Research and Development (15+ years)
  Financial Services and Law Enforcement Agencies
- Courses, Tutorials and post-graduate Training:
  Police, BSc, MSc, PhD
- Chair IAPR/TC6 – Computational Forensics
- IAPR Young Investigator Award, 2009
  International Association of Pattern Recognition