Digital Forensics: behind the scenes

David-Olivier Jaquet-Chiffelle
Full professor
ESC, University of Lausanne

DFRWS 2015
March 25th, 2015

Forensic science on trial

DFRWS 2015 / David-O. Jaquet-Chiffelle
Forensic science on trial

> Brandon Mayfield

> Attorney near Portland, Oregon, USA

> Wrongly arrested because of an erroneous fingerprint identification

> Wrongly charged with the 2004 terrorist train bombing in Madrid

Forensic science on trial

> Forensic science becomes vulnerable to several kinds of attacks and criticisms

> The trustworthiness of forensic science is now questioned

> How « scientific » is forensic science ?
> How reliable are the underlying technologies ?
> Are expert certifications trustworthy ?

> How can we

> strengthen forensic science ?
> reinforce the identity of forensic science ?
General trend

*To standardize* methods and procedures

*To accredit* labs and *certify* experts

*To partition forensic science into silos* and make it a *patchwork* of technical disciplines

---

Forensic science(s)

[Diagram showing overlapping circles representing various fields: Physics, Biology/med., Chemistry, Law, Criminology, Police, Forensic science(s)]
### Duplication of the world of traces

**The digital domain**
- goes beyond a new discipline
- creates a duplication of the world of traces

<table>
<thead>
<tr>
<th>Analog domain</th>
<th>Digital domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Film photography</td>
<td>Digital pictures</td>
</tr>
<tr>
<td>Handwritten signature</td>
<td>Digital signature</td>
</tr>
<tr>
<td>Safe</td>
<td>Crypto-algorithms</td>
</tr>
<tr>
<td>Paper files</td>
<td>Databases</td>
</tr>
<tr>
<td>(Snail) mail</td>
<td>E-mail</td>
</tr>
</tbody>
</table>

### The « real » world

<table>
<thead>
<tr>
<th>« Real »</th>
<th>Analog</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical</td>
<td>Most traditional traces</td>
</tr>
<tr>
<td>Virtual</td>
<td>e.g. testimony</td>
</tr>
</tbody>
</table>
Digital traces

> Material
physical digital traces

> Abstract
virtual digital traces

The real world

<table>
<thead>
<tr>
<th>« Real »</th>
<th>Analog</th>
<th>Digital</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical</td>
<td>Most traditional traces</td>
<td>e.g. holes at the surface of a DVD</td>
</tr>
<tr>
<td>Virtual</td>
<td>e.g. testimony</td>
<td>Most traces in the information society</td>
</tr>
</tbody>
</table>
New perspective

> Digital traces

> offer
  > a new perspective

> require
  > to extend the traditional paradigms
  > by integrating the virtual one

Forensic science(s)

- Physics
- Biology/med.
- Chemistry
- Computer science
- Internet
- Law
- Police
- Criminology
Digital traces

> Risk

> To isolate the digital paradigm

> To create a new science of
> “digital” traces and identities

> i.e., to split a core domain of forensic science

A strategy to reinforce forensic science

> Accreditations and certifications?
> might be adequate for some technologies or laboratories, not for a science

> Forensic science should not be confined to a patchwork
> of technologies
> of other sciences applied to forensic issues
> of forensic science providers
A strategy to reinforce forensic science

> A true forensic science is needed with

> a stronger scientific approach,
> a broader vision and
> a common unifying language

Forensic science: wikipedia definition

> Forensic science is the scientific method of gathering and examining information about the past which is then used in a court of law
Lausanne school of forensic science

> Forensic science should not be confined to "court of law" requirements only

Role of forensic science

> Forensic science aims at
  > Bringing admissible evidence to a court of law

> But it also aims at
  > Participating in the decision process in the investigation
    > Formulation of hypotheses, choices
  > Finding ways to disable or discourage criminal activities
    > Botnet shutdown
    > Rise the required criminal effort for some key actions
  > Detecting, e.g. through their modus operandi,
    > Series of criminal activities
    > Criminal networks and their structures
Stolen credit card credentials

Extent of the problem

- 1 label supplier
- 1767 labels
- Declared value: US $ 275,328
- 23 weeks of activities
Forensic science should not be confined to “court of law” requirements only.

The trace is the fundamental object of study in forensic science.

Mark, sign or object, the trace is

an apparent sign
(not always visible to the naked eye) that is

the vestige
> of a presence or
> of an action

at the location where this action took place.
The trace: a traditional definition

> The location where the action took place is often relevant
  > for traditional traces
  > in the physical world

but not really for digital ones (cloud computing)

> The concept of traces should be extended to events with
  > no action and
  > no specific presence

The trace: my revisited definition

> A trace is a modification
  > subsequently observable,
  > resulting from an event
The trace: my revisited definition

> The modification can be
  > an adjunction
  > a suppression
  > a transformation

Forensic science

Forensic science
> studies traces
  > Detection, observation and sampling
  > Identification, individualization and authentication of the source
  > Determination of the probative value

> as well as possible links between traces
  > Case study
  > Discovery of a series
  > Understanding networks and phenomena
Potential impact of digital forensics

> The **border** between
>  > the physical world and
>  > the virtual one
> becomes **fuzzy** in our modern Information Society

> Challenges related to digital evidence give an **opportunity**
>  > to **soften** traditional **barriers** between **forensic disciplines** and
>  > to **strengthen** forensic science itself

---

Forensic science

[Diagram showing overlapping circles for Law, Law enforcement, and Forensic science]

**A science in its own right**

**A science to support, in particular, the fight against crime**
Forensic science should not be confined to “court of law” requirements only.

The trace is the fundamental object to be studied in forensic science.

Extending our own domains of expertise to promote cross-disciplinary approaches seems necessary to handle complex criminal activities.
Illegal drugs markets: Criminal activities

> Combined approach
  
  physical world $\leftrightarrow$ Internet

> Optimisation of the ratio gain/risk
  > Cost reduction
  > Scalability
  > Minimization of the risks related to physical contacts/meetings

Illegal drugs markets: Forensic activities

> Regular snapshots of illegal marketplaces in the Darknet
> Analysis of specialized forums

> Ordering of illegal drugs samples

> Chemical analysis and profiling of received substances
> Analysis of the packaging, etc.
Digital traces

> allow a transversal and integrative approach

The global picture

Circumstances: Why? When? How often?
- Physical environment
  - Physical support of traces
  - Place
  - Crime scene
  - Implicated physical entities
- Virtual environment
  - Operating system
  - Chat room
  - P2P
  - Dark web
  - Implicated virtual entities


Criminal activity

Circumstances:
preconditions
motivation
context
Minimizing contextual information can prevent some forms of cognitive bias.

Eliminating all contextual information is a theoretical abstraction, irrelevant in practice.

Using contextual information can help to find the right questions, to get the relevant answers, and allow to link valuable information.

Information, context & confidence

- Uncertainty
- Info reliability
- Info quality
- Info quantity
- Confidence
Digital traces and context

A true forensic science is needed with
- a stronger scientific approach,
- a broader vision and
- a common unifying language

The digital paradigm gives us a unique opportunity
- to revisit traditional and fundamental concepts
- to develop further a true forensic science
- to strengthen the identity of forensic science itself

Conclusion
Thank you for your attention