Digital Forensics - Behind the Scenes

By

David-Olivier Jaquet-Chiffelle

Presented At

The Digital Forensic Research Conference

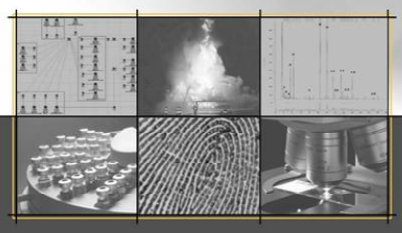
DFRWS 2015 EU Dublin, Ireland (Mar 23rd- 26th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

http:/dfrws.org

Digital Forensics: behind the scenes

David-Olivier JAQUET-CHIFFELLE
Full professor
ESC, University of Lausanne



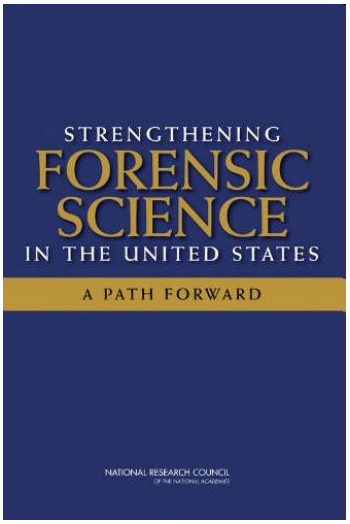
R. A. Reiss

DFRWS 2015
March 25th, 2015

ESC école des sciences criminelles

UNIL | Université de Lausanne

Forensic science on trial



ESC école des sciences criminelles

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

ESC école des sciences criminelles

Forensic science on trial

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

> 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 ?

ESC école des sciences criminelles

General trend

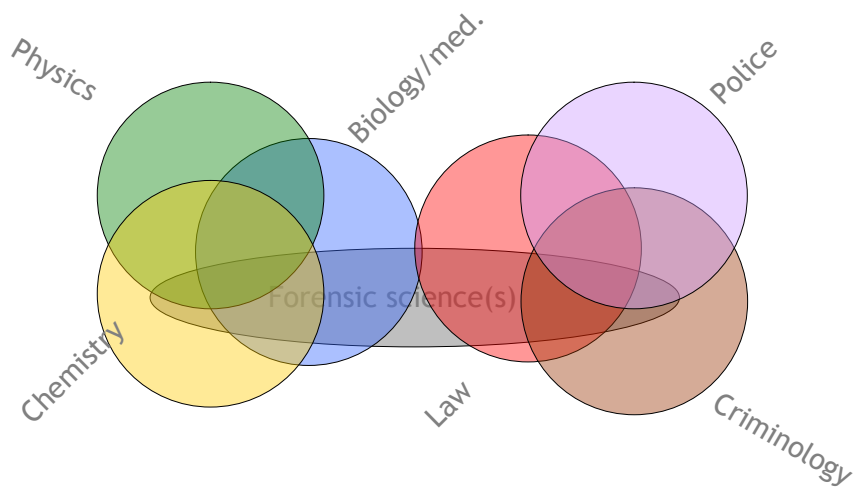
> To standardize methods and procedures

> To accredit labs and certify experts

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

ESC école des sciences criminelles

Forensic science(s)



ESC école des sciences criminelles

Duplication of the world of traces

> The digital domain

- > goes beyond a new discipline
- > creates a duplication of the world of traces

Analog domain	Digital domain
Film photography	Digital pictures
Handwritten signature	Digital signature
Safe	Crypto-algorithms
Paper files	Databases
(Snail) mail	E-mail

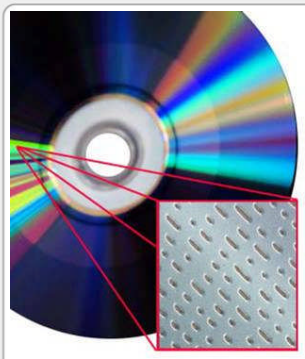
ESC école des sciences criminelles

The « real » world

« Real »	Analog
Physical	Most traditional traces
Virtual	e.g. testimony

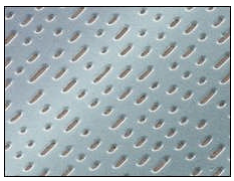
ESC école des sciences criminelles

Digital traces



> **Material**

physical digital traces



> **Abstract**

virtual digital traces

0 1

ESC école des sciences criminelles

The real world

« Real »	Analog	Digital
Physical	Most traditional traces	e.g. holes at the surface of a DVD
Virtual	e.g. testimony	Most traces in the information society

ESC école des sciences criminelles

New perspective

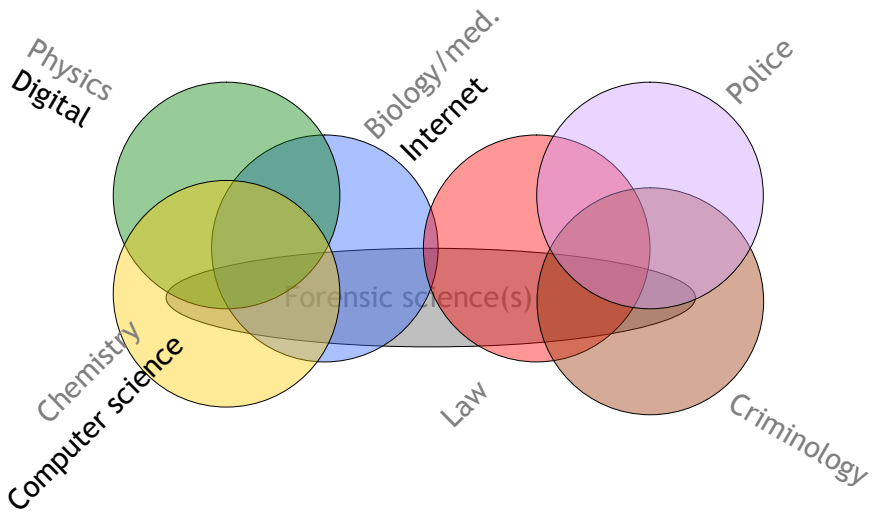
> Digital traces

> offer
> > a new perspective

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

ESC école des sciences criminelles

Forensic science(s)



ESC école des sciences criminelles

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

ESC école des sciences criminelles

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

ESC école des sciences criminelles

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

ESC école des sciences criminelles

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

ESC école des sciences criminelles

Lausanne school of forensic science

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

ESC école des sciences criminelles

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

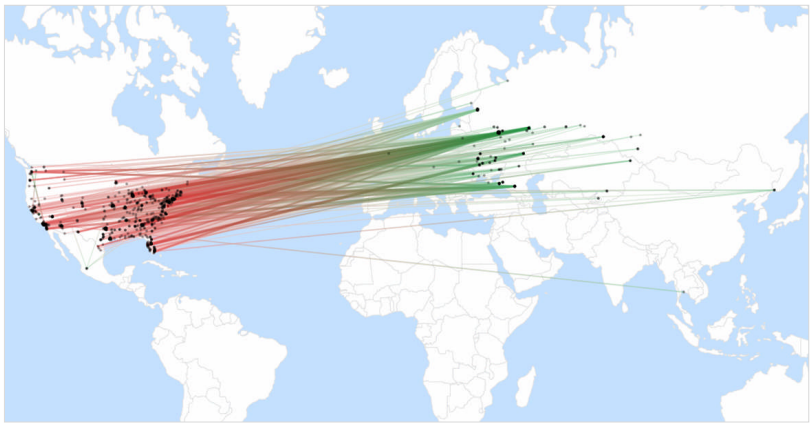
ESC école des sciences criminelles

Stolen credit card credentials

© Eudes

ESC école des sciences criminelles

Extent of the problem



- 1 label supplier
- 1767 labels
- Declared value : **US $ 275'328**
- 23 weeks of activities

© Eudes

ESC école des sciences criminelles

Lausanne school of forensic science

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

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

ESC école des sciences criminelles

The trace: a traditional definition

> 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

ESC école des sciences criminelles

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

ESC école des sciences criminelles

The trace: my revisited definition

> A **trace** is a modification
  > subsequently observable,
  > resulting from an event

ESC école des sciences criminelles

The trace: my revisited definition

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

ESC école des sciences criminelles

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

ESC école des sciences criminelles

Potential impact of digital forensics

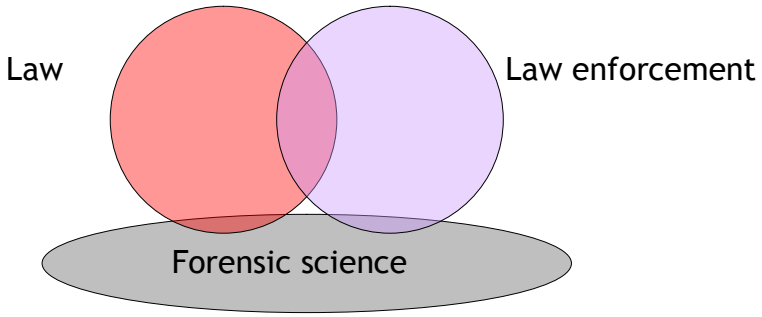
> The border between
  > the physical world and
  > the virtual one

  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

ESC école des sciences criminelles

Forensic science

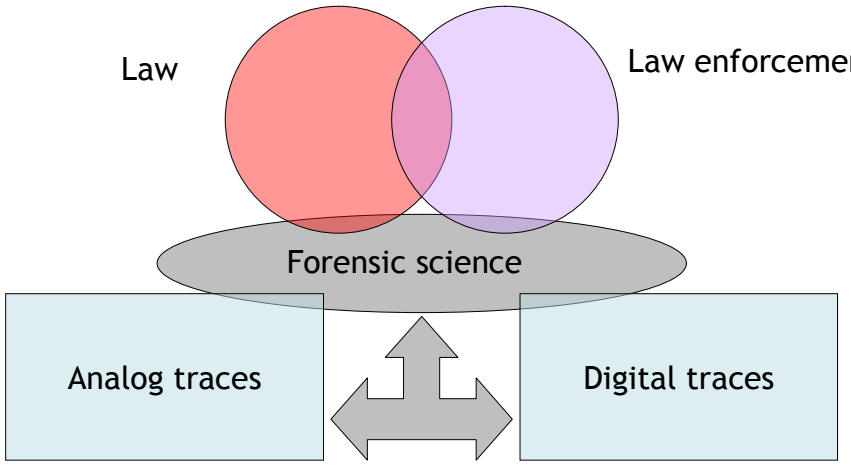


A science in its own right

A science to support, in particular, the fight against crime

ESC école des sciences criminelles

Forensic science



ESC école des sciences criminelles

Lausanne school of forensic science

> 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

ESC école des sciences criminelles

Illegal drugs markets: Criminal activities

> Combined approach

physical world ⟷ Internet

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

ESC école des sciences criminelles

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.

ESC école des sciences criminelles

Digital traces

> allow a transversal and integrative approach

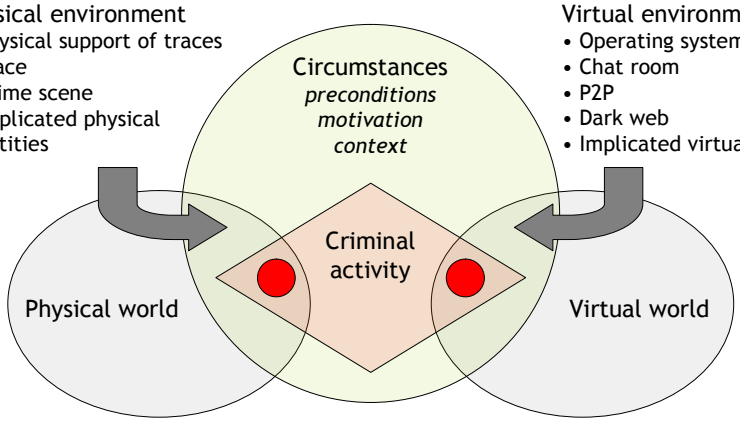
ESC école des sciences criminelles

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



Traces: Where ? What ? Who ? How ?

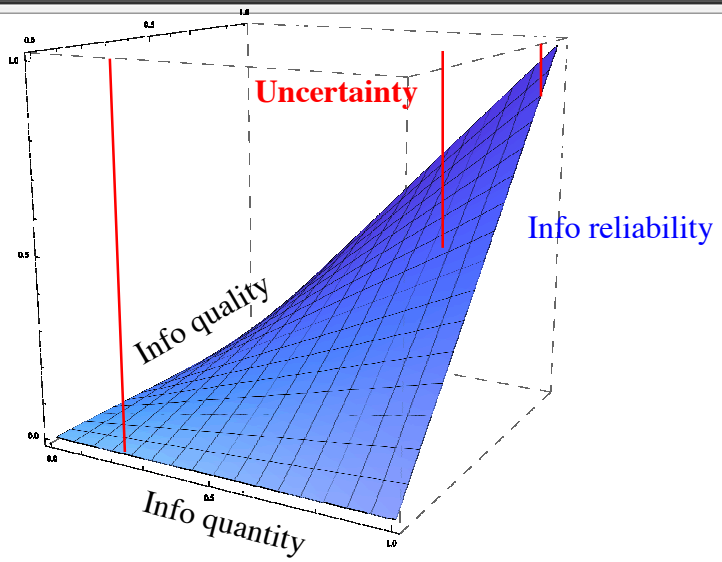
ESC école des sciences criminelles

Contextual information

- **Minimizing** contextual information can
  - prevent some forms of cognitive bias
- **Eliminating** all contextual information is
  - a theoritical abstraction, irrelevant in practice
- **Using** contextual information can
  - help
    - to find the right questions
    - to get the relevant answers
  - allow to link valuable information

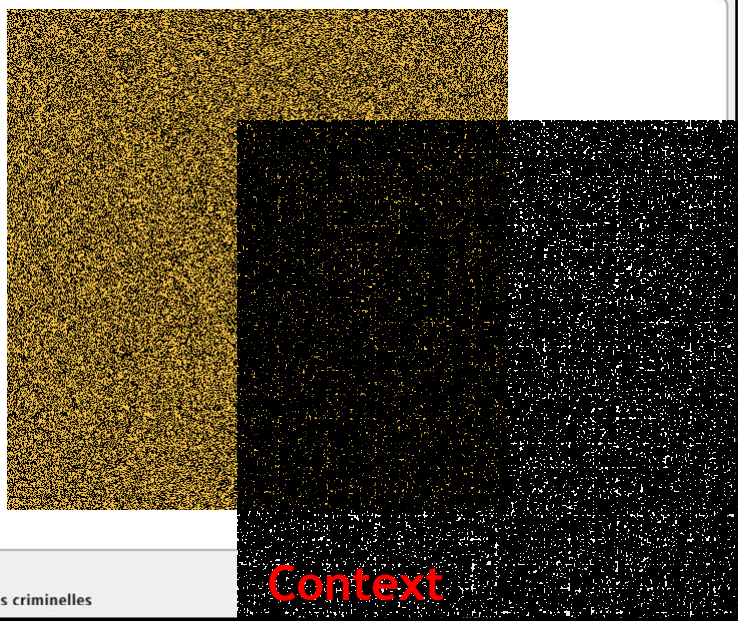
ESC école des sciences criminelles

Information, context & confidence



ESC école des sciences criminelles

Digital traces and context



ESC école des sciences criminelles

Conclusion

> Forensics science is in the line of fire

> 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 strenghten the identity of forensic science itself

ESC école des sciences criminelles

Thank you for you attention