Reliability of digital forensics for criminal investigations

Radina Stoykova – Adi

Dual PhD
University of Groningen, Faculty of law
Norwegian University of Science and Technology

Women in Forensic Computing

DFRWS EU 2022
28.03.2022, Oxford

https://www.essentialresearch.eu/

ESSENTIAL

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under the Marie Skłodowska-Curie Grant Agreement No. 722482.

What it means a ~~trial~~ *investigation* to be fair? (Art. 6 ECHR)

- Fair procedure to evaluate the lawfulness and the lawful use of evidence
- Possibility to challenge the evidence: fair disclosure of and to information about the evidence
- Maintaining equality of arms against technology-assisted expert evidence
- Accurate fact-finding
- Protection against prejudicial effects in evidence procedure

Source: simpson33 | Credit: Getty Images/iStockphoto

Encrochat

NETZPOLITIK.ORG

Wir sind spendenfinanziert. Unterstütze auch Du unsere Ar

dagensjuridik.se/debatt/debatt-encrobevisning-bor-avvisas-av-svenska-domstolar/

neter Näringsliv Krönikor Debatt Platsannonser DJ Play Legali

ONS

DEBATT: ”Encrobevisning bör avvisas av svenska domstolar”

Debatt

Publicerad: 2021-03-22 11:56

7006913f-be3d-49b5-8ba7-7c5b78b551b2

HOME WORLD US COMPANIES TECH MARKETS CLIMATE OPINION WORK & CAREERS LIFE & ARTS HOW TO

Europe + Add to myFT

Hundreds arrested across Europe as French police crack encrypted network

Drugs and weapons seized after investigators infiltrate EncroChat used by organised crime

Vorwurf Befugnis-Shopping

Streit um Encrochat-Ermittlungen vor

ComputerWeekly.com IT Management Industry Sectors Technology Topics

NEWS

Judges refuse EncroChat defe Supreme Court

Experts suggest Parliament and Investigatory Powers Tribunal need implications of a court decision on police use of data from the EncroChat phone

Actueel

altijd het laatste misdaadnieuws

crimesite

HOME LAATSTE NIEUWS UITGELICHT EXCLUSIEF VIDEO TIP ONS OVER ON

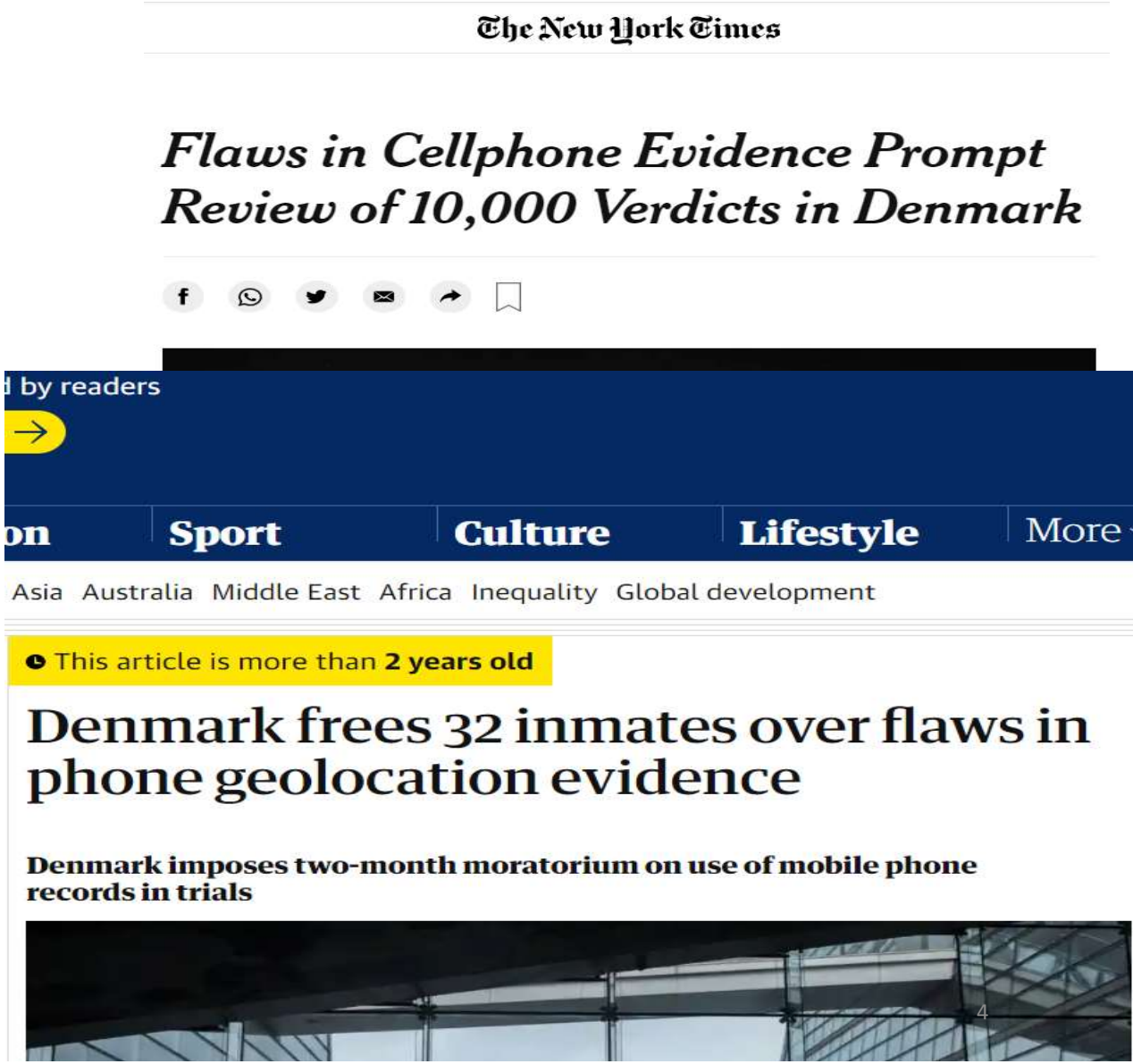
EncroChat: de reconstructie van de hack (UPDATE)

10 februari 2021

Om alle chats van alle gebruikers van communicatiesysteem EncroChat een paar maanden lang te kunnen meelezen heeft de Franse Gendarmerie vorig jaar één van de grootste hostingproviders van Europa bijna een uur platgelegd om daarin malware te kunnen installeren. Dat blijkt uit stukken van opsporingsonderzoeken in het Verenigd Koninkrijk, Frankrijk en Nederland die *Crimesite* heeft ingezien.

A Danish scandal

- How digital forensics capabilities are employed in law enforcement investigations?
- Validation of investigative tools and systems?



The New York Times

Flaws in Cellphone Evidence Prompt Review of 10,000 Verdicts in Denmark

d by readers

on | Sport | Culture | Lifestyle | More

Asia Australia Middle East Africa Inequality Global development

This article is more than **2 years old**

Denmark frees 32 inmates over flaws in phone geolocation evidence

Denmark imposes two-month moratorium on use of mobile phone records in trials

Meanwhile in The UK…

- 916 people had charges dropped
- Evidence not disclosed to the defense: ***increased by 70%***
- Prosecution unable to go through all the data

- Liam charged for over 2 years
- The case was dropped: *evidence on a computer disc - which* ***police had looked through*** *- showed messages from the alleged victim pestering him for "casual sex".*

bbc.com/news/uk-42795058

Liam Allan talks about what it is like being falsely accused of rape

The number of prosecutions in England and Wales that collapsed because of a failure by police or prosecutors to disclose evidence increased by 70% in the last two years, the BBC can reveal.

Last year, 916 people had charges dropped over a failure to disclose evidence - up from 537 in 2014-15.

Fair trial:
Key issues with Digital evidence

- **Encrochat:** need of international standards for digital evidence and better regulation of the investigation stage of criminal proceedings

- **The Danish scandal:** solutions for efficient compliance and enforcement of digital forensics standards in law enforcement work

- **Liam`s case:** ensure active defense rights and accountability in digital forensics?

How reliable is digital evidence?

Fingerprint	
FPR	0.1%
FNR	7.5%

FAIR TRIALS?

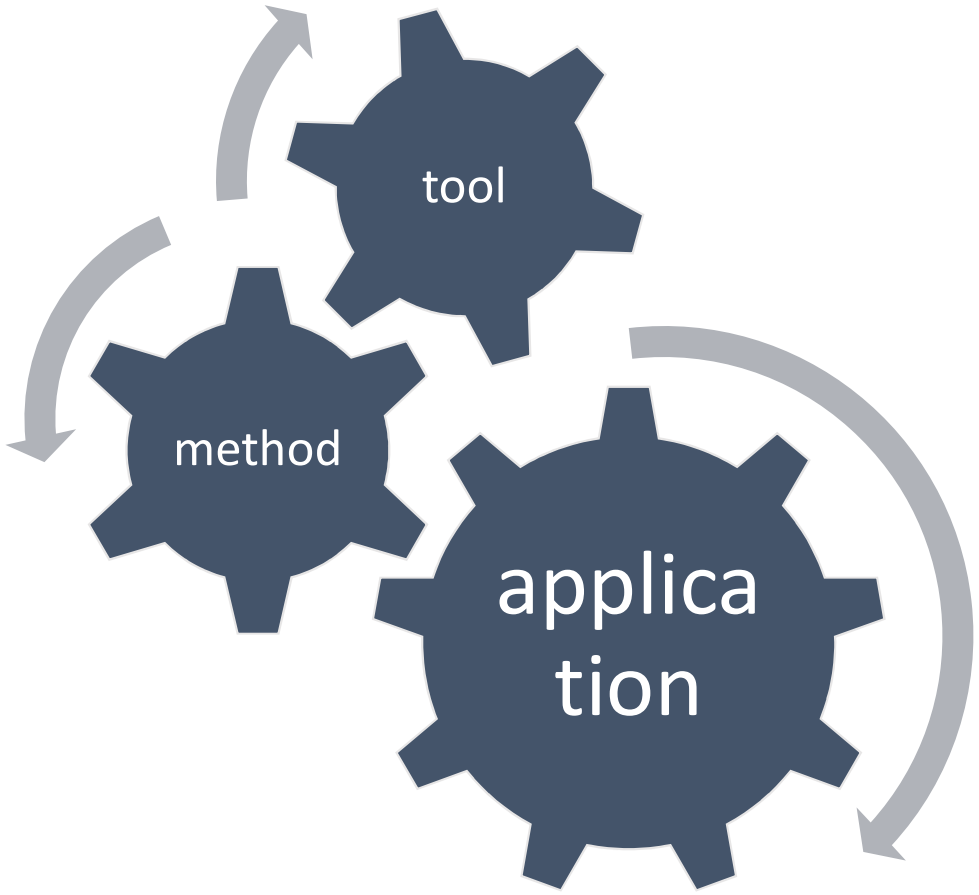
1. Digital Forensics & Practice

- Inappropriate and inconsistent use of technology
- Outdated validation schemas
- Ad hoc verification and tool dependencies
- Subjective human expert opinion
- Method and tool testing is resource consuming

2. Legislators, Standardization & Forensic Regulator Bodies

- Stricter requirements ….
- **Lack of implementation solutions!**

3-Steps Validation criteria

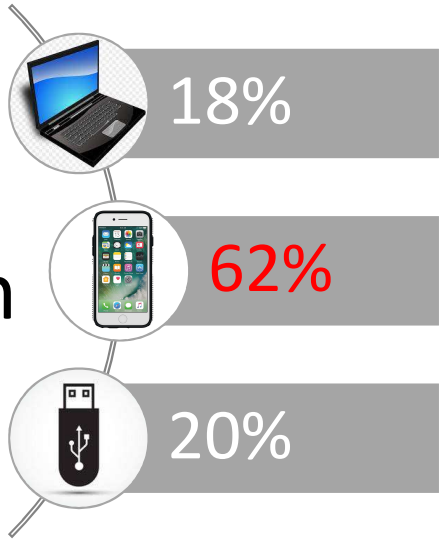


- **Automated Setup** (DF tool name, version, function used; known errors, prior validation; tool ability to report errors);
- **Method**(ref. peer reviewed method; established practice; previous work; pre-processing for input; algorithm and feature selection).
- **Application**(task (hypothesis, assumptions), data set, parameterization, output (separation of facts from inference);

CASE STUDY: Norwegian police (1)

Stoykova R, Andersen S, Franke K, Axelsson S, 'Reliability Assessment of Digital Forensic Investigations in the Norwegian Police' (2022) 40 Forensic Science International: Digital Investigation 301351.

- 21 randomly sampled cases
- 187 devices
- 3-step validation criteria + international DF standards



Number of devices	Acquisition reports	Examination reports	Analysis reports
71 (38%)			
32 (17%)	•		
40 (21%)		•	
0 (0%)			•
41 (23%)	•	•	
1 (1%)		•	•
1 (1%)	•		•
1 (1%)	•	•	•

CASE STUDY: Norwegian police (2) some results:

- Number of reports

Case type	Acquisition	Examination	Analysis	Content	Photography	Sum
Homicide	24 (35 %)	35 (50 %)	2 (3 %)	3 (4 %)	6 (9 %)	70
Sexual assault	7 (10 %)	32 (48 %)	1 (1 %)	23 (34 %)	4 (6 %)	67
Total	31 (23 %)	67 (49 %)	3 (2 %)	26 (19 %)	10 (7 %)	137

- Example of reliability assessment: acquisition reports

Reliability criteria	Yes	%	Partial	%	No	%
Mandate	13	18 %	50	68 %	11	15 %
Data source description	4	5 %	70	95 %	0	0 %
Tool description	17	23 %	38	51 %	18	24 %
Method description	0	0 %	55	74 %	18	24 %
Examiner	1	1 %	73	99 %	0	0 %
Acquisition results	2	3 %	51	69 %	21	28 %

CASE STUDY: Norwegian police (3) highlights:

- insufficient documentation to assess the reliability of the digital evidence.

- not possible to trace the digital forensic actions performed on each item or link the digital evidence to its source.
- none of the cases were shown to comply with digital forensic methodology, justify the methods and tools used, or validate tool results and error rates.

Conclusion & Way Forward

Women in Forensic Computing

- the intersection of law and digital forensics
- an unconventional career path
- an interdisciplinary niche for collaboration

THANK YOU FOR YOUR ATTENTION!

adi.stoykova@gmail.com