Towards Sound Forensic Arguments: *Structured Argumentation Applied to Digital Forensics Practice*

DFRWS EU 2020

Virginia N. L. Franqueira (v.franqueira@kent.ac.uk)

Graeme Horsman (g.horsman@tees.ac.uk)

University of Kent | Kent Interdisciplinary Research Centre in Cyber Security (KirCCS)

Teesside University

Context

- Digital forensics science
  - There has been a push – both in the domain of Forensic Science and of Digital Forensics – to increase *rigor*, *standardization* and *transparency* in practices and reporting

- Digital forensics practice
  - Practitioners have to deal with investigations which are ever more complex
  - Multiple elements have to be considered to address an investigation hypothesis

Problematic phenomena

- It is becoming increasingly **difficult to logically organise all key facts** of a given case to allow full and transparent scrutiny, and evaluation of the investigatory process by

  - the practitioner themselves
  - peers who may undertake review of the work
  - those involved with the wider investigation of the case

    (such as legal professionals, defence council, and jury)

This paper…

1. It proposes **Toulmin's structured argumentation** (Toulmin, 1958) as a practical and versatile mechanism for logical reconstruction
   - Helpful addition to forensic practitioners' thinking toolbox

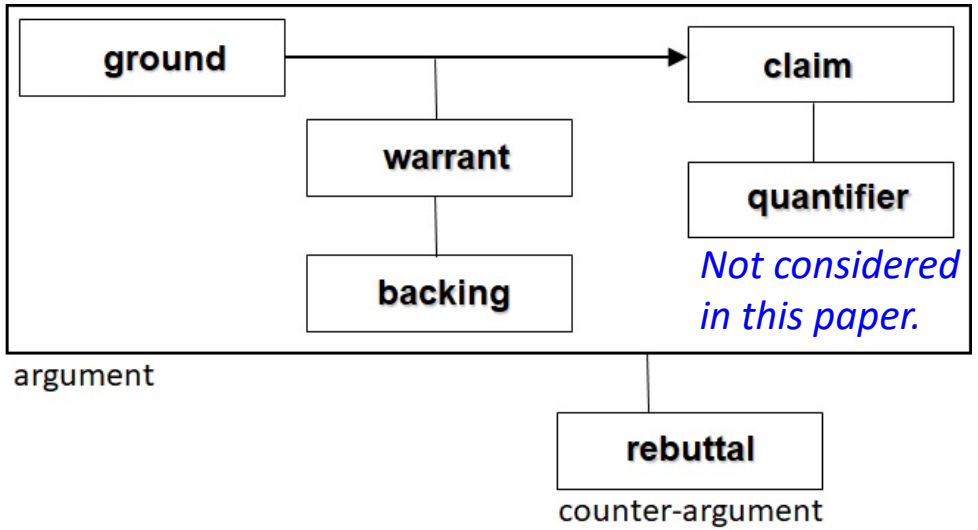
2. It illustrates Toulmin's model using *three case examples* that permit exploring its applicability in real world contexts

3. It elaborates on benefits and limitations of the proposed approach

S. E. Toulmin, *The Uses of Argument*, 1st Edition, Cambridge University Press, 1958.

Toulmins' structured argumentation (SA)

Toulmin proposed a layout for arguments composed of 6 elements



GROUND: *an evidence collected, a fact, a piece of information, data produced, a scientific finding, a legal precedent or an observation*

- gives support to a claim

CLAIM: *what is under evaluation, i.e., to be established as true or false*

- e.g., conclusion, decision, expert opinion, hypothesis

WARRANT: *inferential leap connecting a ground to a claim*

- i.e., a bridge-statement (e.g., cause/effect, empirical generalisation, common sense statement regarded as true)

BACKING: *adds credibility or authority to a warrant*

- e.g., laws, statistics, test results, regulations, standards, best practices

REBUTTAL: *counter-argument which diminishes confidence in a claim*

- e.g., exception, reservation, new fact, additional evidence, novel info
- it can "attack" a ground, a warrant and, occasionally, a backing

Case studies

We illustrate the application of structured argumentation to real world contexts using 3 example cases:

Case 1

- Cross-border case of advance-fee fraud involving a large number of victims

Case 2

- Murder case covered by the media in 2018

Case 3

- Fictitious sexual assault scenario introduced by Casey (2018)

E. Casey, Clearly Conveying Digital Forensic Results, *Digital Investigation* 24 (2018) 1-3.

Case 1

The defendant (suspect ‘X’) was arrested at his home address in the UK.

Several mobile phones, loose SIM cards, laptops, USB sticks, and paperwork containing PII & material related to fraud were seized from the address at the time of arrest.

Claims typical for advance-fee fraud cases.

each claim: true or false?

CLAIM 1	Suspect 'X' lifestyle not compliant with declared income.
CLAIM 2	Suspect 'X' had contact with victims.
CLAIM 3	Suspect 'X' had possession of fraudulent information.
CLAIM 4	Suspect 'X' had access to resources to facilitate fraud.
CLAIM 5	Suspect 'X' operated a money laundering scheme.

Refinement of claim 2.

initial argument from investigation

CLAIM 2	Suspect 'X' had contact with victims.
GROUND 1	Suspect 'x' had in his possession, at time of arrest, *n* mobile phones and *m* SIM cards.
GROUND 2	The phones and SIM cards seized contained reference to each other on contacts list.
WARRANT 1	The phones and SIM cards had recorded missed calls, received calls and contact entries of known victims.
WARRANT 2	The phones and SIM cards contained Western Union reference numbers associated with contact entries of known victims and money they transferred.
BACKING 1	Statistics show that Western Union and Money Gram are often used by criminals for fraudulent activities, i.e., send and receive money.
WARRANT 3	Some known victims handed over Western Union transfer forms used to send money with reference numbers which match with ones recovered from the phones and SIM cards seized.

counter-argument from suspect

REBUTTAL 1	Suspect 'X' affirmed in interview (after arrest) that only one phone seized was owned by him and it was received as a gift one year before being seized.

counter-arguments to rebuttal 1

REBUTTAL 2	All phones and SIM cards had contact entries, photos and emails of family members of suspect 'X', dated prior to one year before being seized.
REBUTTAL 3	All phones and SIM cards contained photos showing suspect 'X' with associates (gang agents), dated prior to one year before being seized.
BACKING 2	Upon testing, photos with family members and with associates contained in the examined phones and SIM cards did not show signs of tampering or of being downloaded..
REBUTTAL 4	While 'search and seize' at suspect's 'X' address.was taking place, officers asked suspect 'X' about the phones and SIM cards: "Are they all yours?"; the suspect replied "Yes".

>>>> they restore confidence in the original argument

Case 2

Murder case where defendant Mr Patel (suspect ‘X’) allegedly killed his wife (victim ‘Y’).

BBC | Your account | News | Sport | Weather | iPlayer | Sounds

NEWS

Home | UK | World | Business | Politics | Tech | Science | Health | Family & Education

England | Local News | Regions | Tees

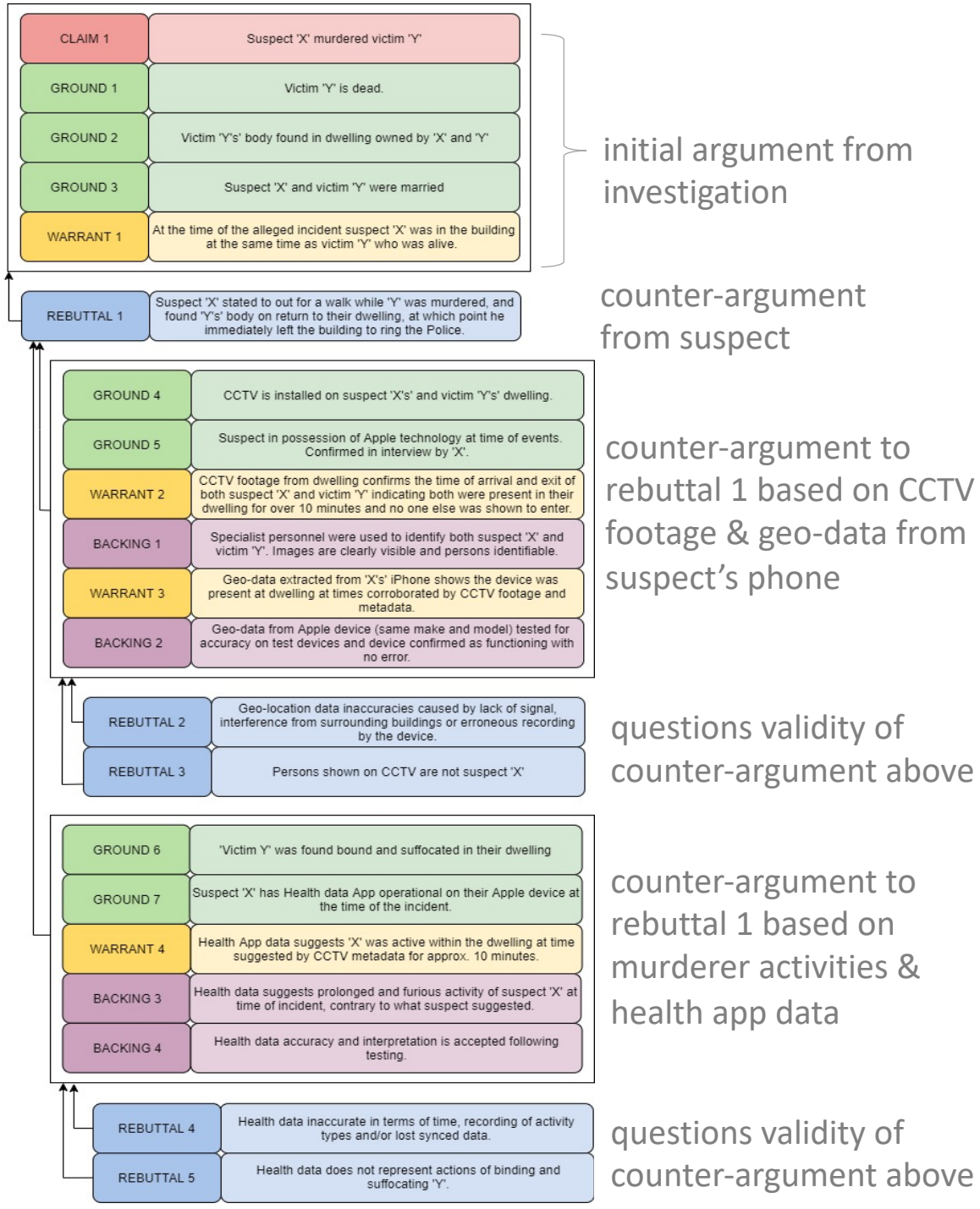
Grindr cheat pharmacist claims murdered wife was 'best mate'

26 November 2018 Share

FAMILY PHOTO

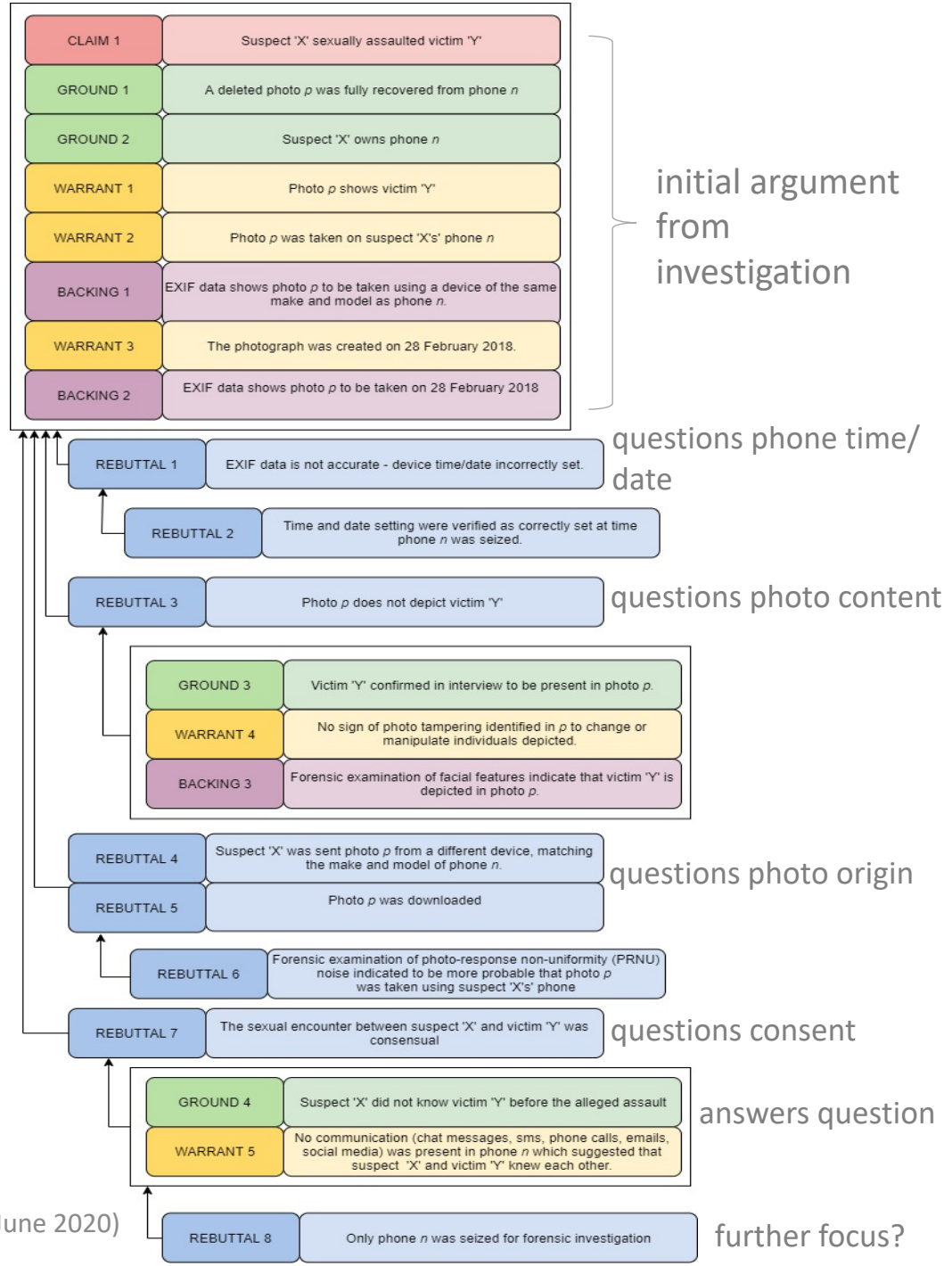
Jessica Patel had been strangled and suffocated with a Tesco Bag For Life

A man accused of murdering his wife so he could start a new life with his male lover told detectives he loved her and she was his "best mate", a court heard.



Case 3

Case of an alleged sexual assault committed by suspect ‘X’ against victim ‘Y’.



Discussion – potential benefits of SA

- Decipher-ability
- Logical Reconstruction
- Peer Review
- Jury Interpretation
- Error Detection

Discussion – potential benefits of SA

- Flexibility
  - can be used *during* or *after* the process of investigation
  - can be used at different levels of abstraction and granularity
  - can serve different purposes
    - case 1: refinement of claims as building blocks for logical reconstruction
    - cases 2 & 3: hypothesis elaboration, falsification, considering defence council arguments
  - apply to any type of case

Discussion – potential limitations of SA

- Quality of Argumentation
  - often discussed aspects affecting quality of SA in general are convincingness, soundness, and completeness of arguments / counter-arguments

- Risks
  - risk involved in: too much details leading to “combinatorial explosion“
  - risk exposed by: unacknowledged rebuttals

Discussion – potential limitations of SA

- Overhead of Argumentation
  - *Learning curve? Time consuming? Effort draining?*

  - yes, there is a learning curve to understand the basic rules and gain practice
  - but:
    - no specialised background (theoretical or mathematical) is required
    - it draws from *inferences* that forensic practitioners already make during their work (mostly subconsciously)

    >> *short training should suffice*

Conclusion

- SA has the potential to become a very *practical tool* to support practitioners all the way through their investigations
- Despite the need for further empirical evaluation, the proposed SA method indicated several relevant benefits *aligned with the push for a more science-oriented model* for DF investigations
  - transparency
  - accountability
  - accessibility

Related work (structured argumentation)

- It has been applied extensively in Computing to build confidence on a target audience that the conclusion reached is justifiably true, e.g.:
  - to build safety cases & dependability cases
  - to demonstrate compliance to laws and regulations
  - to establish confidence in software development
  - to show satisfaction to security requirements
  - to expose threads of risks/mitigations for risk assessment

- In fields indirectly related to forensics, it has been used, e.g.:
  - to help decision making aiming at transparent accountability in cases of child protection
  - to validate claims about offenders' profiles

- In the field of DF, it has been used scarcely, e.g.:
  - to expose a claim in a child abuse imagery case and validate it (Boddington, 2012)
  - to evaluate forensic readiness for incident response purposes (Pasquale et al., 2013)