Digital Evidence Strategy

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

Teesside University

Introduction

- Digital evidence is important in many inquiries.
- Reliance on devices means the data they maintain can describe events where no other information may be present
  - *'Digital Witness'*
- It is important that we are able to identify, capture and interpret all **relevant** and available information which can support an inquiry. **BUT, that we limit interaction with redundant data.**
  - For purposes of investigation **efficiency, interpretation (or preventing misinterpretation) and privacy protection.**

- This requires a '*digital evidence strategy*'.

Pollitt (2013) - ...we can no longer look at every single file on a device...

But why?

….resource issues? time, deadlines, swift & appropriate justice, ***necessity/proportionality****.*

‘It is important that investigators develop appropriate strategies to identify the existence of digital evidence and to secure and interpret that evidence throughout their investigation’ (ACPO, 2012 p.9).

‘Due to the volume and complexity of data stored on digital devices, it is not possible or desirable to extract all data held on a device for review by investigators. Instead, a forensic strategy needs to be formulated to enable the examination to be focused on the relevant data’ (ACPO, 2012 p.11).

Important

- Digital investigations should not be an exercise of '*look and see*'. There are a number of reasons for this, which arguably largely fall into one of two categories:-
  - **Investigation/inquiry success.**
  - **Impact upon those involved.**

- Just as we see in more traditional forensic science inquiries, a digital inquiry should be structured and driven appropriately in line with the needs of the case.

- These '*needs*' require prior identification and evaluation for suitability.
  - How we do this assessment is arguably a current challenge, where protocols must be in place to ensure both quality and consistency of practice.

Digital Evidence Strategy (DES)

- What is it?...there are multiple elements to it

  '*An **agreed, defensible, and dynamic** plan that identifies those **investigative actions** which are deemed both **proportionate and necessary** to establish the potential **existence and meaning** of any available and **relevant digital information** that can assist with any/all **reasonable lines of inquiry**. This plan must **define and justify the scope of any investigative actions,** outline all known **procedural limitations and risks which could impact upon the success of a case outcome and how they will be managed/mitigated**, along with consideration of **applicable legal, ethical and professional factors**.'*

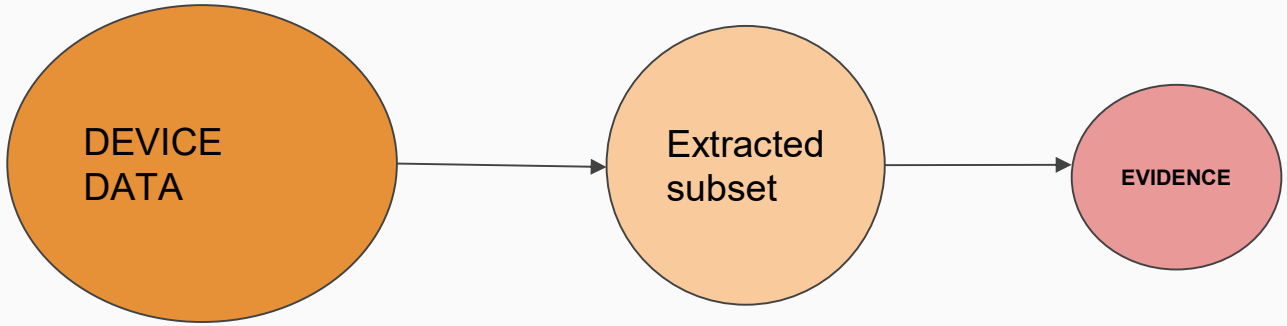
- It should map across the stages of a DF workflow - 'Crime scene to court' and all that sits in between.

No DES means….

1. Inconsistency of approach
2. *Ad hoc* processing…..driven by what…..?
3. Increased risk of unsuccessful case outcomes?
    a. But what is a successful outcome?
4. Prevention of proper evaluation of investigator actions
    a. What have you done and why?
5. Inefficiency
6. Lack of accountability

A bad DES means...

- Our inquiries are wide of the mark.
- Impact upon victims and suspect.



Building a DES

Probably a combination of all three, right?...

- If we take a minute to think about what drives our decisions to develop a DES?

1. Offence related?
    - Those aspects of an offence we know/believe to exist?
    - Limitations? - us, the practitioner? Our knowledge?

1. ‘Jump in, swim out’ (hopefully)?
    - Start looking for relevant trails?
    - Impact - privacy where it moight to too late to avoid.

1. Informed approach?
    - What do we know and why do we know it? How reliable is this info?

DESs support quality review checks

- A DES not only structures an approach to an investigation but also serves as a support for those who evaluate/peer review the work.
- We often don’t ‘redo’ a case.
- Peer review can be facilitate and supported by the narrative that the practitioner provides.
- If this is formally documented and available, it provides greater access to what has been done, why and how.
  - Error detection increases?
  - Easier to suggest improvements to the examination?

Starting at the scene...

Starting at the Scene...

For a digital device to have value, it must contain information which supports an investigative inquiry above and beyond what is already known, or corroborates a series of events which are in need of confirmation.

Upon entering a crime scene, first responders should acknowledge the following series of fundamental questions in regards to their scene processing and investigation and digital evidence:-

1. Does the scene contain or is likely to contain a ‘digital presence’?
2. What does the existence of any digital device at the scene mean?
3. What could the device contain which would be of value to the investigation?
4. Do I need that device and why?

'*Evaluating*' the device

Do we need this device and how does it help us with our inquiry?

Horsman, G., 2021. Decision support for first responders and digital device prioritisation. Forensic Science International: Digital Investigation, 38, p.301219.

Question 1 - 'what is the severity of the alleged offence?'

Question 2 - 'why do you need the data (consider necessity and proportionality)?'

Question 3 - 'what is the potential 'solvability' of inquiry through access to data?'

Question 4 - 'do you know if the data can technically exist?'

Question 5 - 'how strongly do you believe that relevant data about the offence exists?'

Question 6 - 'what role is the device believed to play in the inquiry?'

A minute on ‘privacy’

R v Bater James and Mohammed [2020] at 70 EWCA Crim 790 -

it is stated that for the formation of a reasonable line of inquiry is ‘not dependent on formal evidence in the sense of witness statements or documentary material, but there must be a reasonable foundation for the inquiry’. Support for determining a reasonable line of inquiry is provided by the CPS (2018).

Important that a DES now strongly considers privacy preservation as a fundamental investigatory concept.

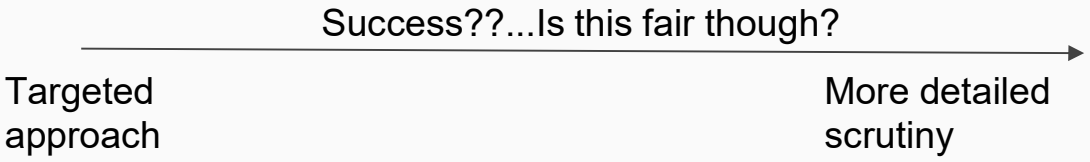
- We know that digital evidence can offer support for our inquiries, but the depth of description provided by this data means often non-relevant data is captured and possibly reviewed.
- How do we develop a DES that limits this - a key research question moving forward.
- We have seen both the ICO and College of Policing pass comment on this.
- A balancing act between privacy and effective investigation.

‘In cases where allegations are unproven, these must be managed to allow those individuals to return as close to the position which they resided prior to the investigation’

(Croft and Olivier, 2010 p.96).

Objectively defining criteria

- If we consider that we want to try and get a good precision and recall approach to potential ‘evidence’ recovery, then risk is involved.
- We have to accept that we will not get this right all of the time…
- So, in the development of a DES, we need to define criteria which describe/justify actions and the scope of their deployment.
- This allows retrospective audit - transparency.



We need principles which sit at the examination level and provide more support/detail regarding privacy preserving conduct.

A ‘check point approach’ - some basic **principles**

Making sure we take one step at a time to prevent ‘over analysis’

- The scope of any investigation should be defined and evaluated prior to its implementation for the purpose of ensuring that it is both **proportionate** and **justifiable** in terms of **breadth and depth** in order to be able to **effectively pursue any reasonable lines of enquiry**. In all cases, steps to reduce privacy invasion should be taken where possible and appropriate, and these measures should be evidenced.

- The extraction and examination of all available digital data from a given device or set of devices should be reserved for cases where there is a real risk that using targeted approaches for data extraction and examination may compromise the purpose of an investigation.

- Is it possible to define the ‘minimum point of inquiry’ needed in a specific case? - arguably this is the ideal situation.
    - **In reality, risky and difficult.**

BUT

- A DES should be designed with privacy protection in mind. However...
- The DES must be dynamic - shifting if and when required
  - JUSTIFIABLY and this need evaluated
- Those conducting an investigation of a device should acknowledge when an investigation threshold has been met and prevent further probative work.
  - Meaning - a threshold must be defined from the beginning where possible.
- ‘Full data’ scrutiny should not be prevented - but it must be justified.
- Consistency in approach - doing the same thing in the same circumstances
  - If possible?!
  - Case-specific Vs offence specific possibility.

Developing a DES

Stages of development

1. What is both relevant and known about any suspected action(s)/offence?

- Of this information, what is considered to be reliable?
- Of this information, what is considered to be ‘speculative’ where accuracy is unknown/unverifiable?
- How does this information translate into suspected digital actions?

1. What are those actions which are subject to inquiry?

1. What are the investigative questions which require answering **AND HOW**?

1. Proportionality and justifiability of actions undertaken?

1. Risk of investigative actions taken and the management of it?

1. Evaluation and acceptance of DES?

- A DES should be considered a collaborative construction.

DES & Screening

Examining data in line with the needs of an inquiry

How to know what to look for and how to do it?

Analysts may deploy computational 'data-screening' mechanisms designed to target any subset of data which may exist on a device deemed likely to contain information of worth to those involved in an investigation. These include approaches such as keyword searching, timelining digital artefacts or targetting known file types. Screening as an investigative technique, therefore, aims to reduce the quantity of data that a practitioner must interpret, however, as with any process which attempts to automatically sift and identify useful data, risks exist with regards to their effective configuration and deployment.

Questions to address when deploying & justifying a DES

Not just individually, but as a field. How do we learn going forward?

1. How are we screening?

1. Why do we screen the way we do - what drives the decision making?

1. How do we know if we are screening effectively
    a. Have we missed something or was it not there?

1. Who screens best - are we consistent?

1. How is screening evaluated?

DES Risks

- How is data found interpreted?
- Tool use and deployment.
  - Do we understand the tools we are using & can we trust them?
- Where do we draw the line?

Questions

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