Digital Evidence Dashboard

The organisation of digital forensics in investigations

Hans Henseler* and Adrie Stander**

DFRWS EU 2016, March 29-31 2016
Lausanne, Switzerland

* Amsterdam University of Applied Sciences & Tracks Inspector
** University of Cape Town
A collaboration between:

Project members:
- tracksinspector
digital forensics for investigators
- TNO
innovation for life
- in-pact
Samen voor veiligheid

Involved:
- Inspectie SZW
Ministerie van Sociale Zaken en Werkgelegenheid
- Politie
Oost-Nederland
Noord-West Holland
Den Haag
- Politie
Politieacademie
- Koninklijke Marechaussee

This project has been made possible by the Municipality of The Hague and the Hague Security Delta.
Why did we do this project?

• Enormous growth of data per device

• Growth of number of devices per person and location

• Growing volume of digital case data

• Limited capacity for investigations

Solution: Enable All detectives to investigate digital evidence.
Project goals: realise ...

• An overview of alternative working ways (process organisation, assignment of tasks)

• Present information in a non-technical manner: dashboard with a simple interface.

• Support continuous reporting and progress monitoring.

• Facilitate collaboration between detectives and experts.
Project approach

**Explore**
- Ways to improve and change working processes and responsibilities.
- Desired / required functionality

**Design**
- Concepts for the DED
- (Screen)designs (“Powerpoint”)

**Ontwikkelfase**
- Software DED in Tracks Inspector
- Proof of Concept: website and demonstration case
## Scope DED

<table>
<thead>
<tr>
<th>'Fast response’</th>
<th>‘Normal’ adversary</th>
<th>‘Expert’ adversary</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Live investigation with consent of suspect</td>
<td>• No or little digital expertise</td>
<td>• Hidden information and booby traps more likely</td>
</tr>
<tr>
<td>• No (initial) seizure of evidence</td>
<td>• At most deleted files</td>
<td>• For instance organised fraud, child pornography, computer crime</td>
</tr>
<tr>
<td>• Police report is sufficient for prosecutor</td>
<td>• Acquire forensic copy or image of evidence</td>
<td>• Requires specialist knowledge and tools</td>
</tr>
<tr>
<td>• Forensic image as source of the investigation</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Everyone

Digital evidence dashboard

### Detective

In-pact

### Digital forensics expert

TNO innovation for life

Tracksinspector digital forensics for investigators
Digital investigation processes

**Forensic preparation**
- Prepare devices
- Make forensic copy
- Back-up & archiving
- Setup case

**Case configuration**
- Authorizations
- Legal privilege review
- Formulate investigation questions

**Investigation**
- Investigate digital data
- Investigate specialist questions (by expert)
- Reporting
Different variations in processes

• In large and middle large organisations: detective doesn’t play any role at all \textit{without digital expert}.

• Local law enforcement is suffering from delays due to \textit{distance and back logs}. This is a “Bottleneck”

• Small organisations are completely \textit{self-supporting}, but are taking risks. They have no support at all from digital experts.
Implementation choices

Focus on **efficiency** in terms of:

- Distance between detective and expert
- Reducing turn-around time

Also focus on **content**:

- **Understanding the case & context** is necessary for the investigation
- When using the DED: **roles and job separation**
  (e.g. ‘case manager’ role, legal privilege review, technical preparation, investigation question set, etc.)
Organisational choices

2 choices: exist for locally organising the investigation of digital materials:

• Organise digital expertise close to the process (but is there enough capacity?)

• Enable detectives so that they can perform digital investigations themselves:
  • This is what the Digital Evidence Dashboard is intended for
  • Requires (some) training
Interesting facts about investigations

- At the start
  - **Verification cases** (eg. a known story that needs to be verified)
  - **Search cases** (eg. a victim with an unknown story)

This was used as guidance for the concepts and the design
Interesting facts about investigations

• **Fear** to destroy evidence (by accident)

• **Clues** are not (yet) evidence

• Detectives seem restrained in their *report narrative* when digital media is involved

Causes:  - **Limited skills**,  
- **Attitude** towards digital media
(Part of the) Solution

Non-technical detectives should (also) investigate digital media:

1. Increase investigation capacity
2. Get results faster
3. Aim for bulk cases (no expert ‘adversary’)
4. Look for clues (that are relevant for the entire investigation)

Threats:
• Lacking ICT-knowledge / aversion
• Fear of making mistakes/ unable to find information
• Draw premature conclusions

Opportunities:
• Being involved directly increases efficiency & effectiveness
• Investigation by expert is still possible
Design Goals: The DED enables...

... the case manager to oversee the digital investigation so that he can monitor the progress more easily and adjust the investigation in a timely manner.

... the detective to perform perform the investigation in an independent manner so that he can prioritize, search, analyse and record findings.

... the digital expert to be involved in a natural way on complex and relevant digital issues so that his expertise is used in the most efficient way.

... the investigation team to conduct the investigation of digital media and collaborate in order to have the process run smoothly and quickly.
DED building blocks

Keeping Oversight

“Digital case dashboard”

Analysing Data

“Evidence locker”

Recording Findings

“Drawing board”

Detectives collaborate with each other and with digital experts
Storyboard
Using the functions in the Digital Evidence Dashboard
Formulate investigation questions

Investigation Questions

Case info

Teaminfo

Detector
Refine Search results

Search digital media

FILTER

Search Term  Location  DATE  ....

Refine Search results

BLACKBERRY

36  3
0  112
14  50

....  ....  ....  ....

DED digital evidence dashboard

i-n-pact  TNO innovation for life

tracksinspector digital forensics for investigators
Investigation Question 3

Recording
Findings
<table>
<thead>
<tr>
<th>Investigation Questions</th>
<th>✓</th>
<th>+</th>
</tr>
</thead>
<tbody>
<tr>
<td>_______________________</td>
<td>✓</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>_______________________</td>
<td></td>
<td>DONE</td>
</tr>
<tr>
<td>_______________________</td>
<td></td>
<td>ACTIVE</td>
</tr>
<tr>
<td>_______________________</td>
<td></td>
<td>ACTIVE</td>
</tr>
<tr>
<td>_______________________</td>
<td></td>
<td>DONE</td>
</tr>
</tbody>
</table>

Progress & briefing
Evaluation

Multiple workshops with end users

Judging: Effectiveness, efficiency, working processes and points for improvement

Feedback via questionnaires, discussion & assignments
Feedback from end users

As a case manager you stay informed about searches, make adjustments and add new questions. Great!

Handy! I can put away my little notebook

Very clear. I can see what’s on there in no time.

As an expert I look in exactly the same system that the detective is referring to. We are on the same page!

Entities and analysis are notoriously difficult areas. The DED adds value because it offers easy to understand investigation questions and dashboards.
Demonstration website

https://www.digitalevidencedashboard.com

- DED video
- Login to prototype
- Simple verification case scenario
Thank you
j.henseler@hva.nl
adrie.stander@uct.ac.za