Digital triage of data evidence for suspect interview

Transforms the digital scene capability focusing on both training and environment. It also strives to understand the digital demand workflow in Bedfordshire Police and how best to meet this demand.

First published
7 June 2023

Key details

Does it work?	Untested – new or innovative
Focus	Organisational
Topic	Criminal justice Digital Intelligence and investigation
Organisation	Bedfordshire Police
HMICFRS inspection report	**An inspection into how well the police and other agencies use digital forensics in their investigations**
Contact	Peter Ward
Email address	Peter.ward@beds.police.uk
Region	Eastern
Partners	Private sector
Stage of practice	The practice is implemented.

Key details

Start date	May 2018
Completion date	June 2019
Scale of initiative	Local
Target group	Offenders Victims

Aim

The aims were:

- Reduce current digital backlog causing delays in criminal justice outcomes.
- Examine and eliminate digital devices belonging to family members of suspect.
- Obtain swift evidential attributed evidence from suspect device and make available to interview team for first suspect interview.
- Professionalise the Digital Media Investigator (DMI) working environment, removing risks associated with working inside suspect address.
- Future-proof the digital scene capability harnessing all available volatile and cloud-based digital evidence that cannot be obtained via the traditional methodology of 'dead boxed forensics'.

Intended outcome

The intended outcomes were:

- A reduction in a two-year digital backlog that was causing delays in the criminal justice system and posing significant risks in terms of the availability of data at the point of examination, due to attrition risks caused by time delays.
- Obtain an increase in anticipated guilty pleas from suspects, due to the early availability of attributed data obtained from suspect devices on the day of arrest.
- Professionalise the working environment of DMIs operating at crime scenes, by providing a stable, repeatable, mobile lab-based environment that could meet the future challenges of International

Organisation for Standardization (ISO) accreditation.

Description

The DMI Team identified that the model prior to May 2018 revolved around the seizure of 10-30 digital devices following the arrest of a suspect. Often, this meant ignoring volatile data opportunities, along with not recognising the issues of cloud-based data availability, and the issue of encryption once a device is switched off. They also recognised by scanning the previous year's data, that over 60% of the seized devices examined were non-evidential, and likely to be used by family members, and not the suspect.

Clearly a methodology was needed that afforded the DMIs to spend longer at scene, and instead of switching off and seizing, using systematic methods to triage/examine devices with a view to eliminating at scene those belonging to family members that yielded no evidential value. The other main undertaking based on a 'dual deployment' DMI model, would focus on the main attributed handset belonging to the suspect to enable a fast turnaround of an evidential package, which could be placed in front of the interview team for the first suspect interview.

To enable both of these functions, we had to find a controlled environment that wasn't the suspect's lounge.

A suggested model revolved around taking a blank canvas transit van and retrofitting it to produce a professionalised working environment that could be controlled, aka the Beds 'Cyber Triage Vans'. The funding for Van 1 came from an innovation bid to the then Beds PCC, which was supported to the value of £50k. Van 1 was purchased from Peugeot having completed a transparent procurement exercise and was then retrofitted by a local company again via another procurement exercise. The costs for initial purchase were £18k, and the retrofit came in approximately £27k.

Evaluation

The evaluation took place over 12 months and involved tracking the monthly impact of the DMI at each and every scene, including:

- how long they spent at the scene in hours
- how many devices were examined
- how many were evidential

- how many were eliminated
- the type of devices examined
- how many suspect extractions were produced and handed to the officer in charge (OIC) on the same day
- what was the impact of more devices being examined at the scene on the Digital Forensic Unit (DFU) backlog

The evaluation revealed a significant reduction in the DFU backlog from over two years to under six months.

Staff surveys and feedback identified significant productivity gains in both output and wellbeing in terms of recognising their contribution and the accompanying risks of operating in the suspect's address.

Overall impact

- It reduced the DFU overall digital backlog from two years to six months. This has since been reduced further by the introduction of three further 'Cyber Triage Vans' and an increase in the DMI staffing model.
- It reduced the timescale for criminal justice prosecutions, ensuring that digital device examinations could no longer be quoted and blamed for criminal justice backlogs and cases failing.
- It demonstrated a commitment to the professionalisation and wellbeing of DMI practitioners.

Learning

- ISO Accreditation being used as a blocker internally due to internal policing politics. Importantly it was not sighted as a potential problem or insurmountable issue by the forensic regulator who was engaged for advice.
- It is important to track your performance and data metrics right from the word go.
- Prepare your Standard Operating Procedures (SOPs) to demonstrate and acknowledge how you intend to operate at the scene.
- Invest and financially plan and commit to a training package and pathway that mirrors that of a force DFU.

Copyright

Legal Disclaimer

Disclaimer: The views, information or opinions expressed in this shared practice example are the author's own and do not necessarily reflect the official policy or views of the College of Policing or the organisations involved.