



LEEDS
BECKETT
UNIVERSITY

Citation:

Schreuders, ZC and Smith, V (2017) Police Knowledge Fund Showcase: CARI Project. In: Police Knowledge Fund Showcase, Coventry, UK.

Link to Leeds Beckett Repository record:

<https://eprints.leedsbeckett.ac.uk/id/eprint/5080/>

Document Version:

Conference or Workshop Item (Published Version)

The aim of the Leeds Beckett Repository is to provide open access to our research, as required by funder policies and permitted by publishers and copyright law.

The Leeds Beckett repository holds a wide range of publications, each of which has been checked for copyright and the relevant embargo period has been applied by the Research Services team.

We operate on a standard take-down policy. If you are the author or publisher of an output and you would like it removed from the repository, please [contact us](#) and we will investigate on a case-by-case basis.

Each thesis in the repository has been cleared where necessary by the author for third party copyright. If you would like a thesis to be removed from the repository or believe there is an issue with copyright, please contact us on openaccess@leedsbeckett.ac.uk and we will investigate on a case-by-case basis.



CARI Project



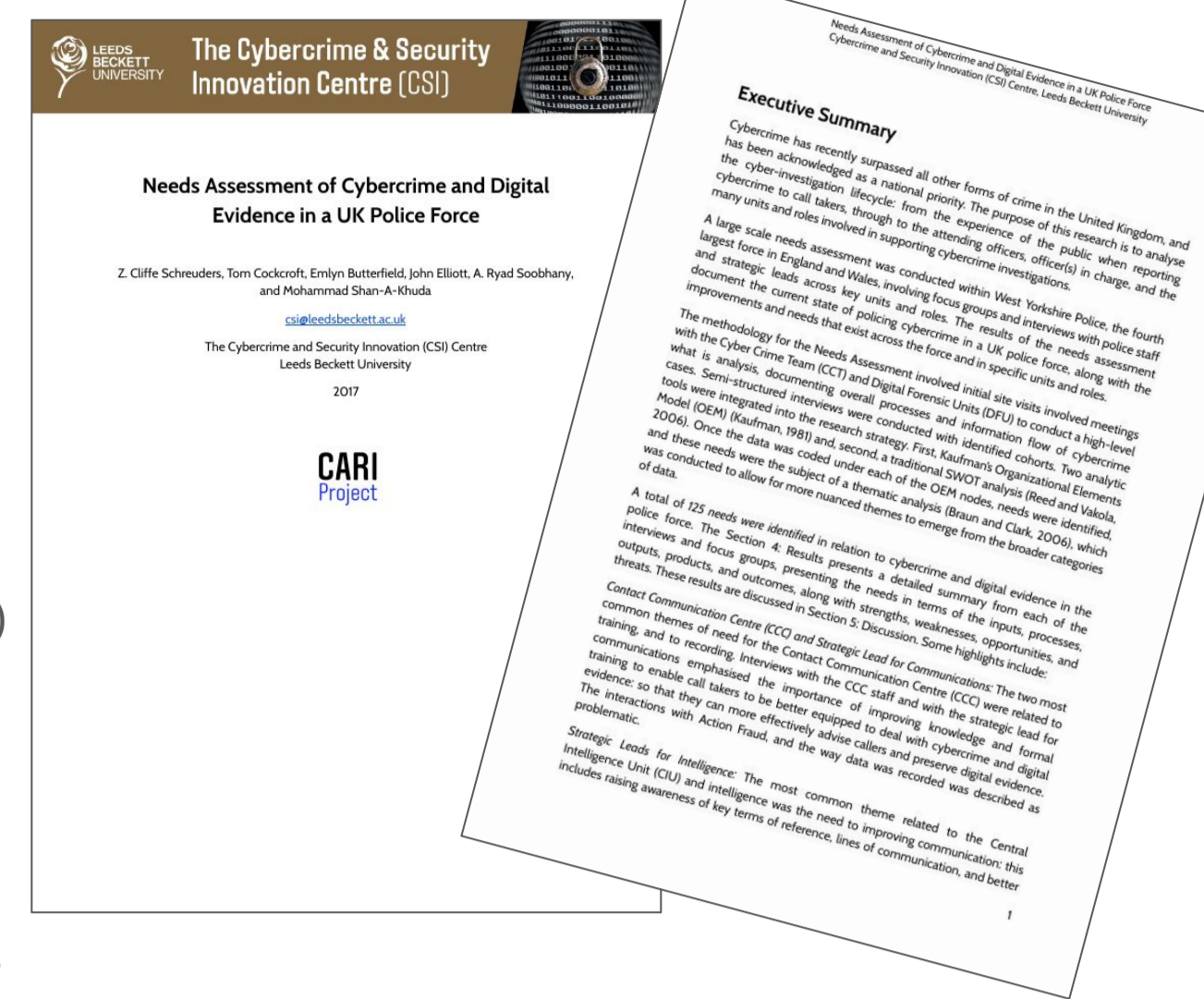
Needs Assessment

Aims

Police face many challenges dealing with cybercrime

Analysed the cyber-investigation lifecycle: from the experience of the public when reporting cybercrime to call takers, through to the attending officers, officer(s) in charge, and the many units and roles involved in supporting cybercrime investigations

Documented the current state of policing cybercrime in a UK police force



Results

Thanks to an openness to the need for improvement, the focus groups and interviews produced data that identified a large number of issues within the force...

With practical needs that can be addressed to mitigate those issues.

A total of **125 needs** were identified

Our needs assessment report presents a detailed summary results from each of the cohorts, and a force-wide thematic analysis of needs.

Common themes identified include:

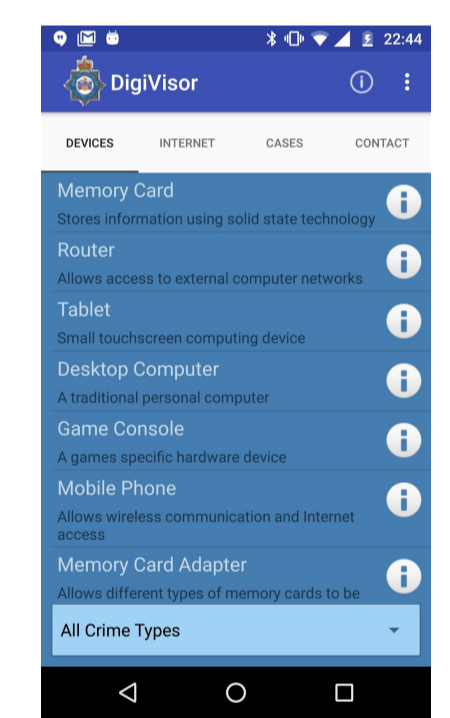
- Knowledge/training
- Communication
- Recording
- Software
- Roles
- Governance
- Procedures
- Resources
- Consistency
- Staffing
- National input
- Face-to-face
- Interactions with the public
- New capabilities
- Triage

Frontline officer awareness development and decision support mobile app

Developed an Android app to assist front-line officers

User participatory design:

- Focus groups and input from: Front-Line Officers / Safeguarding; DFU; Cyber Crime Team (CCT); Central Authorities Bureau (CAB); Telecom Unit
- Input on requirements: Legislation, and Policies / Procedures; and app design



Development of animated training videos

Captures evidence and notes at the scene (including Wi-Fi and Bluetooth), which are not currently captured by forces

Provides structured guidance for preservation of digital evidence and contact details

Evaluation: simulated seizure, measuring usability, confidence and correct selection of devices to seize

- Statistically significant improvements to seizure accuracy
- Acceptable usability

Linking images to source camera devices

Forces would benefit from a method to link digital pictures to the source camera devices

Sensor Pattern Noise (SPN) can be used as a Digital Fingerprint to link images to cameras, yet is under-utilised by forces

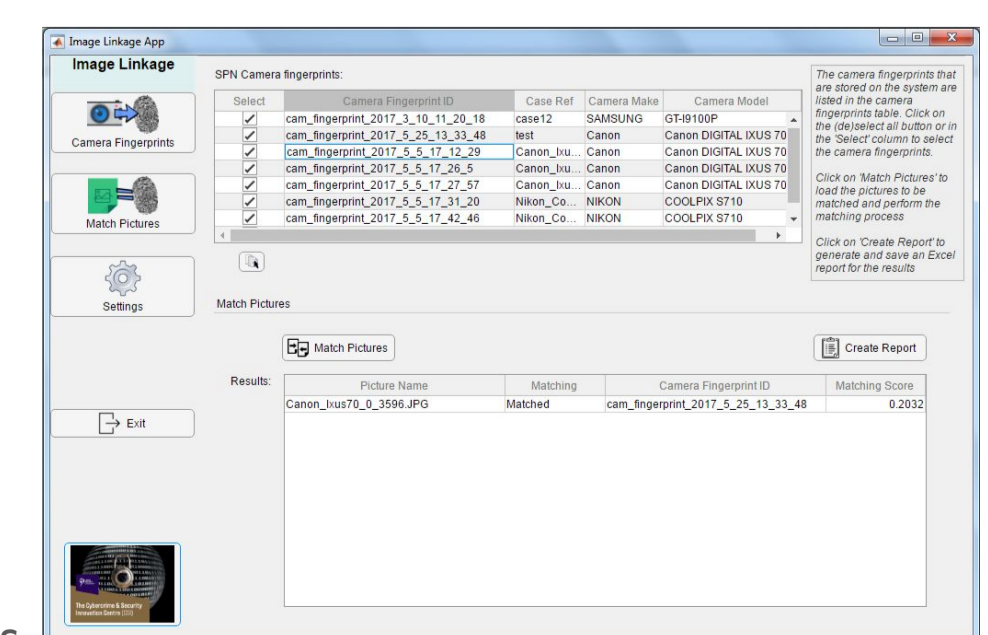
- Natural imperfections in the silicon chip and different sensitivity of pixels to light
- SPN created by one sensor is different to other imaging sensors
- Can differentiate between sensors from same model

SPN algorithm improvements

- A less lossy algorithm, that was shown to improve accuracy of results
- Evaluated against state-of-the-art SPN, using image datasets

Development into a software tool available to forces, with procedures and user guide

Installed and evaluated in WYP Digital Forensics Unit (DFU)



The bid

'An evidence-based approach to fighting cybercrime from the frontline: improving the effectiveness and efficiency of investigating cyber enabled crime'

Aiming to investigate and improve police response and capability for cybercrime and digital evidence

Steering Group:



Structure

- Starting with a needs assessment
- Research training
- Research workstream project selection
- Nine workstreams

- Automated forensic analysis
- Image linkage for victim identification and framework for image fingerprint management
- Automated grooming detection
- Frontline officer awareness development and decision support mobile app
- Assessment of methods of cyber training
- Framework for seizure, preservation and preservation of cloud evidence
- An evaluation of the role of the Digital Media Investigator within WYP
- Characteristics of victims of cybercrime
- Broadcast media artefacts

Outcomes: Technical and software

- Advances in digital forensics analysis approaches
- Improvements to the use of image processing for digital forensics (SPN) to match photos to seized camera devices
- Automated chat log processing for grooming detection
- A mobile app for front-line police for training and decision support

Outcomes: Improved understanding

- Best practice guidelines and procedures for the police force making use of technologies
- Needs assessment results of WYP in terms of cybercrime and digital investigation
- Statistical insights into classes of victims of cybercrime
- An evaluation of the role of Digital Media Investigators
- An assessment of styles of cybercrime training within WYP