



LEEDS  
BECKETT  
UNIVERSITY

---

Citation:

Schreuders, ZC and Smith, V and Butterfield, EM and Miller, S and Cockcroft, TW and Horvath, D and Trevorrow, PA and Elliott, JR and Lambourne, AD and Dixon, MB and Sheikh Akbari, A and Halmshaw, LD (2017) CARI Project Showcase Event. In: CARI Project Showcase Event: Tackling Cyber Crime and Improving Police Response Showcase, Headingley, UK. (Unpublished)

Link to Leeds Beckett Repository record:

<https://eprints.leedsbeckett.ac.uk/id/eprint/5081/>

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](mailto:openaccess@leedsbeckett.ac.uk) and we will investigate on a case-by-case basis.



# CARI Project



LEEDS  
BECKETT  
UNIVERSITY



WEST YORKSHIRE  
**POLICE**



# Introductions by Session Chair

Detective Chief  
Superintendent Mark Ridley





# Chief Constable Opening Statements

Chief Constable Dee Collins





# Introduction by the ACC

Assistant Chief Constable  
Russ Foster





# Introduction by the Dean

Professor Colin Pattinson





# Tackling Cyber Crime in West Yorkshire

Detective Chief Inspector  
Vanessa Smith





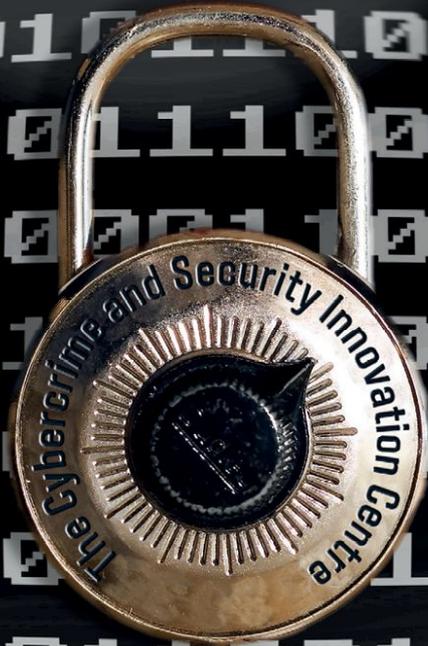
# CSI Centre and the CARI Project

Dr Z. Cliffe Schreuders





LEEDS  
BECKETT  
UNIVERSITY



# The Cybercrime & Security Innovation Centre (CSI)



## The Cybercrime & Security Innovation Centre

“The CSI Centre aims to improve and incorporate an evidence-based approach into the frontline policing of digital forensics and cybercrime investigations, and to advance human factors of computer security and forensics mechanisms and practice.”

“A collaborative hub for high quality research, with a collegial, supportive and cooperative research-intensive group, aimed at high-impact outputs.”

Partnerships and collaboration



## Teaching Forensics and Security @ Leeds Beckett

BSc (Hons) Computer Forensics  
BSc (Hons) Computer Security  
BSc (Hons) Computer Forensics & Security  
MEng Computer Forensics & Security  
MSc Computer Security (Distance Learning)

Digital forensics: analysis of digital systems, from the seizure of exhibits through to the analysis and presentation of all forms of digital evidence

Security: ethical hacking, defensive controls and hardening, incident response and investigation

NSS Overall Satisfaction:

2015/16: 100%

2016/17: 94%





## Current projects

£1.5m in recent funding

In partnerships with industry, academia, and police

The CARI Project

Knowledge Transfer Partnerships

Nuclear Power Plant Safety

European Union Agency for Network and Information Security (ENISA)

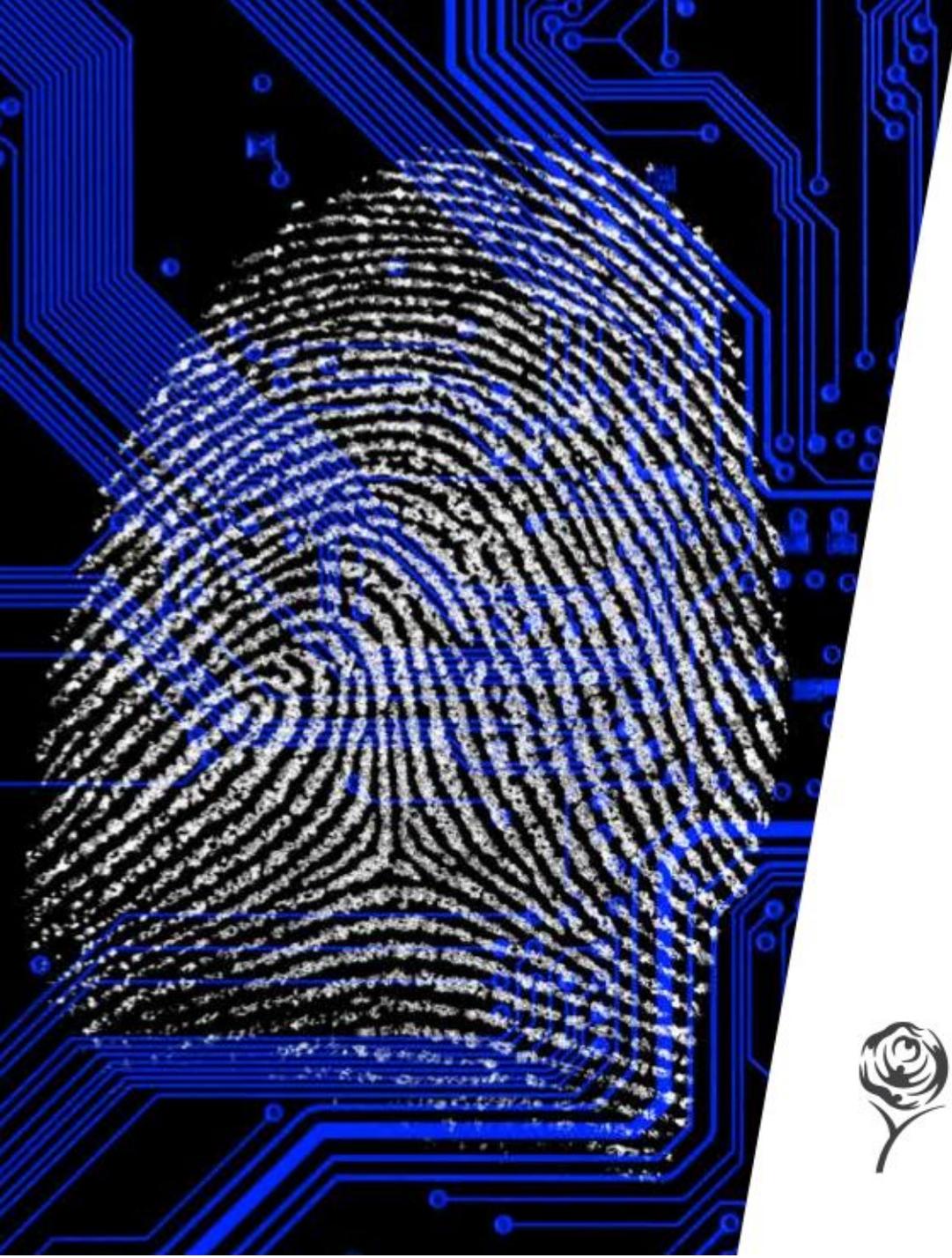
Randomised hacking challenges

Hosting Capture The Flag hacking competitions for universities and schools



# The Cybercrime & Security Innovation Centre (CSI)





# CARI Project



LEEDS  
BECKETT  
UNIVERSITY



WEST YORKSHIRE  
**POLICE**



# CARI Project

## The bid

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

£640,000 funded by the Police Knowledge Fund

Home Office, College of Policing, Higher Education Funding Council for England (HEFCE)



College of  
Policing



Home Office





# CARI Project

## The bid partners

Leeds Beckett University

West Yorkshire Police

Steering Group:

- WYP West Yorkshire for Innovation (WyFi)
- College of Policing
- Canterbury Christ Church University
- CENTRIC Sheffield Hallam University





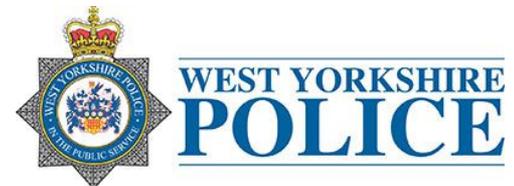
# CARI Project

## Starting with a needs assessment

Larger scale than originally planned

Over 24 hours of interviews and focus groups

Investigated the entire lifecycle of investigations regarding cybercrime and digital evidence





# CARI Project

## Research training

All members of DFU and CCT received research training

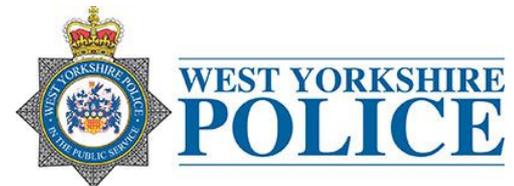
4 x full day of research methods, with sessions for developing research ideas

Research methods: including qualitative and quantitative techniques

Research ideas development

Development into research proposals

Supported by online materials and ongoing research meetings





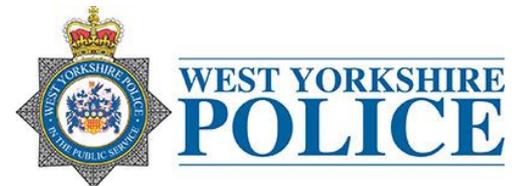
# CARI Project

## Research workstream project selection

Driven by police needs, rather than purely academic curiosity

Selected based on impact for WYP, academic impact, and scope

Projects refined





# CARI Project

## 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





# CARI Project

## Challenges

Delays due to vetting, contracts, police restructuring, and data access

Brought in more academics, and employed a full time West Yorkshire Police team

Extended end date: September 2017





# CARI Project

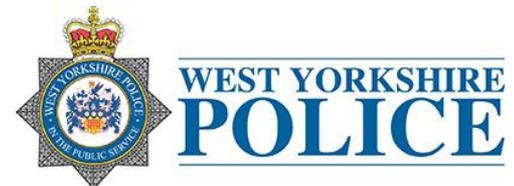
## Outcomes: Technical and software

Advances in digital forensics analysis approaches

Improvements to the use of image processing for digital forensics (SPN)

Automated chat log processing for grooming detection

A mobile app for front-line police for training and decision support





# CARI Project

## Outcomes: Improved understanding

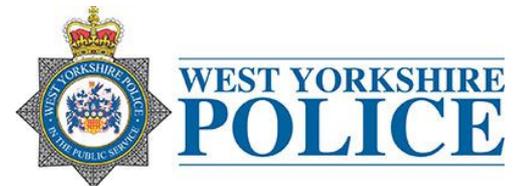
Best practice guidelines and procedures for the police force making use of technologies

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





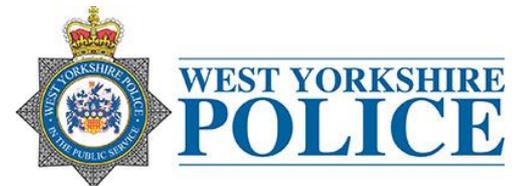
# CARI Project

## Outcomes: Dissemination

Broadcast media and training videos

Reports and papers

Shared with police forces







# CARI Project

## Conclusion

Today we are presenting each of the CARI Project workstreams

The product of police and academia collaboration

Technical solutions and improved understanding





# CARI Project

Questions





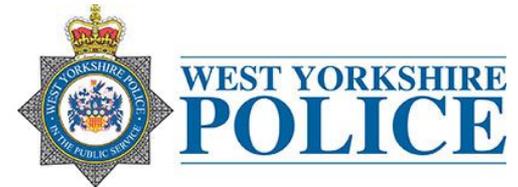
# BREAK





# Workstream Session 1: Introduction by Session Chair

Detective Chief  
Superintendent Mark Ridley





# Needs Assessment

Dr Z. Cliffe Schreuders  
and  
Dr Thomas Cockcroft





# CARI Project

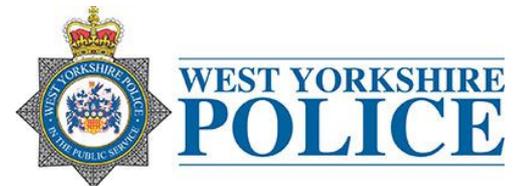
## Aims

Police face many challenges dealing with cybercrime

Analyse 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

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

Improvements and needs that exist across the force and in specific units and roles





# CARI Project

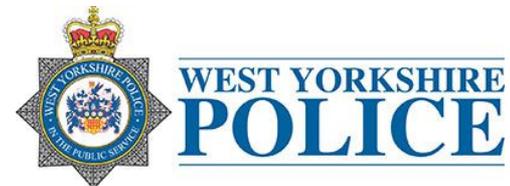
## Methods

### Initial site visits

Meetings with the Cyber Crime Team (CCT) and Digital Forensic Unit (DFU) to conduct a high-level what is analysis, documenting overall processes and information flow of cybercrime cases

### Identification of cohorts of interest

### Semi-structured interviews and focus groups





# CARI Project

## Analytic tools

Kaufman's Organizational Elements Model (OEM)

Traditional SWOT analysis

Interviews were transcribed; and coded under each of the OEM+SWOT nodes

Needs were identified

Needs were the subject of a thematic analysis

Kaufman's Organizational Elements Model (OEM)

	INPUTS	PROCESSES (Means)	PRODUCTS (En route results)	OUTPUTS (Delivered to society)	OUTCOMES (Effects in or for society)
WHAT IS					
WHAT SHOULD BE					



# CARI Project

## Sample

- Contact Communication Centre (4 participants)
- Strategic Leads for Training (3 participants)
- Covert Authorities Bureau (4 participants)
- Cyber Crime Team (2 participants)
- District Strategic Lead (1 Participant)
- Dedicated Source Unit (2 participants)
- Digital Forensics Unit (3 participants)
- District Staff (7 participants)
- Economic Crime Unit (2 participants)
- Strategic Lead for Communications (1 participant)
- Strategic Leads for Intelligence (2 participants)
- Investigative Analysts and Researchers (6 participants)
- Homicide and Major Enquiry Team (2 participants)
- Strategic Lead for Safeguard and Central Governance (1 participant)
- Strategic Lead for Murder and Serious Crime (1 participant)
- Technical Support Unit (2 participant)
- Telecoms staff (2 participants)
- Strategic Lead for Telecoms (1 participant)





# CARI Project

## 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





# CARI Project

## 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





# CARI Project

## Training and knowledge

The most prevalent theme of need was training (n=28) and knowledge (n=30)

The training should take the needs of the various roles across the force into account (rather than a one-size-fits-all approach for everyone including those in specialist roles)

Teaching approaches appropriate for the purpose (e-learning is perhaps overused, and ad hoc Q&As may be more effective)

Existing training packages were perceived by many as being outdated and not guaranteed to develop skills.

Refresher training should be provided





# CARI Project

## Training and knowledge: Recommendations

Materials are in need of updating

Current training should be reviewed to ensure that it is fit-for-purpose

Time needs to be allocated to enable police personnel to engage in the training

A modular set of training packages mapped to the needs of police roles, delivered face-to-face might enhance the effectiveness of the training





# CARI Project

## Training and knowledge: Training should include

- The nature, form and impact of cybercrime.
- General cyber-awareness/knowledge in regards to cybercrime.
- Advice to give callers, and walk-throughs on selected issues.
- Preservation of digital evidence: for example, preserving mobile phone data.
- Further knowledge/training around digital technology (including raising frontline awareness of current apps and technology in use).
- Further knowledge/procedures around Social media and online harassment, to improve frontline response and advice.
- Knowledge of cybercrime and how this relates to digital sources of intelligence.
- Technical content for DFU, CCT, DMI to ensure it contains up-to-date and relevant content.
- Cascading of basic skills around open source intelligence gathering.
- Further bespoke training according to various role requirements (DSU, TSU, HMET, ECU, Frontline officers, CCC, etc), to improve relevant cyber skills.
- Training should better cover updates in legal and technological issues.
- Ensure that police dealing with child abuse cases have sufficient cybercrime/digital training and support. Training should be bespoke to (or inclusive of) child safeguarding and cybercrime.
- DMIs/CCT (or other intermediaries) need to have increased training regarding proportionate means re: data requests, to avoid overburdening Telecoms.
- Improved officer understanding regarding forensic examination outputs.
- CCT training to conduct investigative interviews, and help direct investigations.
- Safeguarding trained to make use of triaging tools.
- Improved training on techniques and tools for cyber attacks.



LEEDS  
BECKETT  
UNIVERSITY



WEST YORKSHIRE  
POLICE



# CARI Project

## Communications

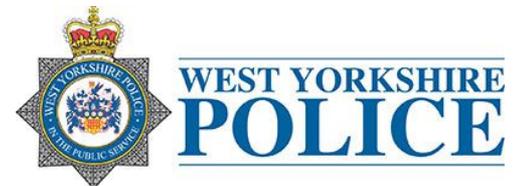
The second most common theme of needs was related to communications (n=28)

Within this, the most prominent sub-theme was that of role definition and clarity (n=14). Part of the problem is the general lack of cyber-skills within the police service, and the subsequent lack of clarity over key terms of reference and definitions.

A related issue is the need for improved communication and collaboration between units (including DSU, TSU, CCT, DFU, DMI, Telecoms, and ECU)

A need for further face-to-face communications

There is a need for improved data sharing with Action Fraud





# CARI Project

## Quality of recording

The need to improve the quality of recording of cybercrimes and case data was another major high-level theme of need within the force (n=17)

A subtheme was that of the correct flagging of cases. CCTs work in this area has identified that there has been a vast underreporting of “cyber” related cases. Correctly labeling can improve the force's response to cybercrime and digital evidence.

Need for more complex flagging of incidents (e.g. in respect of allowing multiple labels, and clearer definitions)





# CARI Project

## Quality of recording

Further context could be made available by linking datasets across the force

CRM (Customer Record Management System) which would draw together other systems such as Storm and Niche

Analysts felt that research and analysis would be improved through joined up computer systems within the organisation.

The Charter system is in need of workflow changes

Additional workflows to better suit the needs of telecommunication requests

CAB: Include one-sided consensual directed surveillance authorities, and authority applications in other jurisdictions.





# CARI Project

## Other common themes

Software: changes to Charter, interacting with members the public; monitoring registered sex offenders; improved case management; automation of data analysis of digital evidence; Received Data Handover Interface (RDHI); automated forensics reporting; and aggregating results from various tools.

Governance: a review of differences between districts' response to cybercrime; increased co-ordination of how police engage with the public; and, review resource management such as the allocation of cases to districts based on operational capacity.

Procedures: clear guidance on how police should perform certain tasks.





# CARI Project

## Other common themes

### Resourcing

National input: legal interpretation; national assistance with Home Office provided RDHI and ADM systems; increased relationships with additional service providers; national guidance and accreditation on covert cyber capabilities



# CARI Project

Output

124 page report



The Cybercrime & Security  
Innovation Centre (CSI)



## Needs Assessment of Cybercrime and Digital Evidence in a UK Police Force

Z. Cliffe Schreuders, Tom Cockcroft, Emlyn Butterfield, John Elliott, A. Ryad Soobhany,  
and Mohammad Shan-A-Khuda

[csi@leedsbeckett.ac.uk](mailto:csi@leedsbeckett.ac.uk)

The Cybercrime and Security Innovation (CSI) Centre  
Leeds Beckett University

2017

CARI  
Project

Needs Assessment of Cybercrime and Digital Evidence in a UK Police Force  
Cybercrime and Security Innovation (CSI) Centre, Leeds Beckett University

### Executive Summary

Cybercrime has recently surpassed all other forms of crime in the United Kingdom, and has been acknowledged as a national priority. The purpose of this research is to analyse 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.

A large scale needs assessment was conducted within West Yorkshire Police, the fourth largest force in England and Wales, involving focus groups and interviews with police staff and strategic leads across key units and roles. The results of the needs assessment document the current state of policing cybercrime in a UK police force, along with the improvements and needs that exist across the force and in specific units and roles.

The methodology for the Needs Assessment involved initial site visits involved meetings with the Cyber Crime Team (CCT) and Digital Forensic Units (DFU) to conduct a high-level what is analysis, documenting overall processes and information flow of cybercrime cases. Semi-structured interviews were conducted with identified cohorts. Two analytic tools were integrated into the research strategy. First, Kaufman's Organizational Elements Model (OEM) (Kaufman, 1981) and, second, a traditional SWOT analysis (Reed and Vakola, 2006). Once the data was coded under each of the OEM nodes, needs were identified, and these needs were the subject of a thematic analysis (Braun and Clark, 2006), which was conducted to allow for more nuanced themes to emerge from the broader categories of data.

A total of 125 needs were identified in relation to cybercrime and digital evidence in the police force. The Section 4: Results presents a detailed summary from each of the interviews and focus groups, presenting the needs in terms of the inputs, processes, outputs, products, and outcomes, along with strengths, weaknesses, opportunities, and threats. These results are discussed in Section 5: Discussion. Some highlights include:

**Contact Communication Centre (CCC) and Strategic Lead for Communications:** The two most common themes of need for the Contact Communication Centre (CCC) were related to training, and to recording. Interviews with the CCC staff and with the strategic lead for communications emphasised the importance of improving knowledge and formal training to enable call takers to be better equipped to deal with cybercrime and digital evidence: so that they can more effectively advise callers and preserve digital evidence. The interactions with Action Fraud, and the way data was recorded was described as problematic.

**Strategic Leads for Intelligence:** The most common theme related to the Central Intelligence Unit (CIU) and intelligence was the need to improve communication: this includes raising awareness of key terms of reference, lines of communication, and better



LEEDS  
BECKETT  
UNIVERSITY



WEST YORKSHIRE  
POLICE



# CARI Project

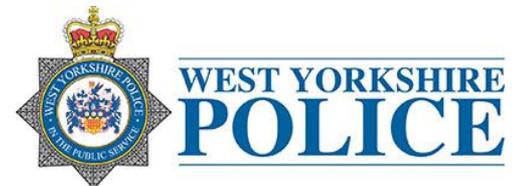
## Impact for West Yorkshire Police

Informed the selection and design of CARI Project workstreams

This work was designed to be used to directly inform WYP policy and practice.

Presentations to the Tactical Board, Strategic Board, and Independent Advisory Group on cybercrime

Due to the nature of the findings, it is likely that these findings may apply nationally.





# CARI Project

## Future work

We have submitted a Police Transformation Fund bid to transform the training provided within the police force

“CyberTRAIN: The Provision of 21st Century Cyber Training to all Police Officers and Police Staff involved in the investigation of Cyber Crime”





# CARI Project

Questions





# Frontline officer awareness development and decision support mobile app

Det. Ch. Insp Vanessa Smith  
DFI Stephen Miller



LEEDS  
BECKETT  
UNIVERSITY



WEST YORKSHIRE  
**POLICE**



# CARI Project

Traditional

Fingerprint

DNA

Drugs

Footwear

Fire

Firearms Residue

Marks



LEEDS  
BECKETT  
UNIVERSITY



WEST YORKSHIRE  
POLICE



# CARI Project

Digital

CCTV

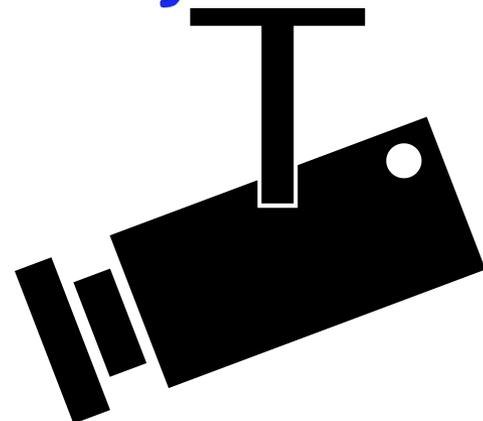
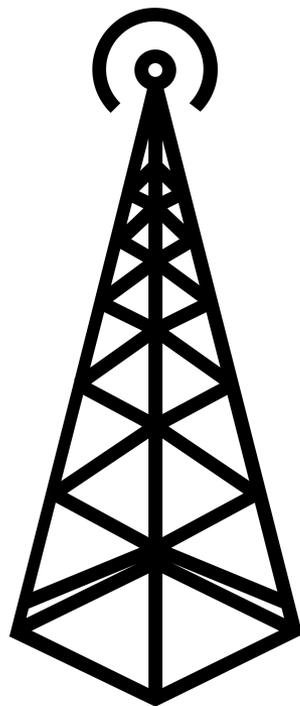
Mobile Phones

Photograph Scene

CSP / ISP Data

Social Media

Cloud Storage



**WEST YORKSHIRE  
POLICE**



# CARI Project

## Wi-Fi (Seldom Recovered)

Max. 90 Meter Range (300 Feet)

Broadcast SSID

Status

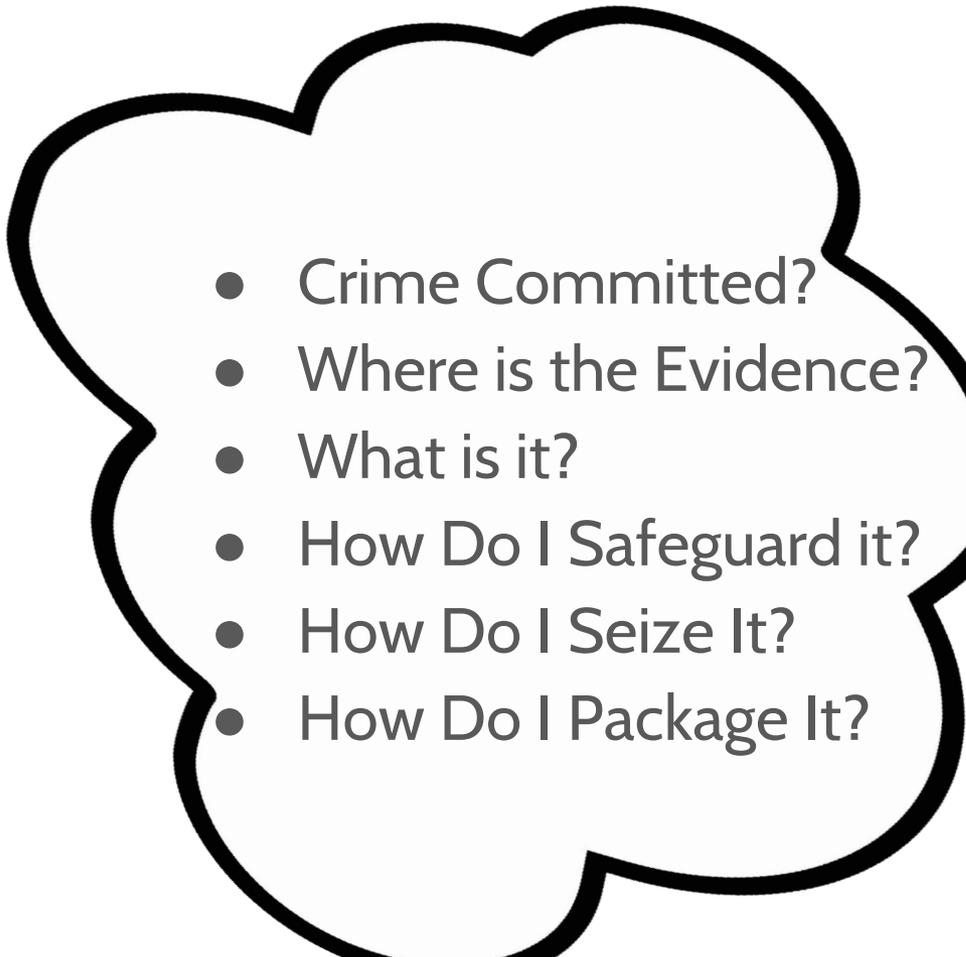
MAC Address (IEEE.org)

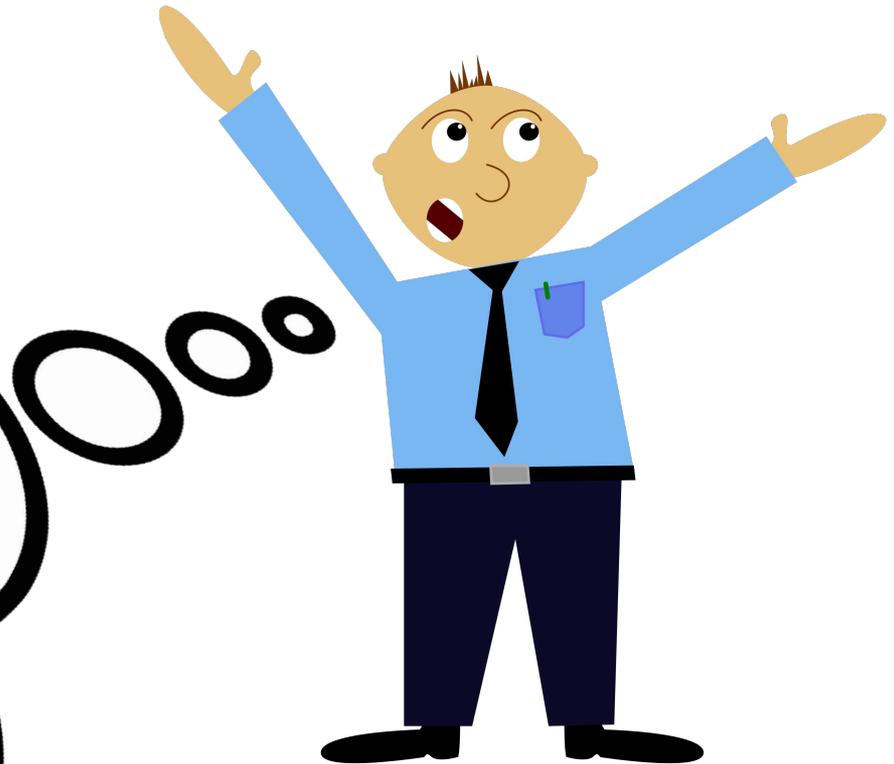




# CARI Project

## Front-Line Officer Issues

- 
- Crime Committed?
  - Where is the Evidence?
  - What is it?
  - How Do I Safeguard it?
  - How Do I Seize It?
  - How Do I Package It?



LEEDS  
BECKETT  
UNIVERSITY



WEST YORKSHIRE  
**POLICE**



# CARI Project

## The problem

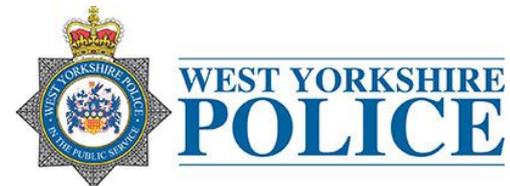
Frontline officers need assistance:

Identifying digital evidence: both physical devices and Internet-based evidence

Require access to training materials and to procedures on the go

Capturing information about cases

DFU struggle with workload related to officers seizing irrelevant devices





# CARI Project

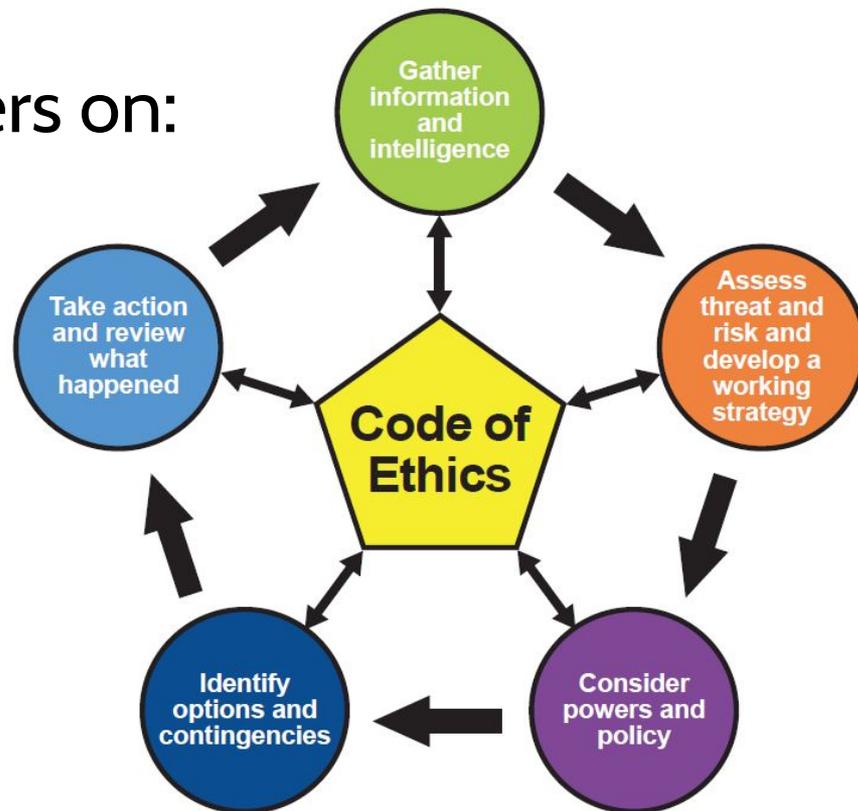
## Android App to Advise Officers on:

Types of Devices and where digital data is stored

Potential Sources Digital Evidence

Policies, Legislation and best practice guides

Preservation and Seizure of Digital Based Evidence



## National Decision Model





# CARI Project

## Methods

Focus Groups (Front-Line Officers / Safeguarding)

Digital Forensic Unit (DFU)

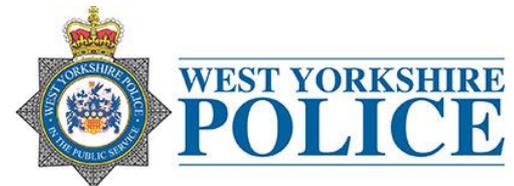
Cyber Team

Central Authorities Bureau (CAB)

Telecom Unit

Legislation

Policies / Procedures





# Digital Devices

Identify Devices

Types of Information

Relevant Evidence

Sample Device Images

Information Videos

Seizure Policy / Procedures





# Internet / Cloud

Identify Online Information

Sources of Evidence

Social Media

How to Capture Evidence

Authorities

Which Department?



**DigiVisor**

DEVICES    **INTERNET**    CASES    CONTACT

- Cloud Storage**  
Supports storage of files remotely on a server
- Social Network**  
Web-based application allowing interaction with remote users
- Email Server**  
Stores email messages
- Chat Application**  
Allows on-line chats with other users
- Instant Messaging**  
Allows messaging other users

All Crime Types



# Cases

Scene Notes

Automatically Capture GPS

Photograph Information

Record Audio / Video

Scan Wi-Fi

Scan Bluetooth

Create a package for DFU/Cyber





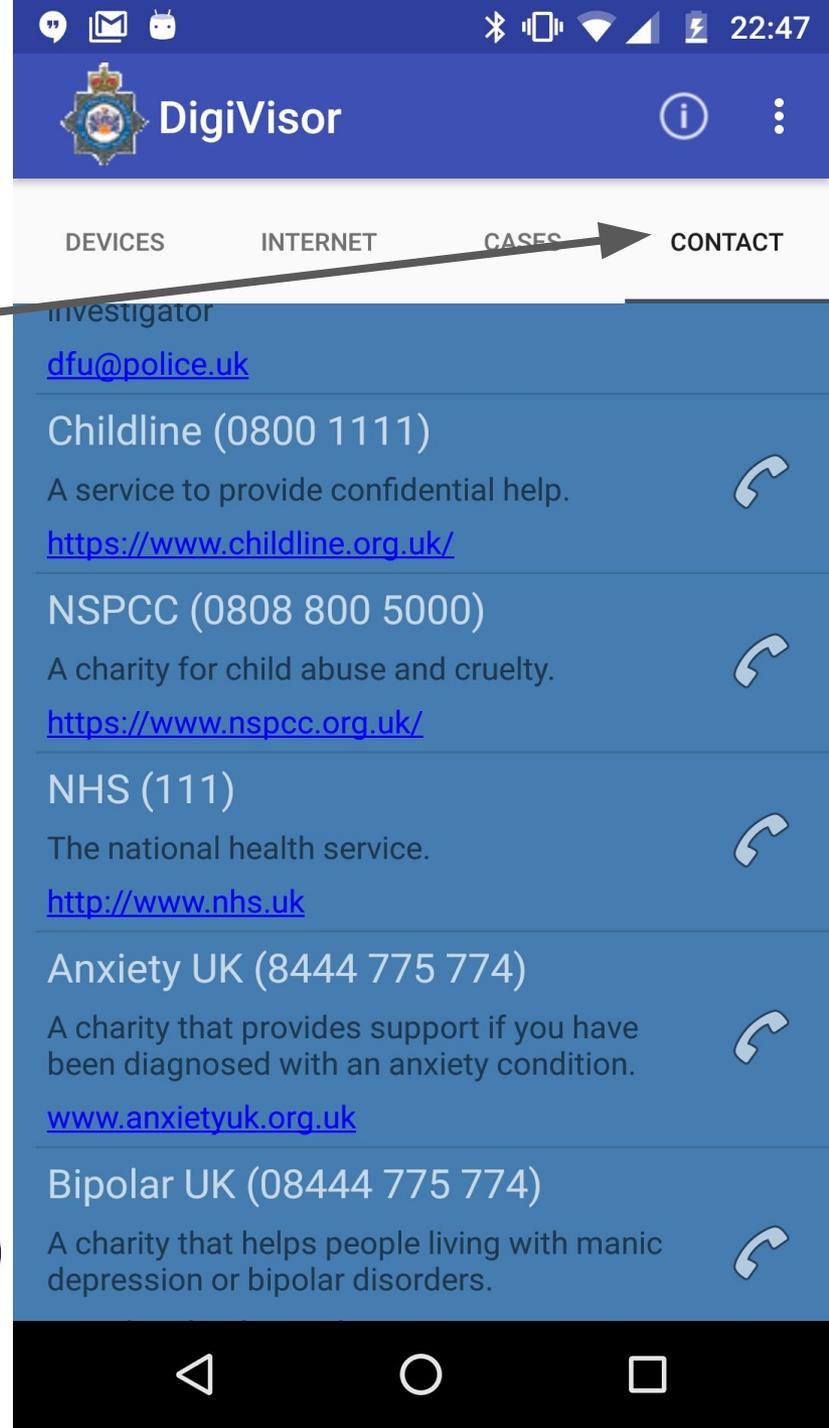
# Contact

Helpline

Useful Contact Information

Victim Support / Advice

Staff Welfare





# CARI Project

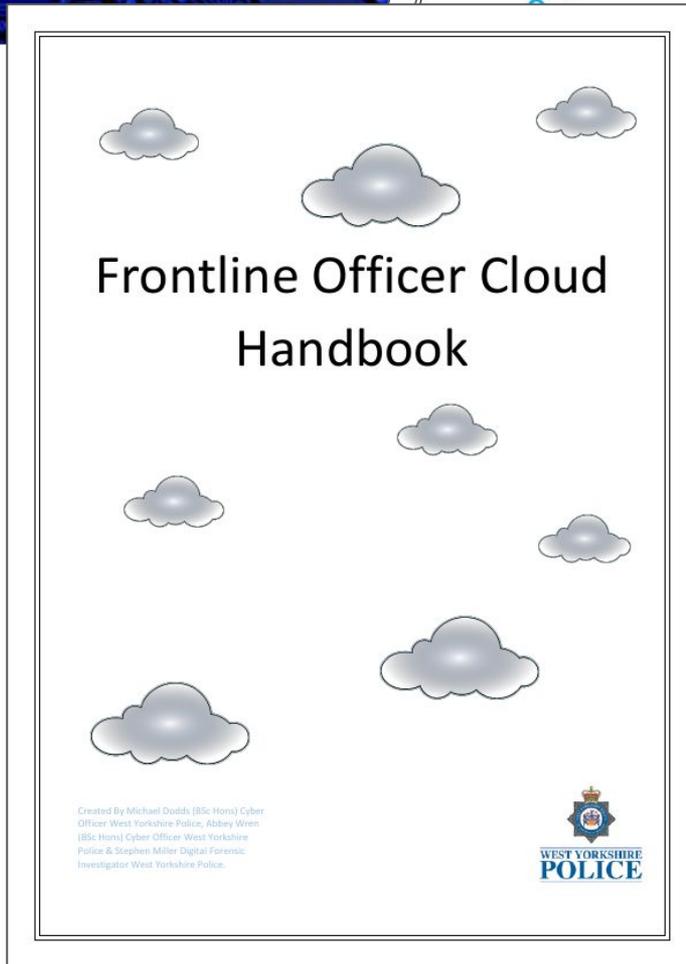
Live demo



# CARI Project

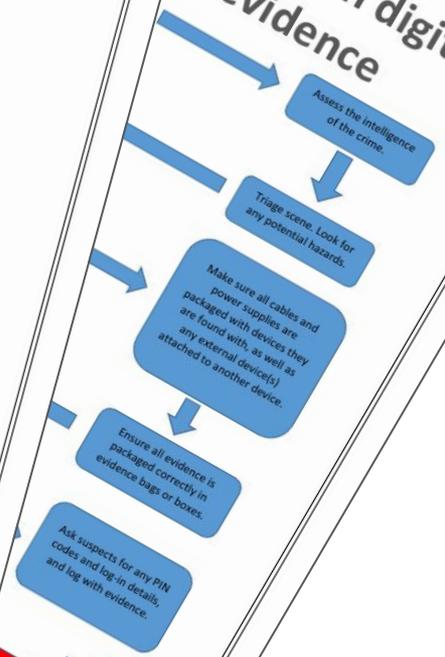
Output

Handbook



(K.A. cloud storage):  
allows a user to store information and files by  
accessible to the Internet. This data is then stored  
n then be retrieved or viewed online via any

## Deal with digital evidence



LEEDS  
BECKETT  
UNIVERSITY



WEST YORKSHIRE  
POLICE



# CARI Project

## DigiVisor

DigiVisor has been developed:

By creative and talented people

An effective joint partnership (between Leeds Beckett & WYP)

Through practical “Bobbying” and Necessity.

DigiVisor is only Limited by:

Your Imagination and

Current Legislation





# CARI Project

## Future work

Development of app to adapt for national use

Log activity on usage of device

Delete stored Wi-Fi data after 30 days (MOPI)

Review Wi-Fi capture capabilities (strength, range, appropriate warning when scan performed)

Piloted within a district in West Yorkshire

Proactive & Reference App

Function offline – (black spots)

Central updating of app





# CARI Project

## Conclusion

A mobile app to help frontline officers to identify relevant digital-related evidence whilst at the scene of a potential crime

Videos

Reduce the amount of irrelevant exhibits seized

Provide structured guidance for preservation of digital evidence and contact details





# CARI Project

Questions





# In app Video Training

Hugo Smith



LEEDS  
BECKETT  
UNIVERSITY



WEST YORKSHIRE  
**POLICE**



# CARI Project

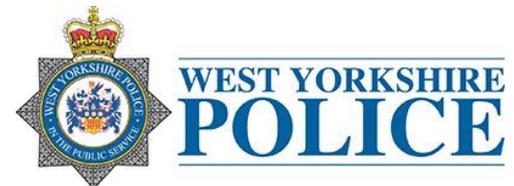
## Training Needs And Issues

The Needs Assessment identified a continuing training need.

'Moore's Law' has indicated for 50 years that technological change is fast and this infers training related to technology would benefit from being at least agile.

There is a bigger elephant than speed of change in this room, though...

**TRAINING IS BORING.**





# CARI Project

## BORING?

Approaches from WYP and contact about training provision before CARI acknowledged that officers are not excited or engaged by all training.

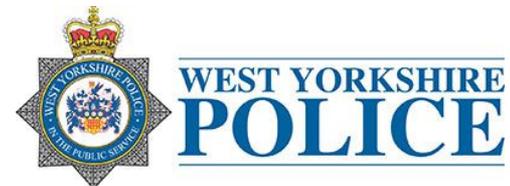
Student-led content production was considered an opportunity for both sides.

This content was not delivered.

## LESSONS:

Training is considered boring.

Making training content is hard. Making interesting training content was beyond our student.





# CARI Project

## Officers want knowledge and development

The focus groups for App Development showed police were open about both the gaps in their knowledge and that they had an appetite for learning.

BUT...officers were also clear that dull training increases resentment towards training and a sense that the time spent training would have been much better served completing their backlog of existing police work.

### LESSONS:

All our work is about preparation and performance. It's also about a sense of purpose and value. We need to be valued. Training has to serve our needs and our availability.





# CARI Project

## Can one size fit all?

Officers were clear about their training needs.

“I had cyber training when I started: ‘unplug the box in the corner and bag it for DFU’”

Many officers mentioned issues with pace of technology change, asset seizure and more. There were also issues with social media harassment cases in the enquiries made to them.

There were different kinds of officer. Young & Techy, Smartphone-Ready and KSPTV.

### LESSON:

Training has deal with basic information *and* fast-paced change.

Training has to engage a varied audience.





# CARI Project

## Development

Academics worked together and with information from focus groups to develop a suite of initial ideas for training videos.

Scripts were produced dealing with:

The need to switch off seized mobile phones

The need to package seized items properly

Laptop & USB seizure

Biohazards

Dealing with Memory Cards & Adaptors





# CARI Project

## Tone and Approach

When themes were developed and approach needed to be decided upon. A few key themes came through clearly from project colleagues and police focus groups:

Police officers are responsible. This does not mean they are dull.

Training needs narrative (we are comfortable with learning through story).

Training needs to be quick and easy to access.

LESSON:

'In-App' offers quick and easy access training possibilities.

Training has to be 'want-to-watch'





# CARI Project

## Two Styles (A)

Two styles of film were produced:

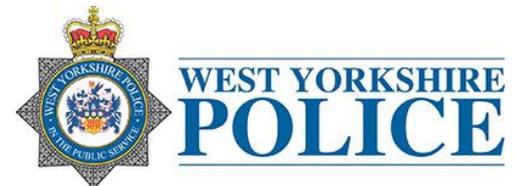
live action: aimed at those who are not

'Modern' tech users. Also aimed at

Satisfying a client potentially nervous

About 'wacky' training on such a serious

subject.

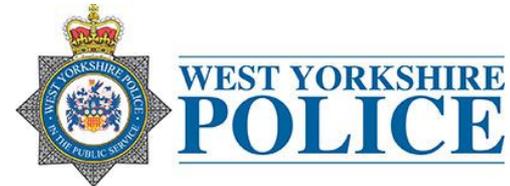
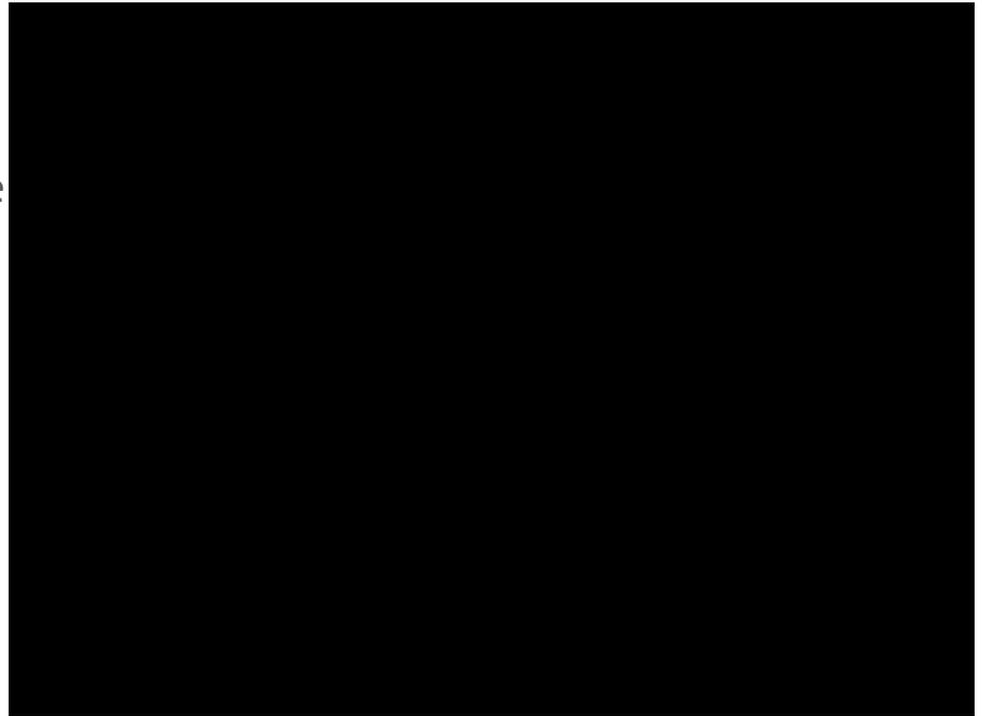




# CARI Project

## Two Styles (B)

Animation: aimed at users who want narrative. Aimed at an audience who are Social media users and are used to Flat graphics and layered messages. Relate-able.  
(All the animations should be viewable in-App or ask me and I'll share.)





# CARI Project

## Two Styles (B2)

Animation:

Some animations deal with seizure, some with contamination. Some deal with both.

These films are specifically designed for police officers and we are told they

have engaged them. Scripts were developed with officers to 'speak' to and about real experience.





# CARI Project

## Lessons

We would like to develop further animations as I am told these have been well received in by trial users.

There are several reasons why this might be the case:

Social media 'silent video use' makes up to 85% of social media video content use. Immediately available layered text and video is how we happily take-up information.

Narrative is fundamental to gripping us (and informing us). Content must be relate-able, especially when dealing with normally un-lovable content such as training.

Character-based training is fun *and* can be knowing.

Successful stories engage without instructing.



LEEDS  
BECKETT  
UNIVERSITY



WEST YORKSHIRE  
POLICE



# CARI Project

## Future Research

We would like to do some more research:

- 1) Comparing the uptake of 'live film' training vs animation by using data that could be recorded in-app to see if 'Narrative & Animation/Motion Graphics' as a style really is more appealing to a modern audience who use video over handheld devices often.
- 2) Measuring learning recall in a study looking at the real effectiveness of live action content, animation and desktop multiple choice style training.
- 3) Taking 'PC123' further as an 'every person' training character and producing more training content that tries to engage officers as a discerning audience, rather than bored captives. Perhaps even beyond cyber?





# LUNCH





# Workstream Session 2: Introduction by Session Chair

Detective Chief  
Superintendent Mark Ridley



WEST YORKSHIRE  
**POLICE**



# Image Linkage App and Framework for Camera Fingerprint Management

Dr Ryad Soobhany



# CARI Project

## Overview

Motivation

Image Acquisition Process & Sensor Noise

SPN Fingerprint Extraction Algorithm

Camera Fingerprint Management Framework

Impact on WYP

Future Work

Image Linkage Application Demo



"Fingerprint" (CC BY-ND 2.0) by CPOA





# CARI Project

## Motivation

Proliferation of pictures created by imaging devices

Some pictures used in the commission of crime

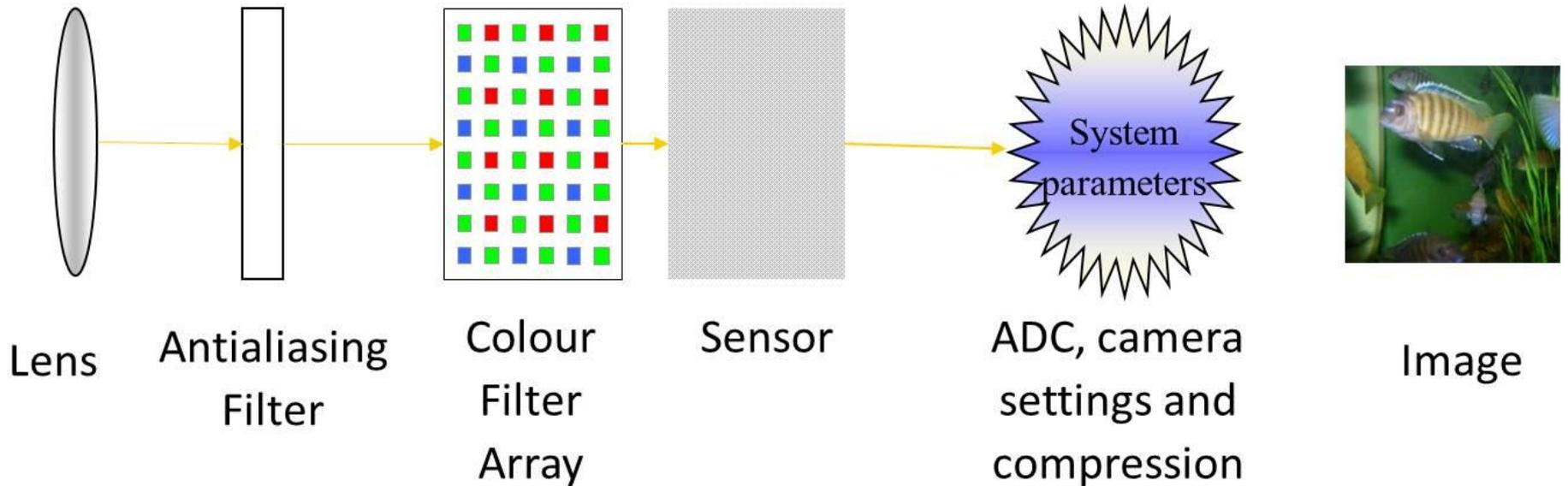
Child Sexual Exploitation

A method to link digital pictures recovered by law enforcement agencies



# CARI Project

## Image Acquisition Process





# CARI Project

## Sensor Noise as Digital Fingerprint

### Sensor Pattern Noise (SPN)

Natural imperfections in the silicon chip and different sensitivity of pixels to light

SPN created by one sensor is different to other imaging sensors

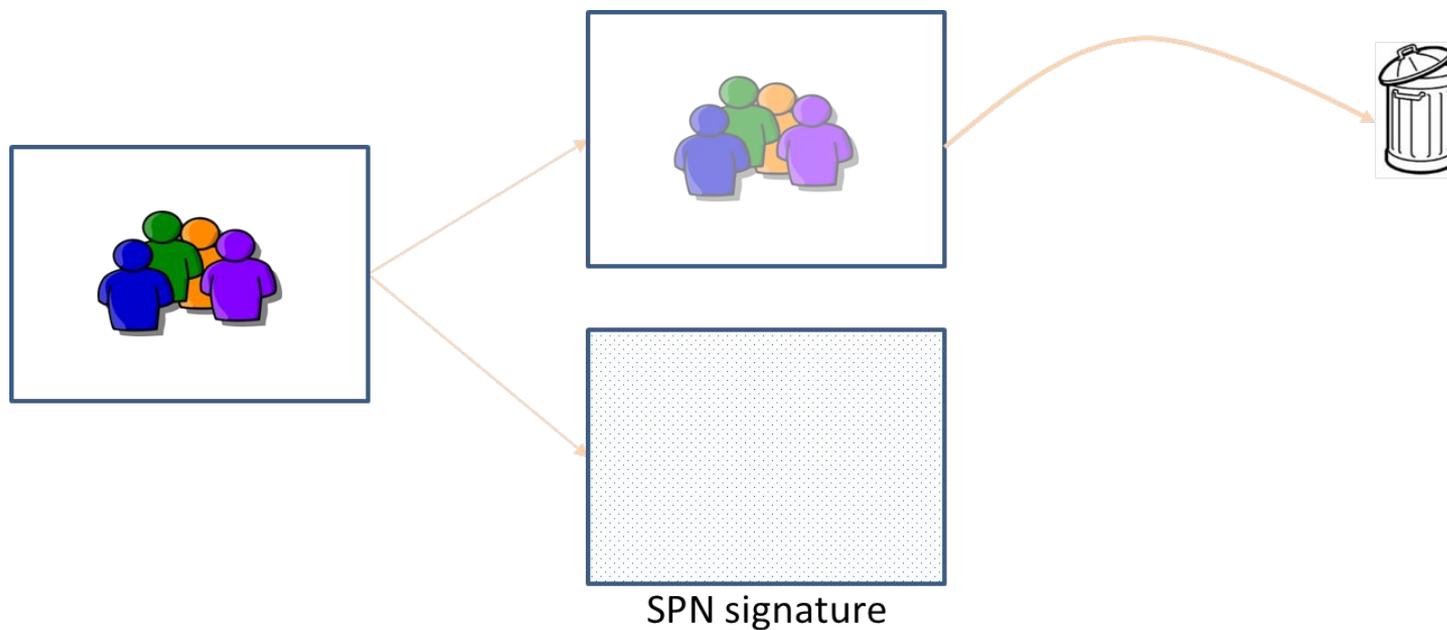
Can differentiate between sensors from same model





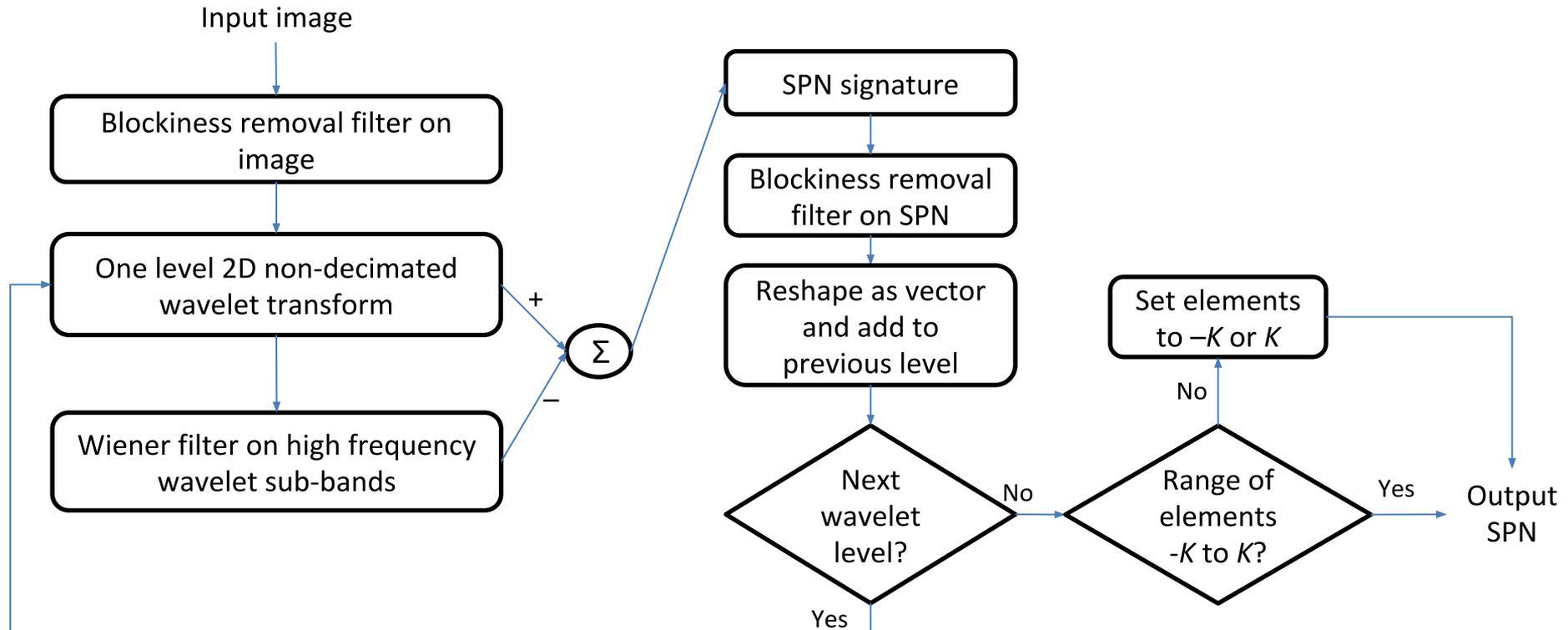
# CARI Project

## SPN Extraction from Image



# CARI Project

## SPN Fingerprint Extraction Algorithm





# CARI Project

## Camera Fingerprint Management Framework

Framework for creation and storage of SPN camera fingerprints

Best practice document

Ensure the imaging device can be used to take pictures

Take the test reference pictures

Store the test pictures





# CARI Project

## Camera Fingerprint Management Framework

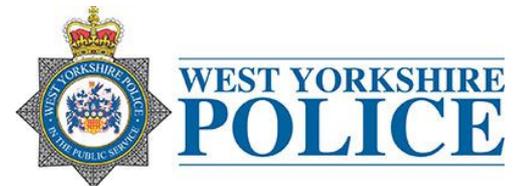
### User manual

Create a camera fingerprint

Store a camera fingerprint

Upload pictures to match against camera fingerprints

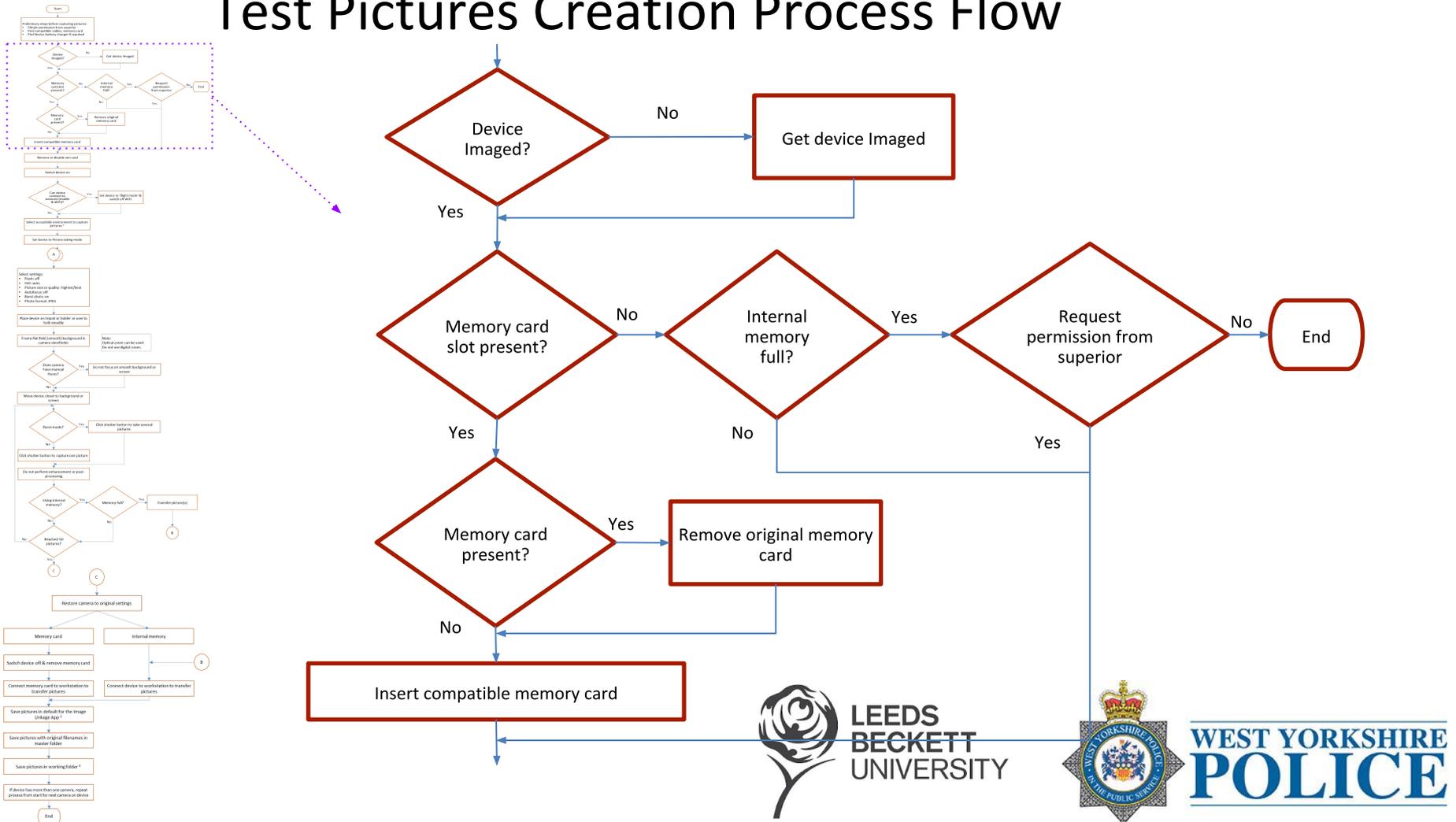
Generate and store result reports





# CARI Project

## Test Pictures Creation Process Flow



**WEST YORKSHIRE POLICE**



# CARI Project

## Evaluation

Evaluation by DFU officers and one DMI officer (observer)

Installation of the Image Linkage App

Follow the best practice policy document to capture and store test reference pictures from imaging device

18 Canon digital cameras with 5 pictures each

Use the app & follow the user manual to:

Create and manage camera fingerprints

Match pictures to camera fingerprints





# CARI Project

## Impact on Policing Cybercrime

Help to identify victims of CSE

Link new cases to historical cases based on imaging devices

Download pictures from Social Networking sites and match against devices fingerprint

Implement as SOP for DFU

Use in other departments within WYP, e.g. DMI





# CARI Project

## Future Work

Process massive volumes of pictures (big data)

Improve camera matching rate of algorithm

Maintenance of App and framework

Integrate as part of CAID

Forensic Science Regulator (FSR) can be approached for a collaboration to extend the camera fingerprint framework





# CARI Project

## Live Demo

Create camera fingerprints

Match suspect pictures against camera fingerprints

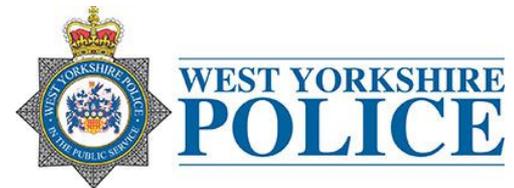
Generate report





# CARI Project

Questions





# Automated Grooming Detection

DFI Stephen Miller  
and  
Dr Ryad Soobhany



LEEDS  
BECKETT  
UNIVERSITY



WEST YORKSHIRE  
**POLICE**



# CARI Project

## Introduction

Digital data from seized devices can provide valuable evidence of grooming

Chat logs and messaging logs may total hundreds or thousand of text lines

Scanning this data manually is both time consuming and error-prone

Can automated scanning reliably identify potentially incriminating content?

How can systems adapt to changing communication styles and vocabulary?



(CC BY-SA 2.0) by ellyn.





# CARI Project

## Objectives for “Early Warning Triage” system (EWT)

Assess historic approaches used by other researchers in this area

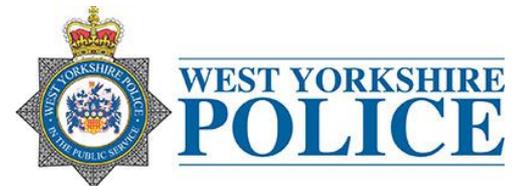
Create a general-purpose tool which can be tuned and evolved

Factor in the evolution in technology and style since early systems

Build models of likely grooming behaviours and their text characteristics

Test them against public-domain annotated logs from (e.g.) Perverted Justice (PJ)

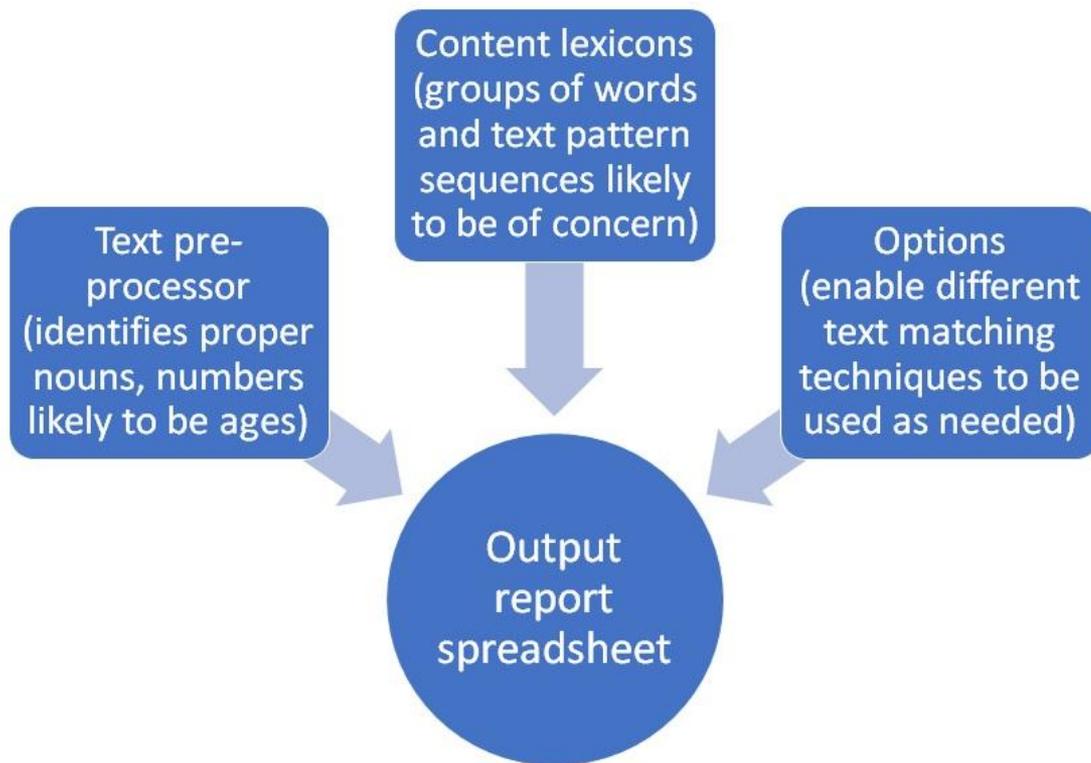
Tune them against real-world logs from West Yorkshire and other forces





# CARI Project

## EWT system overview





# CARI Project

## Input

Currently accepts 'Tab Separated Variable' text files (with known header information) tested with extracts from Industry Standard Forensic Tools:

- UFED Logical / Physical Analyser
- XRY
- Oxygen Forensic Suite
- Internet Evidence Finder (IEF) / AXIOM

*NB: (Simple Python script used to convert Excel outputs to TSV. Outputs can be reduced by exporting tab names 'chat' / 'message'. IEF / AXIOM SQLite table names can be obtained using `SELECT name FROM sqlite_master WHERE type = 'table'`)*





# CARI Project

## Output

Software to detect grooming taking place in online chat

Categorises chat into speech acts:

Communicative desensitisation (sexual)

Approach

Reframing

Pleading

Complement

Negative Response





# CARI Project

## Design philosophy

An “early warning” system needs to be discriminating else it will be ignored

Focus on identifying content which would potentially be of most concern

Recognise that establish genuine relative ages may be difficult by scanning

Enable the user to see an overview of “concern scores” and drill down if needed

Provide guidance on how to tune the text pattern matching in the field

Make the system fast (eg avoid lexicons of all place names, cafes, pubs etc)





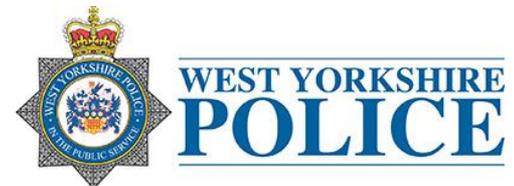
# CARI Project

## Output

Enables high level view of chat logs of interest

Enables high level view of participants

Filtering/viewing chat contents based on categories (speech acts, and traffic light flagging)





# CARI Project

## Outcomes

Design objectives met so far:

High level of rejection of false matches (on PJ data)

Reasonably discriminating detection of content of concern (on PJ data)

Rapid performance and field-tunable lexicons

Still to do:

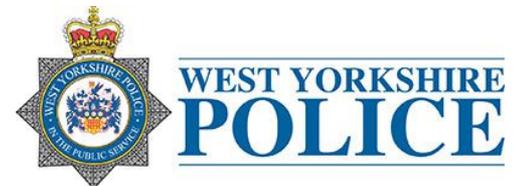
Further testing and tuning against real-world data from UK police forces





# CARI Project

Live Demo





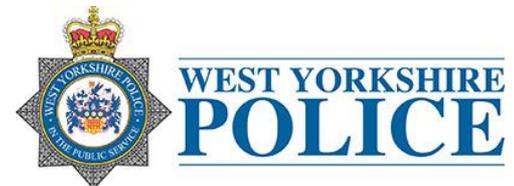
# CARI Project

## Impact for WYP

Provide DFU with the ability to automatically scan large volumes of chat for content related to grooming

Improve investigations

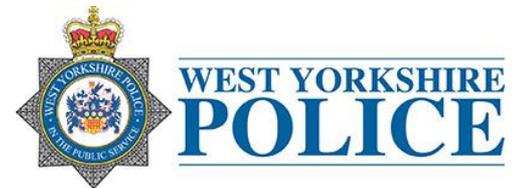
Potential to include in triage processes





# CARI Project

Questions





# Automated Digital Forensics Analysis

Emlyn Butterfield





# CARI Project

## Overview

A critical review and development of multi-source analysis processes and tools utilising expert systems to facilitate automated analysis of data for use during a forensic investigation.





# CARI Project

## Motivation

With the advancement and the ‘socialisation’ of technology a single device seized as part of an investigation is now uncommon

spread across phones, tablets, laptops, computers, gaming consoles, satellite navigation systems, and the list goes on.

This increase in devices and their subsequent storage capabilities also means investigations have now moved from 10’s of GB’s to 10’s of TB’s.

Increased storage means that the traditional forensic techniques and tools employed to analyse devices are no longer as effective

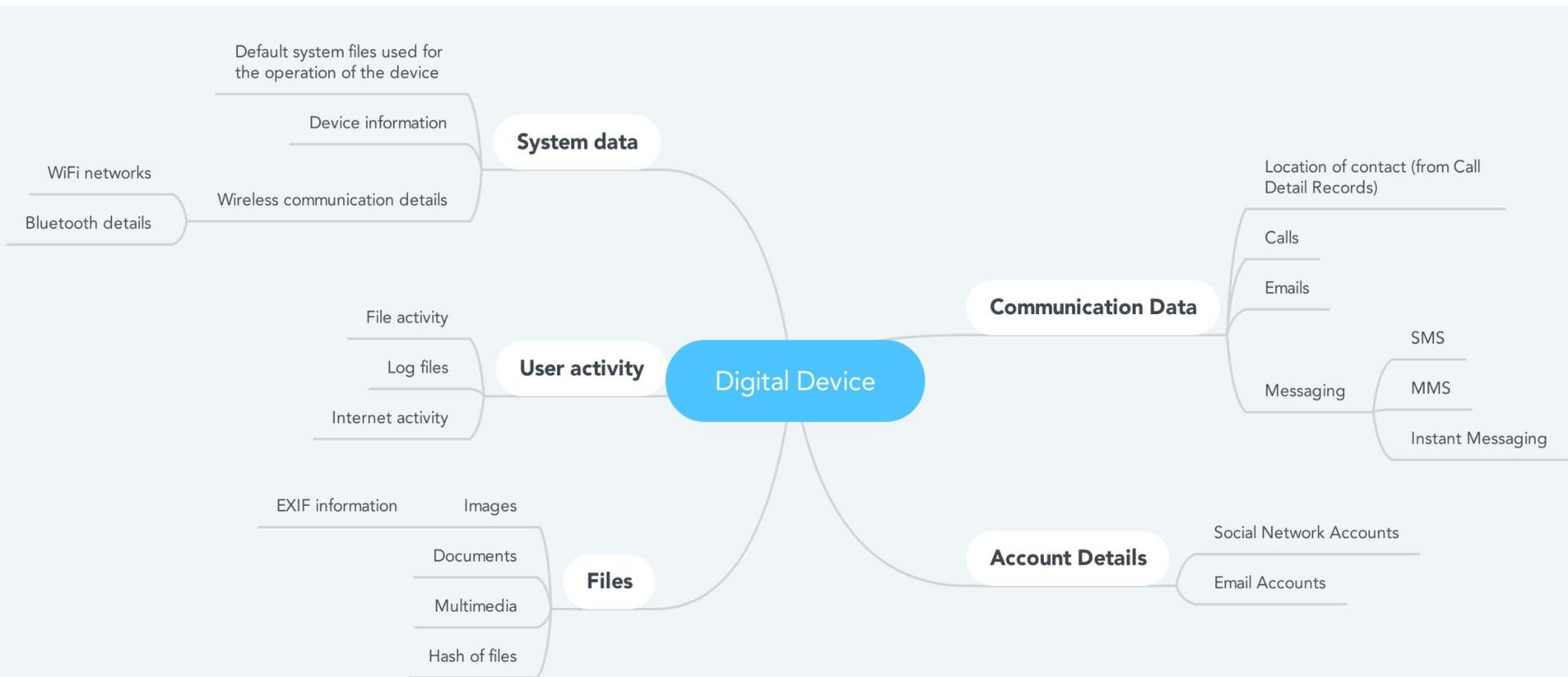
Can lead to “Push Button Forensics”





# CARI Project

## Potential Evidence





# CARI Project

## Motivation for a new approach

Not enough time to conduct an investigation

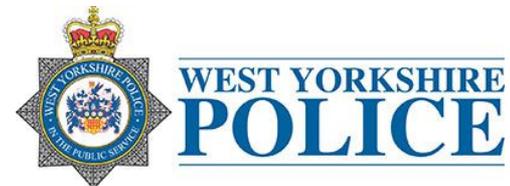
Current tools make it hard to investigate different device types and generally specialise in a certain area - looking at either phones or computers

Each of the tools produce different outputs

Proprietary: XRY, UFED

'Standardised': HTML, XML, XLS, SQLite...

Other tools cannot read these outputs





# CARI Project

## WYP Current Forensic Tools

Phones/Sat Nav/Tablets

XRY

UFED

Oxygen

Computers/Laptops/Gaming Consoles

X-Ways

EnCase

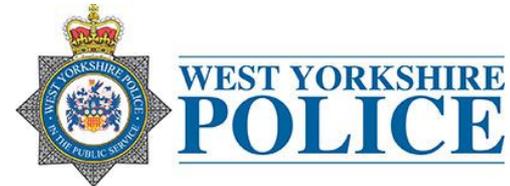
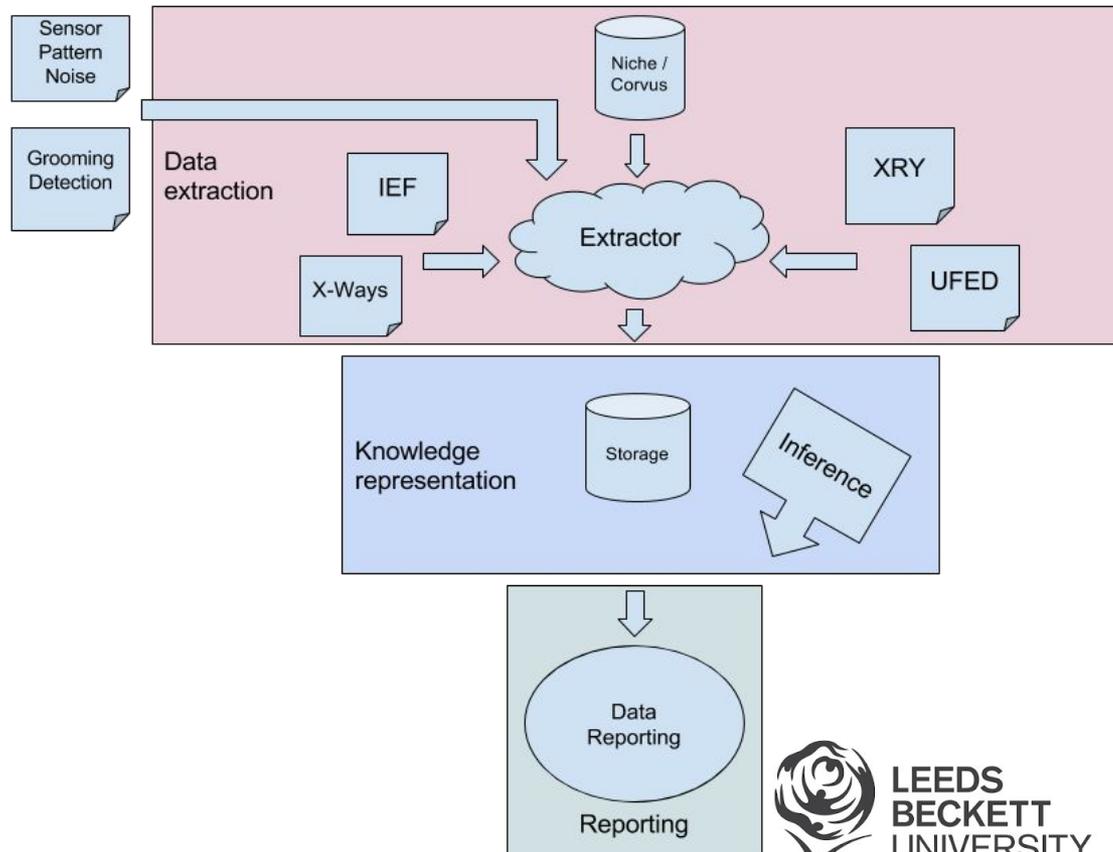
FTK

Internet Evidence Finder (IEF) / AXIOM



# CARI Project

## Developed Solution: Three Stages





# CARI Project

## Data Parsers

Parsers developed in Java

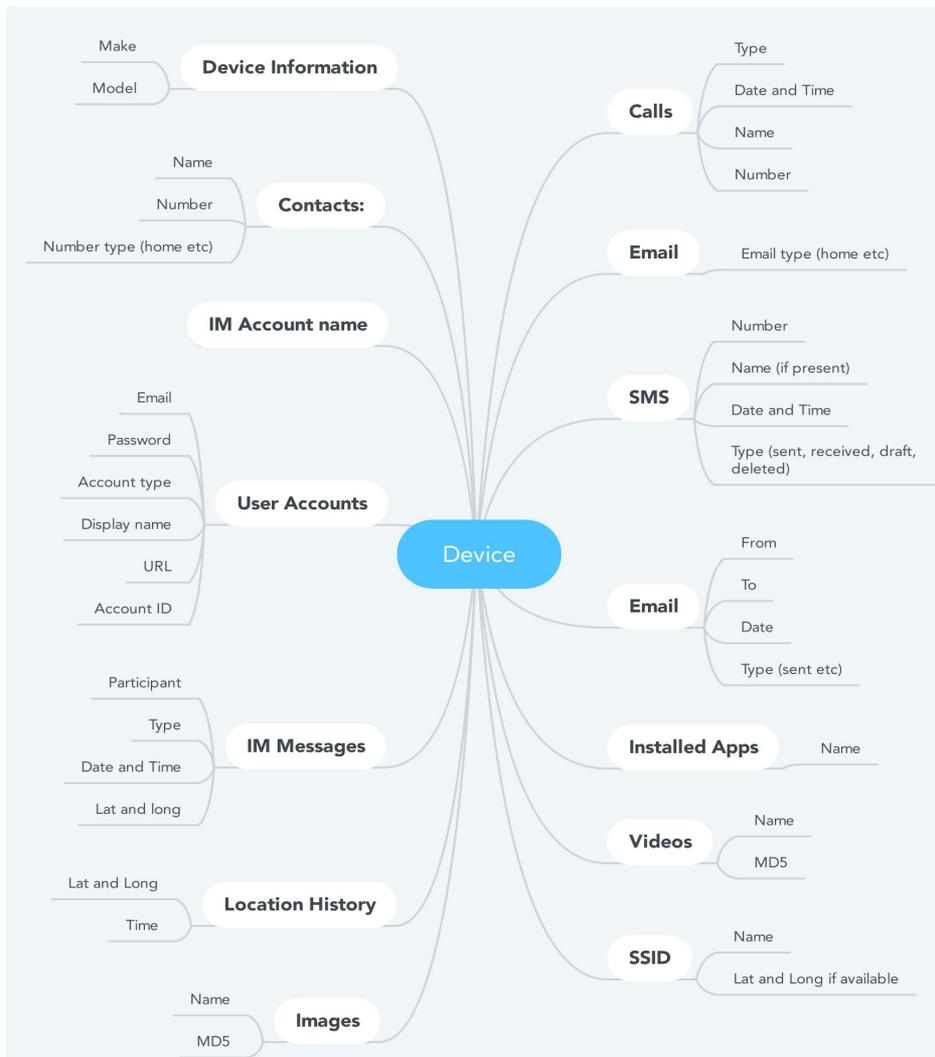
Phones: research and analysis of the XML format of

XRY

UFED

Computers: research and analysis of various tools and outputs

Autopsy



# CARI Project

## Parsed Information from Autopsy





# CARI Project

## Developed Solution - Ontology

Development of a common standard data representation which is populated by modular data extractors

Using Ontological data representation provides

- Definitions of concepts

- Relationships

- Constraints of Data

- Classification of Possible Relationships





# CARI Project

## Ontology

All data can be described by its base features

A contact on a phone has the following features:

Contact hasNumber NUMBER

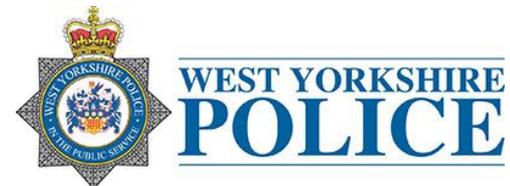
Contact hasfullName NAME

Contact hasFirstName FIRSTNAME

Contact hasLastName LASTNAME

Contact hasEmailAddress EMAILADDRESS

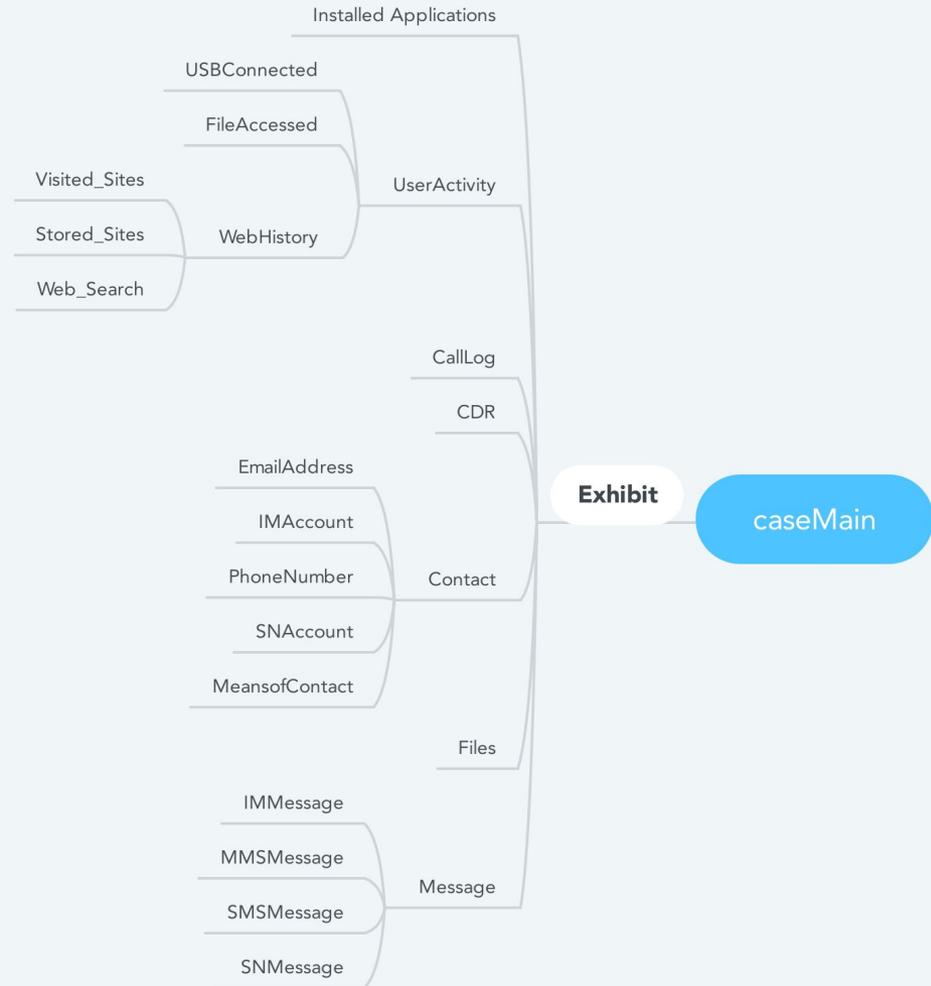
.....



# CARI Project

## Key Areas

These were created through discussion with examiners and through research. Also restricted based upon the outputs of the core forensic tools.





# CARI Project

## Ontology Storage

Each of the datasets are then loaded into a central 'database'

Apache Jena TDB stores

This loading of the data means that it is possible to centralise all of the data over time, allowing queries of cases and data not linked to this particular case.

Within the force the TDB would sit within the DFU





# CARI Project

## Data Queries

Once the data is a 'standard' format it is possible to then query

By storing it in a database it is possible to then query across multiple cases and exhibits

Return all case numbers and exhibit numbers where the telephone is set to 01138124440

```
SELECT ?caseNumber ?exhibitNumber
WHERE {
    ?caseNumber contains ?exhibitNumber
    ?exhibitNumber hasContact ?PhoneNumber
    ?PhoneNumber hasNumber 01138124440
}
```

caseNumber	exhibitNumber
SS/05/06	EMB/1
SS/05/06	EMB/3





# CARI Project

## Data Queries

As the output now contains all of the data from all cases and exhibits, it is possible to generate new queries to provide any information.

- All exhibits with a certain SSID

- All contacts known by an individual

- All names associated with a number

- ....

The strength of an ontology comes from the ability to infer from the data

- Allowing for previously unknown relationships to be identified

- If suspectA has the BluetoothMAC address of suspectB then it can be inferred that they have been in close proximity



# CARI Project

## Limitations

XML outputs will need to be created from the main phone forensic tools

This is not currently done, reports are generated as XLS

The use of Autopsy within the computer forensic investigation process

This is currently not done, although a relatively easy and non-labour intensive process

Tools may change outputs

Rigour of the tool will need to be tested





# CARI Project

## Evaluation

Is an ontological-based approach demonstrable as possible/practical for the analysis of digital evidence within the digital forensic unit?

**Yes, although further development is required to allow further queries**

Is it possible/practical to implement a reasoning system to assist in the analysis of digital evidence within West Yorkshire Police?

**Yes, although further development is required to allow further queries**

Is it possible, and effective, to generate and use data extractors to successfully extract data from the core tool outputs from within the Digital Forensic Unit?

**Yes and No. XRY, UFED completed. X-Ways lack of documentation made it difficult to complete in the timeframe, hence the move to Autopsy**



# CARI Project

## Impact

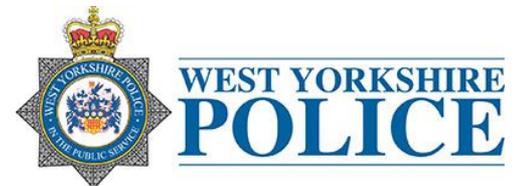
Connection between cases that are entered into the system

Historic and present day analysis of cases and data

Intelligent triage and analysis of exhibits outside of a siloed investigation

Improve investigations

More time to focus on a detailed investigation





# CARI Project

## Future work

Continued development of 'visualisation'/reporting of data output

Further work on the queries to provide more advanced queries across the data

Development of further parsers and integration with main tools within forces

Further testing and tuning against real-world data from UK police forces





# CARI Project

Questions





# BREAK





# Assessing the perceived effectiveness of cyber training

Dr Tom Cockcroft  
and  
Mohammad Shan-A-Khuda





# CARI Project

## Aims

To explore whether those who had undertaken cyber training since 2014 had preferences for different forms of training delivery

To understand the extent to which some forms of training were seen to be a better use of officer time

To understand the extent to which some forms of training were viewed as a more effective means of delivering particular content than others

To investigate the best ways of delivering refresher training



"Training lab" (CC BY 2.0) by mclib





# CARI Project

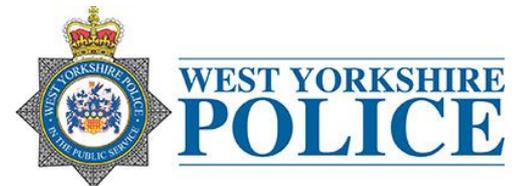
## Existing literature highlights...

Police training and education is an area of perennial interest (Bryant et al)

Police training needs to be delivered in a variety of ways and needs content to be evidence-based rather than drawn from 'received wisdom' (Griffith, 2015)

Problems arise because we do not have enough information in this area (Mastrofski, 2007)

Successful investigations rely on skilled staff and good quality training (Marcum et al, 2010)





# CARI Project

## Existing literature highlights...(cont.)

The growing prevalence of cybercrime has led to increased concerns about front line officers having the necessary skills and confidence to respond appropriately to cyber incidents (Holt and Bossler, 2012)

Cybercrime awareness and investigation skills needed to be embedded within local police officers (Police Executive Research Forum, 2014)

E-learning delivery should not be viewed as a means of producing cut price training and that it needs to be underpinned by technological and pedagogic expertise (Monett and Elkina, 2015)





# CARI Project

## Methodology

### Mixed Methods

1. Survey to gather a mixture of qualitative and quantitative data
2. Semi-structured interviews to contextualise the survey data

### Survey Sample

Circa. 600 officers

### Semi-Structured Interviews

Ex-trainer and an officer with Strategic Oversight of Training





# CARI Project

## Quantitative analysis (Reliability of the questionnaire and Research questions)

The questionnaire has a high reliability in all three training styles (Cronbach's alpha  $>.88$ ). It means that participants' scores across the 7 measures of perceived effectiveness are consistent with the overall aim in comparing the existing formal cyber training style in WYP.

Two research questions for quantitative study:

What do the 7 measures of perceived effectiveness in each training style tell us? Is there any unique characteristics of a training style?

Is there a training style preferred by the participants?





# CARI Project

## Research Question 1 (Factor analysis--Online training style) Rotated Component Matrix<sup>a</sup>

	Component	
	1	2
Format was appropriate for training delivered	.901	.109
Satisfaction with what learnt	.887	.164
Training received was relevant to job role	.228	.739
Will use any knowledge gained in job role	.091	.951
Knowledge has increased as a result of training	.692	.443
Skills have increased/improved as result of training	.758	.433
Job performance has improved as a result of training	.446	.756

Extraction Method: Principal Component Analysis.

Rotation Method: Varimax with Kaiser Normalization.

a. Rotation converged in 3 iterations.



# CARI Project

## Research question 2 (Assessing preferred training style through Paired sample t-test)

Comparing each of the 7 measures in each training style:

Participants scored considerably less for 'Online format was appropriate' ( $M = 2.94$ ,  $SD = 1.140$ ) than 'Face to face format was appropriate' ( $M = 4.60$ ,  $SD = 0.629$ ), a statistically significant decrease in average score of 1.66 on a scale of 1 to 5, 95% CI [-1.97, -. -1.33],  $t(66) = -10.26$ ,  $p < .001$ ,  $d = 1.66$  (Large effect).

Overall participants' perception between Online and Face to face training style differ significantly in all of the 7 measures of perceived effectiveness of a training style.





# CARI Project

## Research question 2 (Assessing preferred training style through Paired sample t-test)

Comparing overall score of each participant:

Participants' overall score for Face to face cyber training ( $M = 30.72$ ,  $SD = 4.811$ ) is considerably higher than Online cyber training style ( $M = 22.36$ ,  $SD = 5.275$ ), a statistically significant higher mean of 8.36, 95% CI [6.673, 10.047],  $t(49) = 9.956$ ,  $p < .001$ ,  $d = 1.4$  (Large effect)

The quantitative results strongly suggest that participants preferred Face to face training style to Online and Workshop training style in terms of every one of the individual measures, and also in terms of the total score comparison.

The quantitative data did not indicate any situation where Online or Workshop was more effective than Face to face.

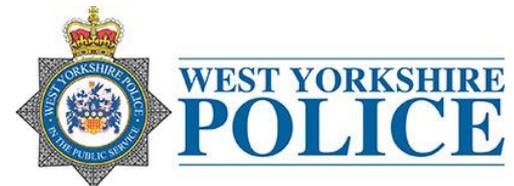




# CARI Project

## Findings - Survey - Qualitative (1)

Online learning was viewed as accessible and unconstrained in terms of pace of learning. Likewise, it cut down on logistical issues of attending a training event at somewhere other than a member of staff's regular workplace. However, it was viewed as not encouraging a particularly deep level of learning, as being limited due to the lack of interaction and not appropriate for complex subjects. It was viewed as appropriate for basic or refresher training, or as a learning stage to be delivered prior to attendance on a classroom-based session.





# CARI Project

## Findings - Survey - Qualitative (2)

Face to Face learning was viewed very positively due to the interactive elements of it. The presence of skilled and knowledgeable trainers was valued by those attending sessions and the ability to seek clarification on complex issues was perceived very positively. Likewise, the group nature of such events allowed for learning and clarification through the sharing of experiences with other participants. A significant proportion felt that this mode of delivery was appropriate for all training with more nuanced responses identifying its particular strengths in relation to complex subject areas (such as cyber) and those with a practical element.





# CARI Project

## Findings - Survey - Qualitative (3)

Respondents asked to identify the characteristics of their ideal training session suggested that it would be face to face, involve a classroom environment and have relevance to practice. They also suggested that a combination of online and face to face training could work well.





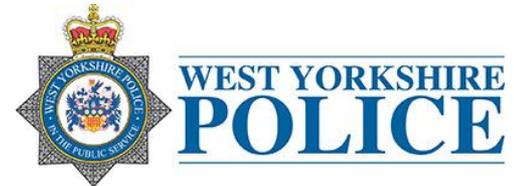
# CARI Project

## Findings - Semi-Structured Interviews

Modes of Delivery

Resources

Strategic Positioning of Cybercrime





# CARI Project

## Key Themes of Discussion

Evidenced Knowledge and Experiential Knowledge

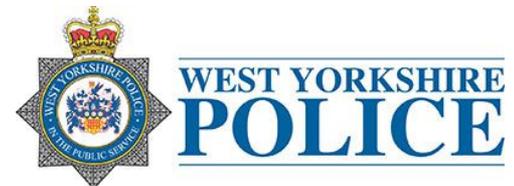
Quality

Resources

Positioning of Knowledge within the Organisation

Online Learning

Pace of Technological Change





# CARI Project

## References

Bryant, R, Cockcroft, T, Tong, S, Wood, D, (2013) 'Police Training and Education: Past, Present and Future' in J. Brown (ed), The Future of Policing, Abingdon: Routledge.

Griffith, D. (2015), '25 Ways to Make Police Training More Effective', Police: The Law Enforcement Magazine, <http://www.policemag.com/channel/careers-training/articles/2015/04/25-ways-to-make-police-training-more-effective.aspx> (last accessed on 31/10/16).

Holt, T.J. and Bossler, A.M., 2012. Predictors of patrol officer interest in cybercrime training and investigation in selected United States police departments. *Cyberpsychology, Behavior, and Social Networking*, 15(9), pp.464-472.

Marcum, C.D., Higgins, G.E., Freiburger, T.L. and Ricketts, M.L., (2010). 'Policing Possession of Child Pornography Online: Investigating the Training and Resources Dedicated to the Investigation of Cyber Crime'. *International Journal of Police Science & Management*, 12(4), pp.516-525.

Mastrofski, S. (2007), 'POLICE Organization and Management Issues for the Next Decade', Paper Presented at the National Institute of Justice (NIJ) Policing Research Workshop: Planning for the Future, Washington, DC, November 28-29 2006.

Monett, D. and Elkina, M. (2015), 'E-Learning Adoption in a Higher Education Setting: An Empirical Study', Proceedings of the Multidisciplinary Academic Conference, Prague, October 2015.

Police Executive Research Forum (2014), The Role of Local Law Enforcement Agencies in Preventing and Investigating Cybercrime, Washington, DC: Police Executive Research Forum.





# Evaluation of the role of the Digital Media Investigator in West Yorkshire Police

Daniel Horvath





# CARI Project

## Aims

Evaluate the role of Digital Media Investigators within West Yorkshire Police

Identify any gaps between the DMI training, support and resources currently provided and what may be required

Inform the force training school, WYP policy and the College of Policing.



"parallel lines" (CC BY-SA 2.0) by their





# CARI Project

## Introduction: What is a Digital Media Investigator?

Digital Media Investigators are accountable for:

- Development of an effective technology and data strategy for investigation / operation
- Timely and effective input from SPoC, Digital Forensics, Open Source and ANPR/CCTV functions into investigation / operation to meet technology and data strategy
- Appropriate management of digital media within investigation / operation to meet prosecution needs, including development of appropriate evidence as well as disclosure of appropriate excess information



LEEDS  
BECKETT  
UNIVERSITY



WEST YORKSHIRE  
**POLICE**



# CARI Project

## Needs Assessment

### Participating departments:

- Technical Support Unit
- Covert Authority Bureau
- Homicide Team
- Cyber Unit
- Economic Crime Unit
- Digital Forensics Unit
- Head Of Communications
- Telecoms Unit
- Crime Researchers/Analysts
- Contact Communications Centre
- Neighbourhood Policing Team
- Divisional Control Room Supervisors
- Dedicated Source Unit
- Chief Inspectors
- Training Team
- Senior Investigators





# CARI Project

## Issues highlighted

There aren't enough Digital Media Investigators

The Digital Media Investigator role is part-time therefore increasing the officer's workload.

It is hard to implement any effective training relevant to the role due to the part-time status.

The Digital Media Investigator training is “obsolete” and “out of date”.

General confusion and misunderstanding around the role.





# CARI Project

## Evaluation of the role of the Digital Media Investigator in West Yorkshire Police

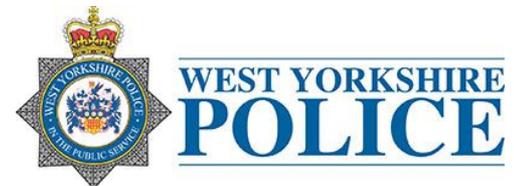
Investigate the issues highlighted.

Evaluate the role in it's current state.

Improve the effectiveness of DMI.

Better utilise the DMI.

Scope: West Yorkshire





# CARI Project

## Design

Identify additional subject areas for investigation:

- The role of DMI's in West Yorkshire Police;
- Training received versus required for the role;
- Equipment available to DMIs;
- Support/ training received after completion of DMI course.

The Digital Media Investigator survey

Focus groups & 1-1 Interviews

Report





# CARI Project

## The Digital Media Investigator survey

### Overview

- 15 Questions
- Qualitative and Quantitative
- 34 invitees comprised of:
  - DMIs,
  - DMI course trainers within WYP,
  - Digital Media Coordinator.

### Statistics

- 61.8% Response rate
- 21 Participants
- 18 Police Officers
- 3 Police Staff





# CARI Project

## Findings

56% of DMIs report that DMI duties interfere with existing officer duties

61% of DMIs think that the role should be full time.

62% of DMIs report that all the equipment they need to perform the role is not readily available to them.

67% of DMIs report that their time is spent 20% on DMI and 80% on other.





# CARI Project

## Findings (cont.)

Approximately 50%/50% split feel that the role profile is/isn't an accurate reflection of the role of the DMI. DMIs that felt the role differed from that of the role profile had the following to report:

Only advisory/advice SPOC and have never been asked to complete any items raised on the role profile

Viewed as an open source and social media downloader.

Do not get to sit in on serious and complex crime cases from the outset. Hostility from others who feel the role is taking away from their own.

DMIs will struggle to deliver high quality investigations without access to up to date and capable equipment.



# CARI Project

## Findings (cont.)

If Yes, how would you rate the DMI training you have received in terms of:	Very Poor		Poor		Fair		Good		Excellent	
	Freq.	%	Freq.	%	Freq.	%	Freq.	%	Freq.	%
The relevance of the topics covered	0	0.0%	2	10.0%	0	0.0%	12	60.0%	6	30.0%
The level of technical detail	2	10.0%	2	10.0%	7	35.0%	8	40.0%	1	5.0%
The time allocated for training	1	5.0%	1	5.0%	6	30.0%	9	45.0%	3	15.0%
The regularity of the courses	4	20.0%	5	25.0%	8	40.0%	3	15.0%	0	0.0%



# CARI Project

## Findings (cont.)

The DMIs were asked to provide explanations if they have responded with poor or very poor. The top recurring themes included:

- No follow up training. (DMIs felt they were losing skills due to not being utilised immediately/having no follow up training to consolidate learning).
- The technical detail within the DMI course was poor and didn't cover key areas (Wi-Fi, Routers, OSR).
- Felt that the course just taught them how to fill in RIPA forms.
- Felt the course was pitched to the wrong level. Either aim the course at technical minds or complete novices. (Due to methods/practices being explained on a very basic level as some did not understand).



LEEDS  
BECKETT  
UNIVERSITY



WEST YORKSHIRE  
**POLICE**



# CARI Project

## Key areas of Investigation

- Training
- Equipment
- Information sharing between DMIs
- Support available for DMIs
- The role profile of a Digital Media Investigator
- Full time or part time role?
- A Digital Media Investigators Work-load





# CARI Project

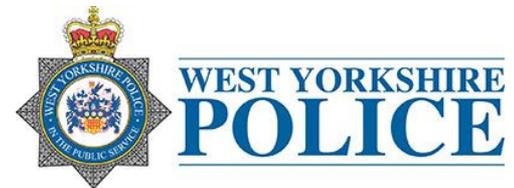
## Discussions

10 Participants

2 Focus Groups

5 One to one interviews

Analysed through thematic analysis





# CARI Project

## Conclusions

Digital Media Investigators do not have the time to perform as an officer and be an effective Digital Media Investigator.

- A lot of pressure to keep up to date with tech.
- Protected learning time not always available
- Having to work longer in order to stay on top of main role.
- Extensive role profile.





# CARI Project

## Conclusions

It was observed that there wasn't a structured implementation plan put in place for Digital Media Investigators within West Yorkshire Police.

- Digital Media Investigators that were trained, simply re-joined their department.
- During that time they have been either proactive/reactive in receiving DMI duties or not been tasked at all.
- The majority of active Digital Media Investigators do not have sufficient equipment available to them in order to perform their role effectively.
- Digital Media Investigators haven't been told specifically what DMI's should or should not be doing. This has resulted in un-standardised Digital Media Investigators throughout the force.





# CARI Project

## Conclusions

Not enough education around the role of the DMI and what value it can bring to an investigation.

- If more people were aware of the capabilities of a DMI then the higher the impact the specialised role would have on investigations.
- This would also have a positive impact on securing future investment for Digital Media Investigators.





# CARI Project

## Conclusions

There is no formal, structured, continuous professional development plan put in place for Digital Media Investigators that is compulsory.

- Local networking events for Digital Media Investigators within West Yorkshire and that the College of Policing offer 'DMI' days that aim to refresh knowledge.
- No formal training plan which outlines set DMI duties and what training they need in order to meet those requirements.





# CARI Project

## Conclusions

The participants in the study feel that the role of the Digital Media Investigator is a full-time role.

- Benefit of placing Digital Media Investigators strategically throughout WYP..
- Proactive assistance on technical enquiries
- More time and care spent on digital enquiries/investigative strategies due to less pressures from an officer's workload, providing a better public service.

A passion and interest in technology is a key factor in the effectiveness of a Digital Media Investigator.

- Mentioned heavily throughout the discussions and the DMI survey.





# CARI Project

## Recommendations

Introduce a selection process for the Digital Media Investigator Training course that has a pass/fail requirement in order to ensure those undertaking the role have a sufficient vested interest.

Standard equipment checklist can be introduced in line with the duties that will be performed.

Education produced around what a Digital Media Investigator can offer an investigation and the value of investing in a DMI.

Digital Media Investigators may become out-dated within the next five years when current specialist knowledge becomes mainstream. Therefore it is crucial that the role continues to specialise and develop.

Plus lots more, detailed in the main report!



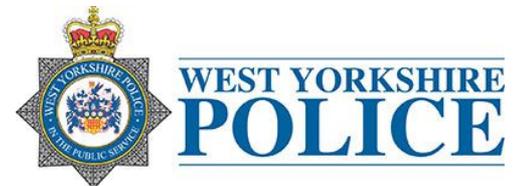


# CARI Project

## Forward thinking

Detective Chief Inspector Vanessa Smith is preparing a paper to the Chief Officer Team around the restructuring of the Digital Media Investigators within WYP.

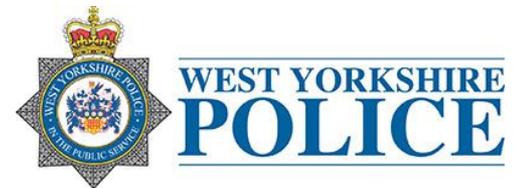
The forensic examination of digital devices and electronic networks policy utilises the role of the Digital Media Investigator as a district advisor in respect to giving advice around additional digital lines of enquiry.





# CARI Project

Questions





# Characteristics of Victims of Cybercrime

Mohammad Shan-A-Khuda





# CARI Project

## Overview

Motivation

Cybercrime victims in West Yorkshire

Key findings

Impact on West Yorkshire Police

Future work



"Happy Planet 2" (CC BY 2.0) by Patrick Doheny





# CARI Project

## Motivation

Developing evidence based profiles of cybercrime victims within West Yorkshire

Developing more holistic insight into cybercrime victims based on:

- Demographics of victims (age, gender)

- Area profiles (socioeconomic measures, such as employment/profession, qualifications, ethnicity, income)

- Beyond simple descriptive statistics (correlations)

Present 'profile' predictions





# CARI Project

## Latent Class analysis and Cluster analysis

*“Latent class analysis can best be thought of as an “improved” cluster analysis, which uses statistical (rather than mathematical) methodology to construct the results. It is based on the statistical concept of Likelihood. Parameters are estimated for: Class profiles (the description of each class) and the size of each class. An important difference is that cases are not absolutely assigned to classes, but have a probability of membership for each class.”*

- Professor Brian Francis, Workshop on Methods for Analysing Crime Data on 18th and 19th May 2016 at Lancaster University





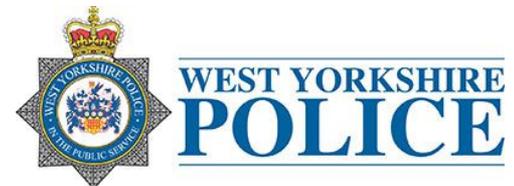
# CARI Project

## The Dataset

Time period: 01/07/2014 to 30/06/2016

Total cases recorded: 7,364 and Total cases included in the final analysis: 4,092 (Deletion of missing Gender and Age)

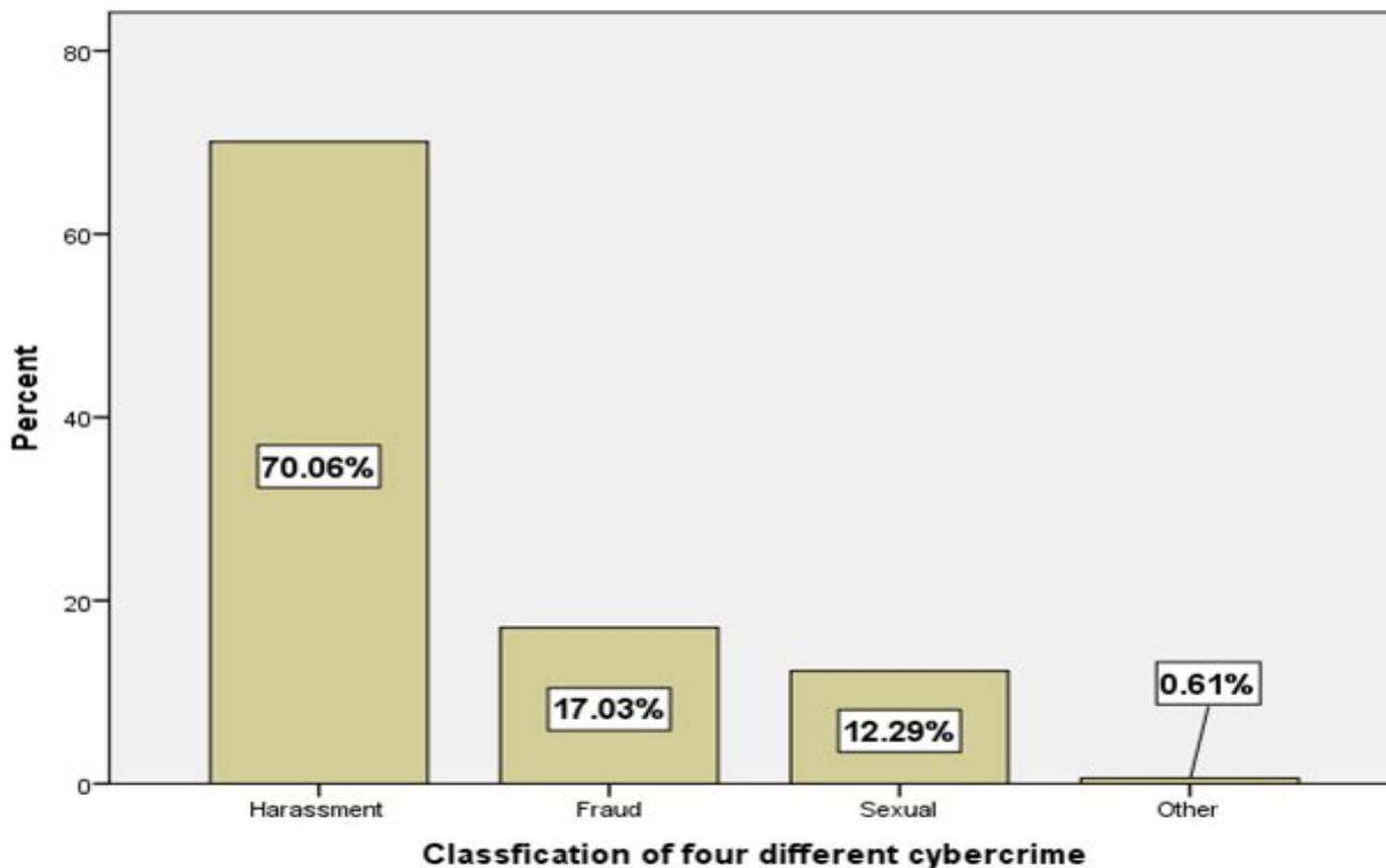
Data sources: West Yorkshire Police datasets, linked with external data sources, such as Census 2011





# CARI Project

## The Dataset: Classification of cybercrimes

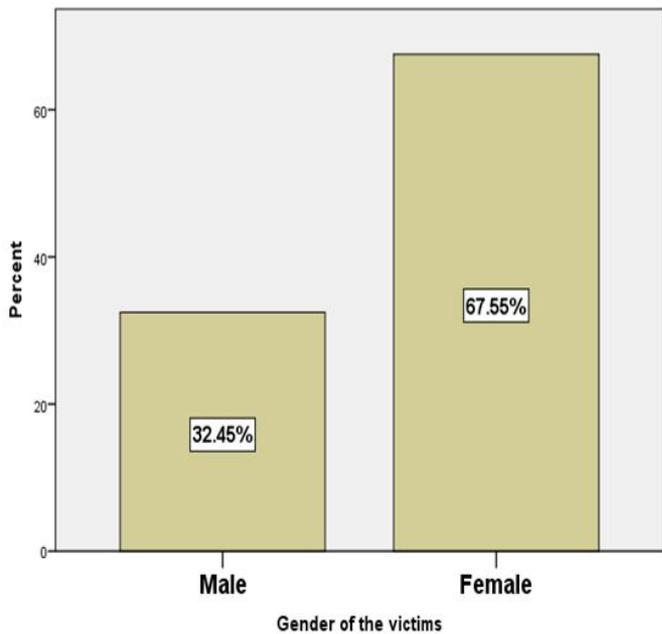




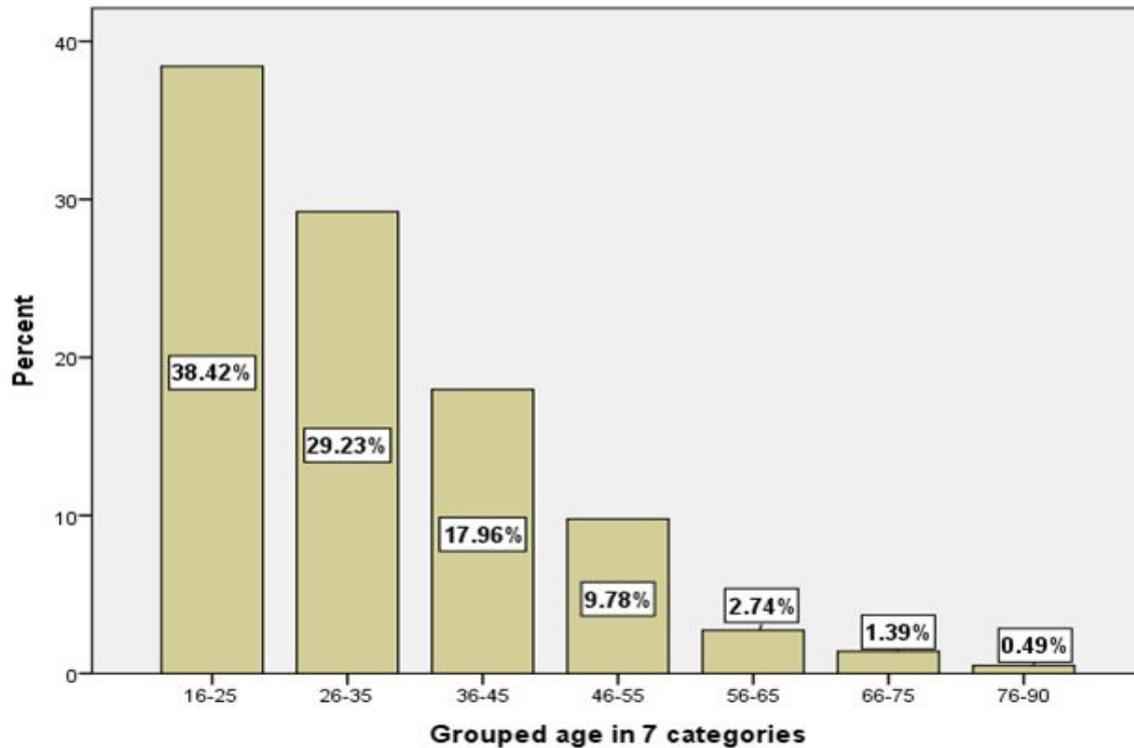
# CARI Project

## Cybercrime victims in WYP: Descriptive

Gender



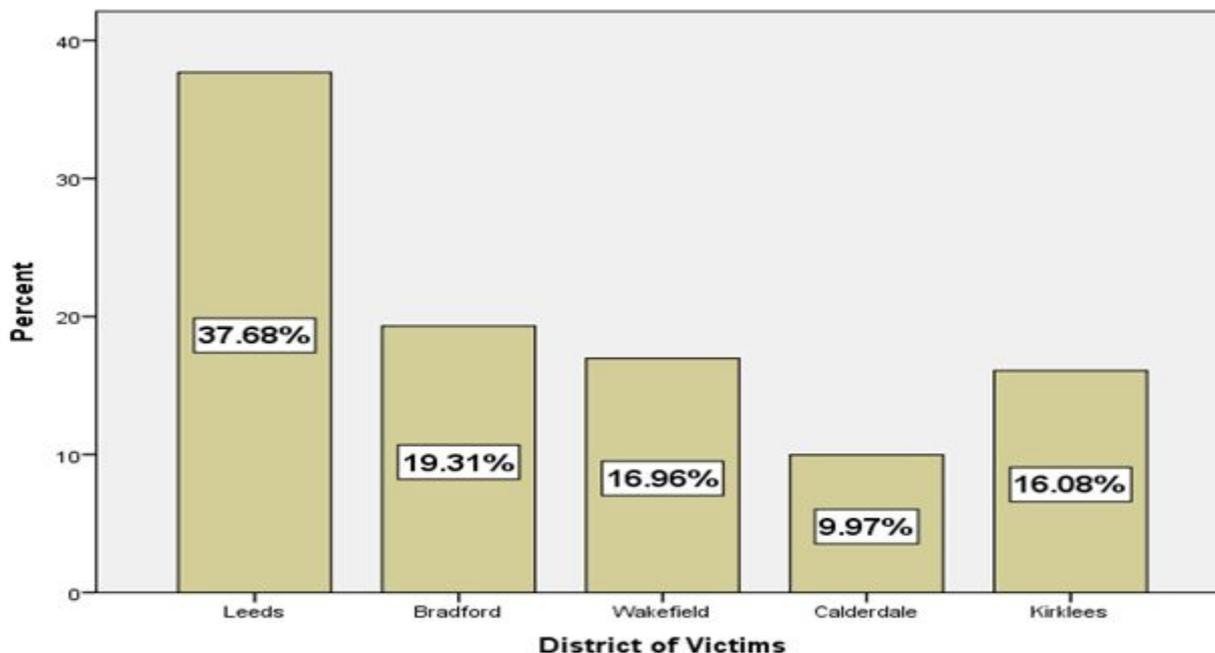
Age groups





# CARI Project

Proportion of victims within the five districts





# CARI Project

## Model selection (model with age and gender)

Model with minimum LL, BIC, AIC(LL), L2 is selected.

Models	Number of clusters	LL	BIC (LL)	AIC (LL)	AIC3(LL)	Np ar	L <sup>2</sup>	df	p-value
Model 1	1-Cluster	-6042.5845	12118.4362	12093.1690	12097.1690	4	5786.6479	206	3.5e-1066
Model 2	2-Cluster	-4145.0872	8423.2431	8322.1745	8338.1745	16	1991.6533	194	2.5e-295
Model 3	3-Cluster	-3283.3698	6799.6098	6622.7397	6650.7397	28	268.2185	182	3.3e-5
Model 4	4-Cluster	<b>-3167.9461</b>	<b>6668.5637</b>	<b>6415.8922</b>	<b>6455.8922</b>	<b>40</b>	<b>37.3710</b>	<b>170</b>	<b>1.00</b>



# CARI Project

## Key findings: Age and gender

Vulnerabilities to cybercrime vary among male and female of different age groups, and importantly, the different types of areas they live in.

Females are much more likely to become victims than males for two types of cybercrimes: 'Harassment/Unwanted contact', and 'Sexual/Indecent'.

The likelihood of becoming victim to 'Harassment/Unwanted', 'Fraud/Theft/Handling' and 'Sexual/Indecent' type cybercrime decreases with the increase of AGE.





# CARI Project

## Key findings: Age and gender (continued)

16-35 year old females are more vulnerable to 'Harassment/Unwanted contact' type cybercrime.

16-25 year old females are much more vulnerable to 'Sexual/Indecent' type cybercrime.

16-45 year both males and females are particularly vulnerable to 'Fraud/Theft/Handling' type cybercrime.





# CARI Project

## Key findings: Areas

Females living in areas with higher number of Professional occupations, and managers/directors/senior officials, skilled trade, Level 3 qualifications are more likely to become victim to 'Harassment/Unwanted contact' than areas with lower number of the above mentioned six categories.

Both males and females living in areas with considerably higher number of Full Time Students and Asian are more likely to become victim to 'Fraud/Theft/Handling' than lower level of these two categories.

16-25 years females living in areas with higher number of full time students are more likely to become victim 'Sexual/Indecent' type than lower number of full time students.



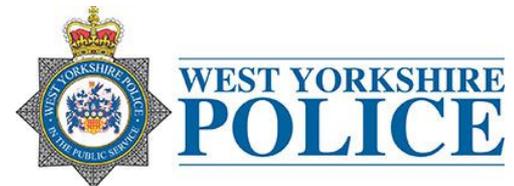


# CARI Project

## Key findings

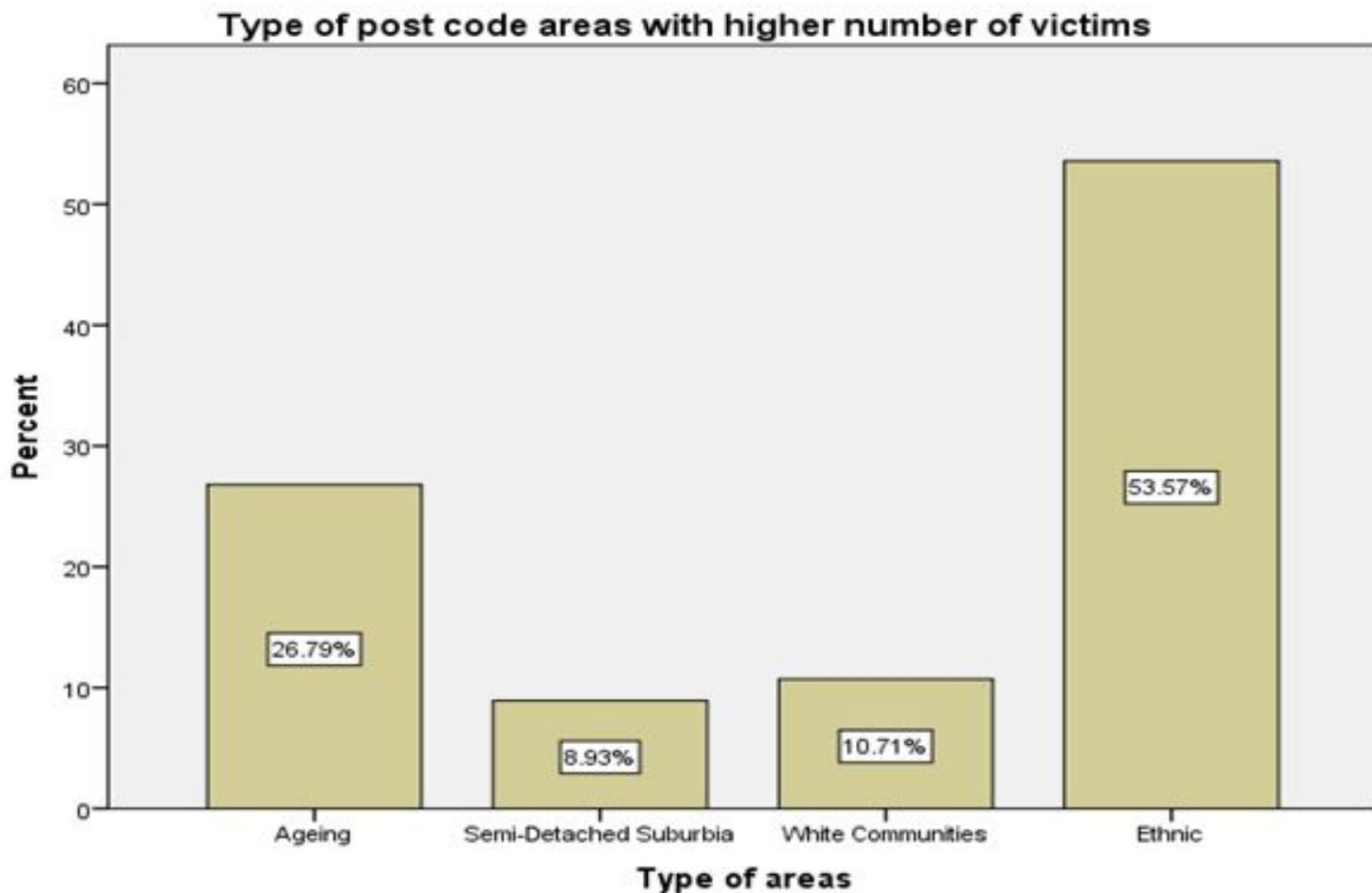
In the hotspots\*\* areas of cybercrime victims, majority of the victims are 16-25 year females (48.2%). In addition, more than half (54.5%) of the males are from Bradford and more than half (51.1%) females are from Leeds in these hotspot areas of cybercrime.

\*\* where more than 3 or 4 number of incidents reported from same post-code



# CARI Project

Key findings: Hot spots (Areas with 3+ victims)





# CARI Project

## Impact on West Yorkshire Police

WYP complies with the National Policing Children and Young Persons Strategy 2013-2016. 18-24 year age range is a key stage of development.

Providing a picture of the vulnerabilities of these younger cybercrime victims compounded with societal aspects.

Helps to build the relationship between young people and the police, a key priority area identified in the National Policing Children and Young Persons Strategy 2013-2016.





# CARI Project

## Impact on West Yorkshire Police

Some of the positive changes from this project will be assessed over time. However, there are positive short term changes that have come about as a result of this work.

WYP police staff who were involved with this project (directly or indirectly) have developed a recognition of the benefits of linking external datasets such as geographical variables with the core victim dataset in underpinning the characteristics of cybercrime victims.

WYP can use this information when designing awareness-raising programmes, to target the information based on specific areas, age, and sex of the target audiences

WYP are now aware of the identified hot spots, and are planning accordingly





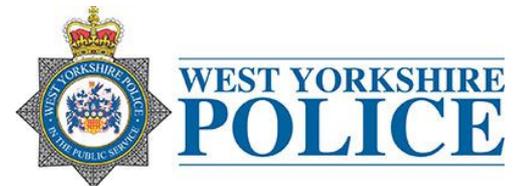
# CARI Project

## Future work

Develop software for automatic victimisation prediction based on the profiles of different types of cybercrime victims.

To understand the cybercrime victims' area variation in depth through further multilevel statistical modelling. These models could be used to explain the differences of victimization between and within districts.

To devise a vulnerability index for different areas of West Yorkshire, and share the knowledge and lessons learned with other police forces.





# Broadcast Media Artefacts

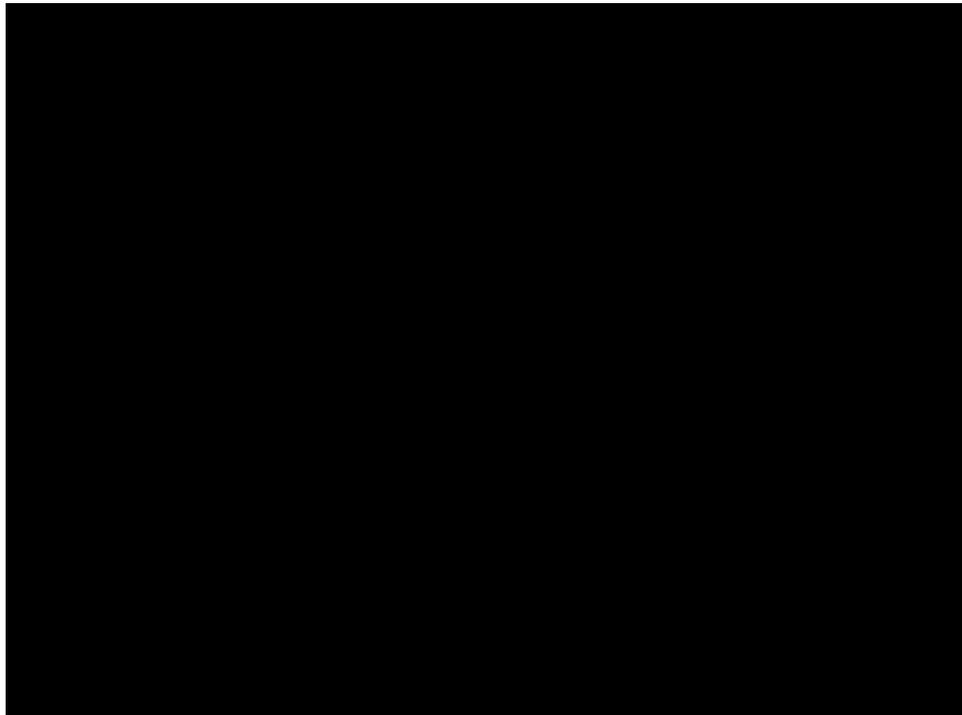
Hugo Smith





# CARI Project

All about the impact...





# CARI Project

## Why impact?

For academics and public service organisations there is a pressing need to generate impact for the public and for service users.

We need impact for funding.

We need impact for relevance.

We need impact to generate and consolidate public confidence.

Our work exists to benefit society, not simply ourselves. Spreading good practice is key to academic excellence and in public service delivery.

Impact is therefore a key a measure of research excellence.





# CARI Project

## How Impact?

For this project we aim to generate additional impact through delivering a variety of layers of professionally produced media content.

The Conference proceedings are being recorded for future use by partners and to assist with generating impact within and out with academic circles.

Short-form “Twitter Videos” are being produced to generate social media traffic towards papers and outputs of CARI projects as they are published/need promotion.

A longer-form Documentary project is in production/post-production that, it is hoped could generate broad impact through online and/or TV distribution.





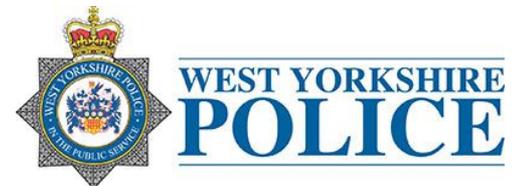
# CARI Project

## Production and Progress

Twitter films are largely finished but awaiting final graphics and links to papers

Recordings of the conference proceedings can be readied for publication as soon as today is finished as required.

Documentary needs filmed content of projects reaching fruition/in action and would benefit considerably from case-based content or officer-based narrative if it is to make TV broadcast but will provide a strong record of academic work across the project and of value/relevance to WYP officers at various levels.





# CARI Project

## Benefits and Challenges

The benefits of getting one's message to a broad audience are clear. (confidence in service, extension of knowledge for public good, drivers to academic papers and positive publicity for public servants).

The challenges have become clear: there is a huge appetite for stories relating to cyber but there is a perfectly reasonable worry within police forces about operational procedure and exposing victims and colleagues to 'media production', even when it isn't necessarily hostile. Can mainstream media take in-house production seriously?

How do we spread valuable messages most effectively? How can or even should we develop trust in a world where everyone with a camera is looking to trip us up? How can we tell our story truthfully and with narratives that are relate-able for peers and public?

I'd like to take this to the panel, if I may?





# Q&A Panel: Future Directions of Cybercrime and Policing





# Police Crime Commissioner Closing Statements

Mark Burns-Williamson  
Police and Crime  
Commissioner for West  
Yorkshire

