CARI Project

An Evidence-based Evaluation of the Role of the Digital Media Investigator Within West Yorkshire Police

Daniel Horvath, Abbey Wren, Lewis Collins, Pip Trevorrow, and Z. Cliffe Schreuders

Leeds Beckett University and West Yorkshire Police

2018

This is a *pre-print*, in the process of undergoing academic publication.

The CARI Project

The CARI Project is a large-scale collaboration between West Yorkshire Police and the Cybercrime and Security Innovation Centre (CSI Centre) at Leeds Beckett University. The CARI Project aims to improve and incorporate an evidence-based approach into the policing of digital forensics and cybercrime investigations. An extensive needs assessment of UK policing and cybercrime and digital evidence was conducted to understand the current situation, and to identify needs across the force. The CARI Project also involved implementing a training and research programme that has impacted the capability of the digital forensics and cyber units within West Yorkshire Police to engage in research. This needs assessment and research training led to the development of a set of research proposals, which were scored and selected. Subsequently, academics and police staff co-produced 9 research and development workstreams: a framework for seizure, preservation and preservation of cloud evidence; 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; an evaluation of the role of the Digital Media Investigator within WYP; and characteristics of victims of cybercrime. Each of these projects were designed to address needs within law enforcement and outputs include evidence-based procedures, new capabilities such as software/algorithms, and actionable intelligence.

This work was supported by a Police Knowledge Fund grant, administered by the Home Office, College of Policing, and the Higher Education Funding Council for England (HEFCE).

LEEDS BECKETT UNIVERSITY

WEST YORKSHIRE POLICE

Contents

Executive Summary

The main objective of this project was to perform an evidence-based evaluation of the role of the Digital Media Investigator using feedback and comments from the Digital Media Investigators themselves. The motivation for the project emerged from the needs assessment that was performed as part of the CARI project (Schreuders et al, 2017), it was found that there was a general confusion and misunderstanding surrounding the role of the Digital Media Investigator. The scope for this project was the region of West Yorkshire. The objective will be achieved by reviewing all aspects of DMIs:

- The role of DMI's in West Yorkshire Police
- How they are currently utilised
- How they could be utilised
- Training received versus required for the role
- Equipment available to DMIs
- Support/ training received after completion of DMI course

A literature review was performed to obtain an understanding of how cybercrime is tackled nationally and globally, followed by what is currently ongoing in the UK (policing specifically), in response to an increased cybercrime threat. The UK is also combatting cybercrime via frontline policing. Numerous forces in UK are now setting up cybercrime units in order to combat the rise of cyber-enabled crime and provide investigators with specialist knowledge in the preservation of digital evidence.

The methodology adopted was to use the gaps identified in the needs assessment analysis to create the questionnaire for a survey, which was then administered to the Digital Media Investigators throughout West Yorkshire Police and the responses and analysis of the survey fuelled the focus groups to follow. Focus groups and interviews were then held with the DMIs, using a specific set of questions that were derived from the survey responses.

The survey was distributed to 34 individuals and amongst them included Digital Media Investigators, the Digital Media Investigator trainers and the Digital Media Coordinator. The survey was compromised of 15 questions inviting both qualitative and quantitative responses from the participants. The response rate to the survey was 61.8%. Once the analysis was complete and the results were obtained, some of the observations made were:

- The technical detail in the training course was poor and didn't cover key areas
- Equipment needed to perform the role is not readily available
- DMI role should be full time
- Technical support from specialised units
- There was no information sharing between different districts

The next stage of the evaluation involved using the results from the DMI survey to structure a series of focus groups and interviews with 10 participants from the following areas; district officers, specialist units and the Digital Media Co-ordinator. The subject areas covered were: training, equipment, full-time (for and against), technical support from other units, information sharing, the work load of a DMI, role differences between the role profile and actual role performed. Some of the questions asked the respondent how they would want the role to be improved. The responses were analysed via a thematic analysis. The data recorded provided in-depth knowledge about each areas to help the elicitations of the observations.

Based on the observations made from the survey, focus groups and interviews, it was found that the Digital Media Investigator role is still going through a development phase and the main findings are:

- Digital Media Investigators reported not having the time to perform as an officer and be an effective Digital Media Investigator
- A more structured implementation plan would assist Digital Media Investigators
- Not enough people are aware of the capabilities of a DMI to help an investigation
- There is no formal, structured, continuous professional development plan put in place for DMIs
- The DMI survey concluded in favour for the position to be full-time
- It was identified that an important factor in the effectiveness of a Digital Media Investigator was a passion and interest for technology

Based on the findings of this research recommendations were proposed in the following areas:

- Core duties of a DMI should be clearly defined
- DMI Training – introduce selection process, more refreshment days
- DMI Equipment – standard hardware and software checklist
- DMI role
    - Full time – proactive assistance
    - Part time – role must be purely in an advisory capacity that is reactive
- DMI role profile based on core duties
- Support from specialised departments (e.g. CCT and DFU)
- Information sharing between DMIs

1.0 Introduction

The goal of this project is to provide an effective evaluation of the role of the Digital Media Investigator using feedback and comments from the Digital Media Investigators themselves. This is in order to create an unbiased evaluation directly from the point of view of a Digital Media Investigator.

1.1 Scope

The scope for this project was the region of West Yorkshire. This was decided due to a mixture of reasons. The Digital Media Investigator is a role that the College of Policing released nationally, therefore if the scope were wider, it would not be possible to complete such a thorough evaluation under the current time constraints. By keeping to a scope of West Yorkshire, it would allow us to perform an in-depth analysis of the current state of Digital Media Investigators and explore all areas whether they be successful or problematic.

1.2 Aims & objectives

The aim of this project is to perform an evidence-based evaluation of the Digital Media Investigators in the West Yorkshire Police. This will be achieved by reviewing all aspects such as: The role of DMI's in West Yorkshire Police; How they are currently utilised; How they could be utilised; Training received versus required for the role; Equipment available to DMIs and support/ training received after completion of DMI course. Through these aims we hope to better utilise and improve the effectiveness of the Digital Media Investigator within West Yorkshire Police.

2.0 Research & Design

During the needs assessment it quickly became apparent that there was a general confusion and misunderstanding surrounding the role of the Digital Media Investigator. Therefore a proposal was made to investigate and evaluate the role of the DMI within West Yorkshire Police.

This section examines the research that took place before the project development stage, covering areas such as the review of literature and the research methodology.

2.1 Literature review

This project aims to evaluate the role of the Digital Media Investigator within West Yorkshire Police. However as the role is new, there was little information publicly available about it.

The literature review will aim to look at how cybercrime is tackled nationally and globally, then analyse what is currently ongoing in the UK (policing specifically), in response to an increased cyber-crime threat.

Giles Herdale from the College of Policing stated that Cybercrime was a classified as a tier 1 national security threat in 2010 and recognised that within the next few years cybercrime is going to become a meaningless term and will just be referred to as crime. He also discusses that 3000 officers nationally will complete the Mainstreaming Cybercrime Course which provides insights into recognizing sources of digital evidence that can support any investigation and the Digital Media Investigator training which also provides knowledge to investigators about different sources of digital evidence (College of Policing, 2014).

Cyber Crime is a global problem and how it is dealt with varies by different governments and police forces. By recognizing the approaches implemented on a global scale, we can gain an increased understanding into how to handle and deal with Cyber Crime in the most effective manner possible.

2.1.1 How the USA is tackling Cyber-Crime

American forces are recognizing that cybercrime is now a part of every crime and certain capabilities need to set up in order to effectively investigate cyber-enabled crime and ultimately provide the best level of service to the public.

The paper *"The role of local law enforcement agencies in preventing and investigating cybercrimes 2014"* discusses what law enforcement agencies are doing globally to help combat cybercrime. It's mainly includes American agencies (FBI, U.S Senate and lots of various state police forces/sheriff's offices) however it also includes responses from the UK (Greater Manchester Police). Key points from this academic paper by the Police Executive Research Forum cover topics such as:

- Failures to Report Cybercrimes to Police
- Making Cybercrime a Priority
- Scale of the Crimes
- Jurisdictional Issues
- Task Forces
- Cooperation with Internet Service Providers and Private Corporations
- Partnerships with Universities
- Personnel Development
- Identifying Talented Personnel
- Cybercrime Training
- Police Executive Fellowship Program
- Police Department Network Security
- Community Education

The main points highlighted by the paper that are relevant to this project are the capabilities that forces are setting up in order to enable them to investigate cyber-enabled crime more effectively. Below are some examples from different forces in the USA, describing capabilities and solutions they implemented in order to better investigate and deal with cybercrime.

Regional Computer Forensics Labs are labs created by the FBI in which there are 16 USA-wide. Each RCFL is staffed by 12 examiners and three support staff. The labs are available to any officers which require assistance with digital evidence. Due to the distance to the nearest RCFL, Kansas City police force decided to open their own forensics lab in order to improve turnaround times in which digital evidence can be examined. Half of the forensic labs services were to assist other agencies which created further waiting times for the force. Therefore the decision to create additional tasking hub which would handle low level downloads of devices such as phones, laptops and other common electronic devices was made. This allowed the faster extraction of digital evidence and if the device required more expertise it would be put into a queue and sent over to the forensics lab (Research Forum, 2014 p.27, 28).

The Police Director of the Newark Police hails social media investigators as an investment that will "pay off". A lieutenant in the Intelligence unit monitors social media and provides them with insight into where the next crime will occur which gives them a better chance at preventing it. He would like to see an expansion of this program in order for them to fully utilise what social media can provide to an investigation. (Research Forum, 2014 p.47).

Lastly Toronto Deputy Chief Peter Sloly recognizes that local police agencies need to *"get in the game"*. The police response to cyber-enabled crime is very important as it can create an issue of community distrust which could lead to cyber-vigilantes investigating matters themselves thus shining a light on the inability of the police. *"Cybercrime is now part of every crime and we in law enforcement have to be in this game"* (Research Forum, 2014 p.16, 17, 18).

2.1.2 How India is tackling Cyber-Crime

New Delhi started addressing the growing rise of cybercrime by revamping their dedicated Cyber Cell by procuring state-of-the-art technology.

This upgrade to the cyber cell came after officers announced they felt "helpless" when they faced investigations requiring high level cyber investigatory skills. They were forced to require on private investigators and external forensic lab as they were lacking the required computer expertise.

The Cyber Cell will be equipped with dedicated data acquisition and access services along with forensic workstations (advanced workstations). The Cyber Cell will also be setting up digital intelligence servers which will help them connect all the systems of the cyber lab on to a single network and centralize the system for easier access (Shekhar, 2016).

2.1.3 How the UK is tackling Cyber-Crime

In order to combat the Cyber Crime, the UK set up the National Cyber Crime Unit (NCCU). The NCCU supports partners with specialist capabilities and coordinates the national response to the most serious of Cyber Crime threats.

The National Crime Agency website (http://www.nationalcrimeagency.gov.uk) defines the NCCU's capabilities as:

- *"Providing a powerful and highly visible investigative response to the most serious incidents of cybercrime: pursuing cyber criminals at a national and international level.*
- *Working proactively to target criminal vulnerabilities and prevent criminal opportunities.*
- *Assisting the NCA and wider law enforcement to pursue those who utilise the internet or ICT for criminal means. This includes offering technical, strategic and intelligence support to local and regional law enforcement, as well as supporting the training of the Cyber Crime Units within each ROCU*
- *Driving a step-change in the UK's overall capability to tackle cybercrime, supporting partners in industry and law enforcement to better protect themselves against cybercrime."* (National Crime Agency, n.d.)

The UK is also combatting Cybercrime via frontline policing. Numerous forces around the country in UK are now setting up cybercrime units in order to combat the rise of cyber enabled crime and

provide investigators with specialist knowledge in the preservation of digital evidence. Digital Media Investigators are the latest addition to UK policing, they have been created in order to advise on the development of an effective technology and data strategy for any investigation and policing operation (Justice Inspectorates HMIC, 2015).

2.1.4 Frontline Policing and Cyber-Crime

As nearly all crime now involves a digital element, it's important that front line police officers are trained to recognise and deal with any cybercrime that they may encounter (Her Majesty's Inspectorate of Constabulary, 2014).

Chapter 7 of the real lives, real crime document produced by the HMIC discusses how Digital Media Investigators assist police forces. Digital Media Investigators were introduced in order to assist frontline staff with dealing with digital evidence (Justice Inspectorates HMIC, 2015).

There are a number of different models that forces have implemented in regards to the deployment of Digital Media Investigators. These are:

- A centrally based, stand-alone unit of digital media investigators, with an additional out of hours capability;
- Digital media investigators embedded within basic command units;
- Virtual teams of digital media investigators, comprising officers who have been appropriately trained, and who are available to provide advice and guidance as required, but who are deployed in other full-time posts.

The College of Policing announced in its May 2014 edition of the College newsletter that they want to end the specialism around investigating cybercrime in the police and make it a core part of every investigators work. Around 6,000 detectives are to be trained throughout 2014/15 and have also developed a series of e-learning and classroom based courses to mainstream cyber skills across the service. The online courses available to police officers include:

- Digital Communications, Cybercrime, Social Media and Policing (Released April 2013)
- Cyber Crime and Digital Policing - Introduction (Released August 2013)
- Cyber Crime and Digital Policing - First Responder (Released September 2013)
- Cyber Crime and Digital Policing - Investigation (Released October 2013)

New guidance is also being developed regarding cyber enabled and cyber dependent crime and highlights local, regional and national capabilities. The guidance will cover reporting cybercrime which includes the role of action fraud, the initial response to online abuse and harassment as well as other cyber-enabled crimes, the preservation of evidence and digital forensics, specialist capabilities and management of complex investigations which includes international liaison (College of Policing, 2014).

2.2 Methodology

The research plan was designed assuming nothing with the idea to use key themes highlighted from the needs assessment as a foothold. Once the key themes had been extracted from the needs assessment, a survey was formed around these areas. This survey was then administered to the Digital Media Investigators throughout West Yorkshire Police and the responses fuelled the focus groups to follow. Focus groups were then held with the DMIs, using a specific set of questions that were derived from the surveys responses.

The initial methodology was to complete a focus group with all the DMIs in West Yorkshire, however due to time constraints and the lack of availability of DMIs themselves, this was not achievable. The methodology was revisited and the decision (based on the factors above) was taken to include one to one interviews. This was in order to capture further views and opinions from the Digital Media Investigators.

Once the results had been collated and written up they will be verified by the Digital Media Investigators as to whether the findings are an accurate representation. The figure below shows the work flow of the project methodology.

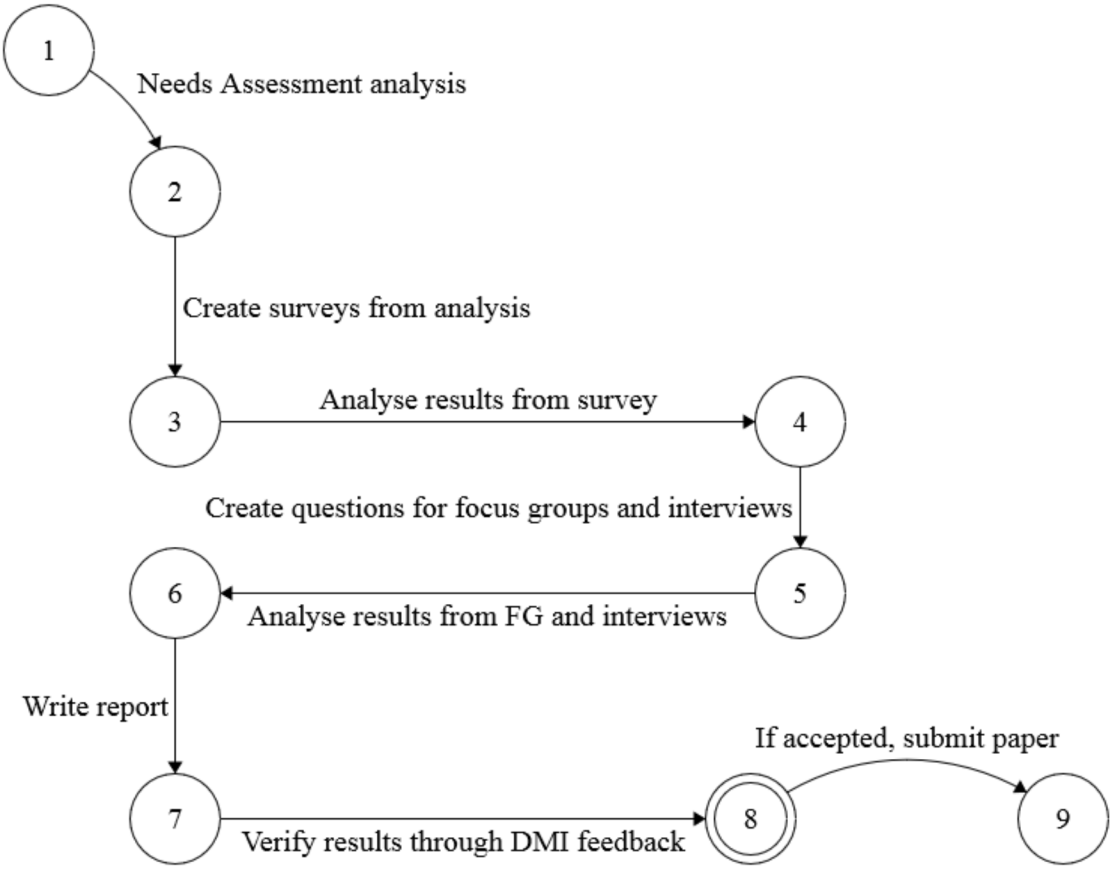

Figure 1 - Displaying work-flow

It was important to design the methodology in this manner due to having to provide an evidence-based evaluation. This was crucial as without the evidence, this study would not in-line with the project goals set out initially. These goals being, to provide an evidence-based response to cyber-crime.

3.0 Development: The Digital Media Investigator survey

3.1 Needs assessment

The initial needs assessment was conducted and held host to 19 focus groups and interviews with a comprehensive range of police officers and staff. The groups of officers and staff that took part in the needs assessment consisted of the:

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

The needs assessment consisted of questions focused around subject areas such as: Role, Inputs, processes, outputs, outcomes, strengths, weaknesses, opportunities and threats. After the process was complete and the data analysis had begun, it became apparent that there were a number of issues raised regarding the Digital Media Investigator role. All of these issues came from other units in the police force, as none of the West Yorkshire Digital Media Investigators took part.

The first issue highlighted from the needs assessment was that the Digital Media Investigator role was part-time, meaning that the officer still had their full duties to complete as well as additional digital media investigator duties. This was seen as potentially problematic as officers already have high workloads without the additional duties.

Secondly, due to the part-time status of the digital media investigator, it made it difficult in order to implement any effective training relevant specifically to their role. This was interpreted as each Digital Media Investigator as having different skill sets and due to their role being part-time, meant it made it difficult to up skill all of the DMI's to the same skill level.

Training was a point that was brought up on numerous occasions that discussed that the Digital Media Investigator training was "obsolete" and "out of date".

Lastly it was noted that overall more Digital Media Investigators were needed throughout the force. There are already thirty two Digital Media Investigators within West Yorkshire and six of those are housed within the Cyber Crime Unit. This leaves twenty six Digital Media Investigators out at police districts and within Protective Services Crime.

The points mentioned above are all from different units from within the West Yorkshire Police and were raised during the needs assessment process. This feedback will provide this project with the base it needs, in order to formulate key high impact surveys that will help us further identify other subject areas of significance.

3.2 Identification of further subject areas

Further research identified areas which can help strengthen the overall evaluation of the Digital Media Investigator. The areas identified are as follows:

- 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.

These were seen as extensions of some the issues identified during the needs assessment. For example, training was brought up a lot during the needs assessment therefore it was imperative that training formed a main part of the evaluation.

The remaining subject areas were chosen because they are stand-out variables that affect the effectiveness of the role of a Digital Media Investigator. By evaluating these additional areas we can create a survey that not only covers the basics surrounding the role, but the concerns about the role from other units within the West Yorkshire Police Force.

3.3 The Digital Media Investigator survey

When creating surveys, it is important to make sure the data that is obtained, is useful. In this case, we were aiming to identify further subject areas of interest surrounding the DMI role therefore, it was critical that the questions reflected this aim.

The subject areas seen above in the body of this report formed the categories that the survey questions were to be structured around. Keeping these in mind, a survey was created using a mixture of qualitative and quantitative survey questions. The survey can be seen below in figure 2.

The Digital Media Investigator Survey

Are you Police Officer or Police Staff?

1. What background experience, did you have that made you feel that you were suited to the role of a DMI (this may be from previous roles, jobs, hobbies etc.)? (*Freetext)*
2. In your opinion, what is the most important technical skill that a DMI can have to enable them to work to the highest standard? (*Freetext)*
3. (Police Officers only) Do DMI duties interfere with your existing officer duties? *(Scale: Yes/No)*
    a. If yes, in what way? (*Freetext)*
4. (Police officers only) What proportion of your time do you spend on DMI duties? *(Scale: 100% DMI, 80% DMI/20% other, 60% DMI/40% other, 50%/50%, 40% DMI/60% Other, 20% DMI/80% other, 100% other)*
5. (Police Officers only) From your experience do you feel the DMI role should be full time? *Scale: yes/no.*
    a. Why do you say that? (*Freetext)*
6. Have you received any training that enables you to carry out the role of DMI
    a. If yes, what was the training? (*Freetext)*
    b. If yes, how would you rate the DMI training you have received in terms of :
        i. The relevance of the topics covered

ii. The level of technical detail
iii. The time allocated for training
iv. The regularity of courses

(Scale: Very poor, Poor, Fair, Good, Excellent). If you have given any ratings of poor or very poor… please provide further details so that we can understand what needs to be done to improve DMI training in the future (please include the name of the course you are commenting on). (*Freetext)*

7. What aspect of the role do you feel the least confident with?
8. What technical support, if any, did you receive following the initial DMI training course (e.g. from other specialist HQ departments)?
9. What resources do you use for support as a DMI? (e.g. where do you go for help)

10. How often is there an exchange of information between DMIs from different districts? (*Scale: At least once per week, approximately once per month, approximately once per quarter, approximately once per year, there is no information exchange)*

11. What technical equipment do you have available to you in your role as a DMI? Eg. Non-attributed machine, Ethernet cable, USB drives, digital camera.
12. Is all the equipment you need for your role as a DMI readily available to you (*Scale: Yes/No)* and if no what is not available. (*Freetext)*
13. Have you got any additional comments or suggestions about the equipment available to you, for example quality, reliability, access etc.)
14. Please see above for the College of Policing Digital Media Investigator Role profile. Do your duties as a DMI accurately reflect this role profile? (*Scale: YES/NO)*

Figure 2

3.4 Dissemination

The survey was distributed to 34 individuals and amongst them included Digital Media Investigators, the Digital Media Investigator trainers and the Digital Media Coordinator in the West Yorkshire Police Force on the 19/09/2016.

The survey was setup to remind the invited participants to complete the survey if they had not already done so, seven days after they had received it (26/09/2016). The deadline to complete the survey was two weeks, this was set in order to keep the project in line with our timescales defined in the project delivery plan.

The survey was compromised of 15 questions inviting both qualitative and quantitative responses from the participants. There were 9 quantitative questions that involved participants selecting a predefined answer and 5 free text qualitative questions where the participant could in their own words answer the question. Several of the predefined quantitative questions contained an additional part where a participant could provide additional free-text detail to explain fully why an answer was selected.

3.5 Results

From the thirty four survey invitees, we received twenty one responses in total. This was calculated as a 61.8% response rate. Eighteen respondents identified themselves as police officers whereas three identified themselves as police staff. It was important that in regards to the Digital Media Investigator

role that we captured the views of police officers and staff that both perform the role, in order to obtain the widest range of feedback possible. The results are as follows:

- 56% of DMIs report that DMI duties interfere with existing officer duties.
- 67% of DMIs report that their time is spent 20% on DMI and 80% on other.
- 22% of DMIs report that they do not spend any time on DMI duties.
- 61% of DMIs think that the role should be full time.
- 39% feel the role should not be full time.
- 100% of DMIs have received some training that enables them to perform the role. The main courses seen are:
    - *DMI training course.*
    - *Mainstream cyber-crime course.*
    - *1/3 day Wi-Fi course.*
- 57% report there is no information share between different district DMIs.
- 62% of DMIs report that all the equipment they need to perform the role is not readily available to them.
- 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.*
- Keeping up to date with skill levels and the latest technology was raised as the most important technical skill a DMI can possess. An active interest/passion in technology was the next highest weighted.
- DMI duties interfere by adding to the existing workload of the officer and mean they could be abstracted at any time.
- DMIs that answered "yes" to whether or not if the role should be full-time feel this is because:
    - *Would be better equipped/experienced if full time (Up to date with legislation, best practices, learn, not "rusty", understanding initially that they would be full-time, best information – accurate).*
    - *Role not yet used to full potential (missed opportunities, no awareness).*

- DMIs that answered “no” feel this is because:

  - *DMIs would work Monday to Friday and they should be available 24/7.*
  - *Not enough work to become a full-time role/remit needs to change to become full-time (need more workload, need more training in all areas rather than trying to self-learn to upskill/work long hours.) The role is in “infancy” as officers/departments don’t necessarily understand what a DMI can do for their investigation.*

- DMIs felt the least confident with the following:

  - *Producing strategy logs/policy logs.*
  - *Searching other social media websites/applications and obtaining information from social media.*
  - *Being utilised in a high priority situation without enough shadowing/live experience. (Eg high risk misper/murder).*

- The units most utilised by DMIs following the DMI course are:

  - *Telecoms unit*
  - *Cybercrime unit*
  - *Digital Forensic unit*
  - *CAB*

- DMIs have reported that they use the following resources for support regularly:

  - *Cyber Team.*
  - *Other DMI's.*
  - *Telecoms.*
  - *Internet.*
  - *Digital Forensic Unit.*
  - *POLKA DMI Community.*

- 11/21 DMIs reported that they have no equipment available for them to use. Other responses included (in order of most weighted):

  - *USB*
  - *Camera equipment*
  - *Non-attributable machine*
  - *Smart phone*
  - *Laptop*
  - *Ethernet cable*
  - *WiFi printer*
  - *Tablet*
  - *Stand-alone computer*
  - *Force networked PC's*
  - *MIFI*
  - *Covert Wi-Fi*
  - *HDD*
  - *Cables*
  - *Non-attributed phone*

- The majority of DMIs reported that they had no equipment available to use for enquiries. Other high weighted answers regarding equipment that was not available included:
  - *Camera*
  - *Non-attributed machine*
  - *Ethernet cable*
  - *USB*
  - *Laptop*
  - *Wi-Fi*
  - *Stand-alone machine*
  - *Laptop*
  - *Website/screen recording software*

- The DMIs were asked to provide additional comments or suggestions about the equipment that is available to use. The highest weighted answer that they reported was the fact that there were no laptops/limited equipment to DMIs out at district. Other responses included Better access to systems (CDA, ANPR). Slow UN-attributable connection lines.

Table showing Digital Media Investigator Training taken directly from the survey.

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%

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).*

3.6 Observations

The Digital Media Investigator survey overall, was a success. Once the analysis was complete and the results were obtained, initial observations were made. Firstly the response rate of the Digital Media Investigators which totalled at 61.8%. The expectation was that it would have been higher due how much this project would be in the Digital Media Investigators interests, however as the project developed it came to the realisation that the DMI's have very limited availability, so the response rate may be a result of a too small time frame window to complete the survey. The method of survey delivery could have also impacted upon this, however distribution via email (under current time constraints) was felt as the best method to deliver the survey.

At first glance the results highlight a number of potential issues that would need to be investigated further.

The first observation was regarding the Digital Media Investigator training. As seen above in the Digital Media Investigator survey, participants who had given poor/very poor as a response were then asked to fill out a free text box explaining in more detail as to why they had responded that way. Some of the top recurring themes seen here were: the technical detail in the course was poor and didn't cover key areas, the course only taught how to correctly fill in RIPA forms and that the course was pitched at the wrong level. Additional comments, although not directly related to the question asking to rate the various aspects of the training, included, that there was no follow up training to the DMI course, therefore DMIs felt they were losing skills/ becoming de-skilled.

The next observation seen during the analysis of the data was that 62% of the Digital Media Investigators that partook in the survey reported that all the equipment needed to perform the role is not readily available. As 62% is a majority weighting, the decision to explore the situation surrounding equipment available to DMIs was taken. Other evidence supporting the decision to use equipment as a further subject area were seen through questions which discussed the equipment was currently available and which was not.

61% of respondents think that the role of the Digital Media Investigator should be full time. This area was highlighted due to the part time status of the role currently. Due to these findings, it became clear that it needed to be explored further in order to find out first-hand from an operational level, about whether the DMI role would work better if made into a full time role.

As the Digital Media investigator role is only part-time, it means police officers are having to often balance the demands from the usual role (criminal investigations/specialist unit) alongside being tasked with additional DMI duties. The survey concluded that 56% of respondents feel that DMI duties interfere with existing officer duties and that for the majority of respondents, their time is split up 20% and 80% across DMI and officer duties respectively. This was chosen for further investigation in order further to explore how Digital Media Investigators are managing two very demanding workloads.

Several questions from within the survey explored which resources and units Digital Media Investigators made use of the most and received support from, while performing their role. Various different units and resources were listed. Observing this, it became clear that we could explore what units the DMIs themselves thought would be the most beneficial to them and their development.

When the survey was created, the researchers wanted to gauge how much information sharing took place between Digital Media Investigators from different police districts. The idea was to try and see if there were any existing information shares and whether or not the DMIs would find this beneficial. While the survey data was being analysed it was discovered that 57.1% of respondents reported that

there was no share of information whatsoever between different districts. Due to this the decision was taken to further explore this area in order to try and establish how information is shared between DMIs.

The last question of the survey asked if the role profile of the Digital Media Investigator is an accurate reflection of the role of the DMI. The respondents answered 50/50 with the same number of responses for/against. This was chosen as an area to review further due to the split decision.

Once the survey data had been extracted and analysed it became apparent that these were the main key areas that needed exploring further in more depth. These subjects will form the base in order to create a set of questions that would then be used to within a series of focus groups.

4.0 Development: Digital Media Investigator focus groups & interviews

The next stage of the evaluation involved using the results from the Digital Media Investigator survey in order to structure a series of focus groups and interviews. These will help to explore the areas that were identified in the survey, in much more depth.

4.1 Design

During this stage of the project several focus groups and interviews took place with Digital Media Investigators from various sectors of West Yorkshire Police. Twenty-one participants took part in filling out the Digital Media Investigator Survey, therefore it was aimed to get least half of this populous to take part in the focus groups and interviews.

The sample size in total was 10 participants which were questioned over five one to one interviews and 2 focus groups. This was decided due to time constraints and the nature of a DMIs work and how un-predictable it can be. Participants fell into the following categories: district officers, specialist units and the Digital Media Co-ordinator (at the time of study).

In section 3.6, observations are made about subject areas of interest that could be investigated further during this stage of the project. All seven subject areas of note were chosen to be explored throughout the focus groups and one to one interviews. These subject areas are: training, equipment, full-time (for and against), technical support from other units, information sharing, the work load of a DMI, role differences between the role profile and actual role performed.

While conducting the focus groups and interviews, the only variable that was controlled, were the questions that were asked throughout. The data that was obtained was taken through note-taking. This felt the most appropriate due to the sensitive nature of some the questions and topics. Recording the responses may have been seen as intimidating and could have skewed the data.

4.2 Focus group and interview plan

The focus group and interview plan was designed using the subject areas discussed above. See below for the breakdown of the focus group and interview plan.

(Subject areas are underlined)

Training (all)

- *If you were to design the Digital Media Investigator training course, what would you include? (Suggestions already made are WiFi, OSR, and Routers. The course currently includes RF, telecoms data, RIPA forms, digital forensic unit submission forms and financial checks form).*

Equipment (all)

Highlighted in the survey 62% of respondents answered no in relation to if the equipment needed to perform the DMI was readily available.

- *What are some of the problems you face when it comes to sourcing and using equipment to perform the DMI role? How did/do you overcome them?*
- *From the training you have received and your practical experiences, what equipment do you think you require?*

Full Time - for and against (All)

"Would be better equipped/experienced if full time (Up to date with legislation, best practices, learn, not "rusty", understanding initially that they would be full-time, best information – accurate)".

- *Do you agree with full time? If so, how could it work? (thoughts)*
- *How are DMIs currently tasked/allocated crimes? (Is there a process within your district (tasking form) or other methods?*

Role Differences (Employees that perform as both a DMI and another duty only)

An advice SPOC/Social Media Downloader was mentioned numerous times throughout the previous study as to how DMIS felt they differed from the official role profile.

- *How do you view the role of the DMI and where it could lead to?*

Technical Support from other units (all)

The units listed below have been obtained directly from the survey. These are listed as the most common places DMIS seek help from. (List of units)

- *Are there any other units where you have received support that are not present on this list?*
- *Is there anything specific you would like from any of those departments?*

Information Sharing (Employees that perform as both a DMI and another duty only)

57% report that there is no information share between different district DMIs.

- *Do you think that collaborating with other DMIs to share information would be beneficial?*
- *How/why?*

Work-load (Employees that perform as both a DMI and another duty only)

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

- *How do you manage your workload alongside performing DMI duties?*

(Allow for additional comments at the end of the focus group/interview)

Each focus group and interview followed this structure except when certain questions did not apply to that DMI. This could be because they are a civilian instead of an officer or they are do not routinely carry out and receive DMI duties, for example the Digital Media Co-ordinator.

When the interview with the Digital Media Co-ordinator took place, the following changes were made to the structure of the focus group/interview plan:

Equipment

- *What equipment do you think they should have?*

Work-load

- *How do you think a workload could be managed alongside DMI duties?*

These changes were made due to the fact that the Digital Media Co-ordinator is a non-operational Digital Media Investigator and the questions would not apply to them.

4.3 Analysis

The data was analysed via a thematic analysis. This involved looking at each of the subject areas for each of the focus groups and interviews, then looking for the common themes seen within the data. These results will be used in order to highlight any potential areas for significant improvement or more effective utilisation of the DMI.

The analysis was performed using spreadsheet/calculus software which allowed the separation of the different topics of discussion. This allowed the cross-analysis of different results that were under the same topic name. Common themes were then extracted.

4.4 Observations

For each of the subject areas identified above in section 4.2, a thematic analysis was undertaken. These were subsequently broken down by the subject areas that were being investigated. Throughout the focus groups and one to one interviews there were often cross-category discussions. For example while on the subject of training, often thoughts surrounding the role of the DMI would appear. For the purpose of clarity, cross category discussions are being allocated to the relevant subject areas.

4.4.1 Digital Media Investigator Training

Through the thematic analysis of this subject area, various findings were observed. Firstly, the analysis suggested that the in order to attend the Digital Media Investigator training course (nationally run by the College of Policing), that a more stringent selection process is put into place. The analysis implied that certain Digital Media Investigators felt that in some cases, baseline knowledge was not fully established by attendees, subsequently having a negative impact on the course and others present. The Mainstream Cyber Crime Training course was also mentioned on several occasions as an “obvious” prerequisite. This may be largely down to the fact that some attendees were “pushed into” becoming a DMI without any pre-knowledge in that area or have no general interest in technology itself.

In addition to improving the selection process for Digital Media Investigator, it was highlighted by the DMIs that an interest in technology is key in order to succeed in role. This was due to the rapid pace in which technology is changing and in order to maximise the success of the DMI, the DMI must be up-to-date.

Secondly the Digital Media Investigators felt that the course content could be improved, as the course only covered an overview of what was expected of a Digital Media Investigator which appeared to be basic and bland in comparison to performing the role. Digital Media Investigators felt that the course was focused more on strategy building due to the scenario-based theme. It was also noted that the course heavily focused on areas deemed "unnecessary". This was particularly aimed at the amount of different form filling exercises there are throughout the training course as Digital Media Investigators felt they already had sufficient knowledge in these areas.

Through conducting the various focus groups and interviews, feedback regarding the level of technical detail on the DMI training course was poor. Digital Media Investigators felt that the course may have included current technology trends, how to secure digital evidence, router downloads and open source research whereas instead it was telecommunications heavy. Other feedback simply summarised the course as "shockingly bad" and that based on the content, the course was "pointless". Upon completion of the DMI training course, Digital Media Investigators felt that they had not gained anything new and that "nothing was delivered and everything was promised".

The Digital Media Investigators highlighted that currently there is no mandatory portfolio to complete in order to remain a Digital Media Investigator. Some suggested that introducing a portfolio would ensure a standardisation of DMI skills throughout the force. Additionally, it would allow the introduction of a mandatory continuous personal development (CPD) program for all DMIs. The program could tie in into the portfolio and unsuccessful completion of the CPD would mean the accreditation of the DMI is revoked.

4.4.2 Digital Media Investigator Equipment

Highlighted in the survey 62% of respondents answered no in relation to, if the equipment needed to perform the DMI was readily available. Upon analysis of this subject area, there were obvious findings.

Firstly, Digital Media Investigators highlighted that equipment, in order to perform to the full extent of the role, was lacking and Digital Media Investigators have a hard time sourcing equipment. Digital Media Investigators reported that no kit was available to them and to them and in order to complete duties they have to use old, slow, force machines. Feedback received around sourcing equipment was generally negative, including responses like "no set equipment", "no equipment generally" and "equipment is non-existent".

Another issue raised through this discussion was that there isn't much funding that goes into supplying Digital Media Investigators with the tools they require for the role, one quote stated "divisions/units would rather spend money elsewhere". Some DMIs reported, that in order to get around the lack of equipment, that they would spend their personal money on equipment, so that they can perform the role duties. It was also noted that if DMIs had the full support of their supervision, then acquiring equipment may not be as much of an issue. This was apparent when discussing equipment with Digital Media Investigators from different districts/units and hearing that a handful have the equipment available and some do not.

In the focus groups and interviews, Digital Media Investigators were asked what equipment they require for the role. The findings that were observed are as follows: Mozilla Firefox (Internet Browser software), standalone laptop, kit bags, USB devices, external hard drives, non-attributable Wi-Fi connection, equipment to perform router downloads (Ethernet cable, standalone laptop).

4.4.3 Information Sharing between Digital Media Investigators

57% of survey participants reported that there is no information share between different district DMIs. Due to this Digital Media Investigators were then asked if they thought collaborating between different districts would be beneficial to them. The findings observed were generally positive, with the majority of Digital Media Investigators in favour of some sort of information sharing system.

One of the popular ideas put forward was for the DMIs to have regular meetings and share examples of good DMI work (case studies). This was a very recurrent theme seen through the data gathered. Recent DMI networking events organised within force and by the College of Policing were also well received, the only drawback being, that they weren't more regular.

The Police Online Knowledge Area was reportedly utilised by Digital Media Investigators for when they required assistance. Although this reportedly used, suggestions were made to implement a POLKA-like system for DMIs within West Yorkshire.

In-force refresher days for Digital Media Investigators were also suggested as a way of keeping Digital Media Investigators up to date. This was proposed as a method of reinforcing skills that may not have been immediately utilised after DMI training and as a means of further DMI networking opportunities.

4.4.4 Support for Digital Media Investigators

Digital Media Investigators were next asked to review a list of departments/units within West Yorkshire Police who have provided support to DMIs throughout their time in role. The departments are as follows:

- *Cyber Crime Team.*
- *Telecoms*
- *Digital Forensic Unit.*
- *POLKA DMI Community.*
- *Economic Crime Unit.*
- *CAB Unit.*
- *Technical Support Unit.*

When discussing what certain units could do to support DMIs further, numerous issues/suggestions were brought forward.

Firstly, DMIs felt that certain units are trying to "empire build" where they are protecting skills and not allowing other units/DMIs certain capabilities. DMIs felt that this was having a negative impact and creating an atmosphere where people do not want to deal with those units. DMIs also reported that units could be more friendly, supportive and open to deal with others. Another concern raised through the analysis was that Digital Media Investigators are sometimes put off going through certain departments due to the wait time and back log.

Several suggestions and improvements came out through this discussion, praising all of the different units and departments mentioned above. One unit in particular was mentioned through the survey and the focus groups/Interviews was the cyber-crime unit. Quoting an excerpt from the analysis "The Cyber Crime Team are the go to people". They also suggested that the cyber-crime unit could have a more proactive role in helping to develop new skills by providing inputs and other various training.

In addition to the cybercrime unit having a hand in performing additional inputs, the Digital Media Investigators also stated that this would be beneficial if other units were to do the same. Spending time with each of the departments was also noted as something that would be beneficial to a DMI, allowing them to see how the unit operates and get some face-to-face time with the staff operating there.

Occasionally DMIs will borrow equipment from other units/departments within force in order to perform the duties of the role. This was taken as a positive due to the collaboration between units/departments. However, this shows some of the issues that were brought up in the discussion around Digital Media Investigators equipment, regarding them having little or no access to any.

4.4.5 The Role Profile for the Digital Media Investigator

The next question discussed the College of Policing's official role profile, for what is expected of a Digital Media Investigator. Please see appendix for the College of Policing's role profile of a Digital Media Investigator.

Through analysis of the survey, Digital Media Investigators felt they were more of an advice SPoC/Social Media downloader instead of how the role profile perceives them. Due to this, the differences between the actual role and the role profile of the Digital Media Investigator was investigated.

Firstly, Digital Media Investigators felt that the role profile was too extensive for an officer to perform, especially while expected to retain normal officer duties. One DMI quoted "We can't be a jack of all trades" while referring to the extensive DMI role profile. If Digital Media Investigators were expected to meet the entirety of the role profile, that they would need protected time in which they could do courses, stay up-to-date and increase their learning. There were also suggestions around making the skills listed on the role profile as prerequisites of the role.

Secondly, most of the Digital Media Investigators interpreted the role as an advisory and not a practical role. Meaning that they are offering their expertise and advice but not directly dealing with digital enquiries. This was also mentioned when speaking to DMIs about their workload and how it impacts on their Digital Media Investigator duties.

Finally, some Digital Media Investigators hadn't been utilised at all, therefore could not accurately respond to this question.

4.4.6 Digital Media Investigator; Full time or part time

Digital Media Investigators were next asked if the role of the DMI should be full-time or remain a part-time role. When discussing whether or not the role should be full time or be kept as a part time, we received arguments, for and against.

Most Digital Media Investigators were in favour of the role being full-time, this supported what was seen through analysis of the survey, which was that 61% of DMIs think the role should be full time. Supporting anecdotes from DMIs included: *"100% Full time role" "Should be full time, other regions are" "If given necessary support and equipment, full time role could be beneficial".*

Digital Media Investigators felt that if the role was full time, they would be able to perform the DMI duties a lot more regular, allowing them to gain confidence in their skills and develop them further. They would also be able to take a more practical role instead of being an advisory SPoC for technical enquiries.

If a full time role was implemented, DMIs put forward suggestions of how it could be implemented and executed. A core team of full time Digital Media Investigators, that become a force asset. This would allow a formal DMI tasking process which could be centrally managed by a line manager and would mean that DMIs could be deployed as a co-ordinated response.

One other immediate benefit of making the role of a DMI full time, would be the alleviation of an additional workload. Many of the DMIs when discussing the current state of the DMI role, felt that DMI duties were suffering due to the level of work they were dealing with (officer duties). An anecdote from one DMI stated *"DMI enquiries are often impossible to do with other jobs"*, another stated *"It's hard enough to keep up-to-date with my current role, let alone another"*. One Digital Media Investigator said, while discussing how the role was currently implemented (part-time), that, *"I do not understand why they did it like this"*. Another suggestion was that a core team of Digital Media Investigators could help remove pressure from small technical departments such as the Cyber-crime Unit and the Digital Forensics Unit by taking on lower-level enquiries from those departments.

Additionally, if a Digital Media Investigator was expected to meet the entirety of the role profile, it would be advantageous to be in a full time DMI role, to allow sufficient CPD and learning time, to meet the requirements.

Generally the feedback around making the role full-time was positive for the reasons mentioned in the above section. One anecdote stated that *"A full-time DMI role would be a fantastic job"*.

On the other hand, not all Digital Media Investigators agreed that the role should be full-time and some opposed the idea. They argued that, if the DMI role were to become full time, then they would have to find their own work, because there weren't enough requests/tasking's for DMI duties.

Another counter-argument was that some police officers enjoy their role as a police officer and wouldn't want to give up the variety of work, as the role is part-time currently, it allows them to perform two roles simultaneously.

Finally, some of the Digital Media Investigators reported that they wouldn't want to give up active policing for more computer-based work. Referring to the fact that a lot of Digital Media Investigator Enquiries will be computer based.

4.4.7 Digital Media Investigator Work-Load

The Digital Media Investigator Survey highlighted that the majority of DMIs (56%), report that DMI duties interfere with existing officer duties. Speaking to Digital Media Investigators around this subject brought up a number of issues.

Digital Media Investigators reported that because they have to manage an officer workload alongside a DMI workload that they face numerous problems. They reported that DMI enquiries are suffering and are often impossible due to managing an officer workload alongside. Another issue raised was the fact that some DMIs, are having to come into work early in order to stay on top of their officer workload creating a poor work-life balance.

The impact of being both an officer and a DMI is particularly felt on small run teams/small departments. This is due to staff being abstracted in order to perform DMI duties. It was also reported that supervision aren't always supportive when DMIs are taken away from operational/live policing. The quote *"Being a DMI is great if you are needed within your department, however not pleased when you need to assist other units/departments"*. DMIs have even said that occasionally, being a DMI is quite inconvenient when performing routine officer duties.

Having an officer workload while being a DMI often meant that DMIs were looking to advise on digital enquiries where possible in order to save time, ensuring their own workload does not suffer. This affects both the service and skills of the DMI. This could be because the DMIs who are afforded time to complete the duties of the role may develop and ultimately give a better service than a DMI who may only get to perform the duties ad-hoc, depending on their workload at the given time. Due to this, it could potentially lead to various DMIs who are more skilled than others and offering an un-standardised service.

5.0 Conclusions

In conclusion, the Digital Media Investigator role is still going through a development phase. To summarise the following, were the main findings observed.

Based upon responses from Digital Media Investigators it does not appear that they do not have the time to perform as an officer and be an effective Digital Media Investigator. It has been found that in order to perform to the full extent of either role, another must suffer. This could be that DMIs are never being utilised due to the demands of their main role or that they are being used effectively as a DMI, but having to work later/longer in order to stay on top of their main role. The role of the Digital Media Investigator is extensive and commands a lot of knowledge around the area of Digital Investigations, this also has an impact on officers/staff who are trying to perform both roles simultaneously. Due to the demands from the required knowledge and the ever-changing pace of technology, Digital Media Investigators are under a lot of pressure to ensure this is kept up-to-date. This is not always practically possible especially if protected time for learning is not always available.

It has also been observed that there wasn't a proactive 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. It was also found that the majority of active Digital Media Investigators do not have sufficient equipment available to them in order to perform their role effectively, resulting in hours wasted trying to find workarounds or a loss in the level of service they are able to provide as a DMI. When reviewing the role profile it was found that the demand of it was extensive and that 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 as some DMI's have had more training and are performing complex duties in comparison to a Digital Media Investigator that is barely or never utilised.

It was found that there could be more education around the role of the DMI and what value it can bring to an investigation. It was observed that 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.

Through this research it was discovered that there is no formal, structured, continuous professional development plan put in place for Digital Media Investigators that is compulsory. It was raised that there are have been local networking events for Digital Media Investigators within West Yorkshire and that the College of Policing offer 'DMI' days that aim to refresh knowledge. However there is no formal training plan which outlines set DMI duties and what training they need in order to meet those requirements. This would help ensure a standardisation across DMIs in West Yorkshire and allow the completion of portfolio. This would also help protect the integrity of the work performed by the Digital Media Investigators as it would help ensure DMI duty competencies.

As there is currently no formal, structured, continuous development plan in place for Digital Media Investigators, a point was raised which discussed the fact within the next five years Digital Media Investigators may become out-dated. This would be due to next generation police officers who have grown up amidst technology and what is current specialist technical knowledge may have become mainstream knowledge. This is a concern which needs to be addressed as it would mean the specialism of Digital Media Investigators would be lost. Implementing a structured development plan for Digital Media Investigators, will circumvent this and allow the role to remain a specialist technical role.

There has been a mixture of responses surrounding the topic of fulltime vs part-time in regards to the role of the Digital Media Investigator. Arguments have been put forward for both a full time role and a part time role. However, the Digital Media Investigator survey concluded in favour for the position to be full-time. As there was a mixed response seen throughout the focus groups/interviews, this was deemed more reliable as it covered a larger sample of DMIs. Therefore this report can conclude that the majority of Digital Media Investigators feel that the role should be a standalone, full-time role.

Lastly, through this research, it was identified that an important factor in the effectiveness of a Digital Media Investigator was a passion and interest for technology. Mentioned throughout the Digital Media Investigator survey and the focus groups/interviews. This skill was seen to recur in almost each and every session while featuring heavy throughout the survey beforehand.

6.0 Recommendations

This section aims to outline some recommendations, based on the findings from this research.

6.1 Digital Media Investigator Training

- 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. This would subsequently ensure only those who are committed to the success of the DMI role get selected.
- Introduce a two-tier DMI course (basic and advanced). To cater for Digital Media Investigators who may already possess a lot of the core knowledge.
- Once the role is fully defined (the core duties of a DMI has been decided upon) tailoring a training course to meet those needs could be put together.
- Education produced around what a Digital Media Investigator can offer an investigation and the value of investing in a DMI.
- More examples and case studies included on future training courses to give Digital Media Investigators real world examples.
- Create and run more Digital Media Investigator refreshment days within West Yorkshire. This could potentially be run in conjunction with training school, providing refresher training

in the various skills a DMI should be performing. Prior to these, surveys/questionnaires could be completed in order to see what skills may need a refresher.

- More experienced Digital Media Investigators could act as trainers for less-experienced DMIs. This could be some sort of shadowing, whereby the less-experienced DMI would accompany a more experienced DMI to get first-hand experience in the role. A competency check could also be introduced and administered through this method.
- Introduce a mandatory portfolio that must be completed and maintained in order to keep the Digital Media Investigator certification. This would give the role more integrity as completing and maintaining a portfolio requires core competency in all areas of Digital Investigations.

6.2 Digital Media Investigator Equipment

In order to implement the recommendations around what equipment Digital Media Investigators need to have at their disposal, firstly the core duties of a Digital Media Investigator must be defined.

Once the above has been satisfied, the recommendations to be implemented are as follows:

- Standard equipment checklist can be introduced in line with the duties that will be performed. For example, if a core duty of a Digital Media Investigator would be to examine routers then equipment that allow a DMI to do so must be provided.
- Standard software checklist can be introduced in line with the duties that will be performed. For example, if a core duty of a Digital Media Investigator would be to examine large amounts of call data records, then software allowing DMIs to do so can be implemented.
- Implement policies in order to ensure the equipment and software is being correctly used and the data is being correctly managed and stored in line with force policy.
- Work with Information Security and other technical units (Cyber, Digital forensics) in order to ensure that certain pieces of equipment (USB, External Hard drives) are used with force systems safely and appropriately.
- Work with Information Security and other technical units (Cyber, Digital forensics) to implement procedures for storing data obtained from Digital Media Investigator equipment. For example, a central database for housing router downloads or live memory captures.
- If no more duties are defined and there is no change to the Digital Media Investigators remit then based on their current role they may require the following equipment: Mozilla Firefox (Internet Browser software), standalone laptop, kit bags, USB devices/external hard drives, non-attributable Wi-Fi connection, equipment to perform router downloads (Ethernet cable, standalone laptop).

6.3 Digital Media Investigator; Full time or part time

The next section discusses recommendations for both a full-time and part-time Digital Media Investigator role.

6.3.1 A full-time Digital Media Investigator role

Create a full-time Digital Media Investigator role that can perform specialised functions:

- **Proactive assistance on technical enquiries** – DMIs able to work within the district, providing real-time assistance on cyber-enabled or enquiries involving a digital element.
- **Proactive** assistance where-possible regarding the Regulatory Investigatory Powers Act (RIPA) and helping **ensure officers and staff are compliant** while conducting digital enquiries.
- The ability to **attend scenes** alongside frontline officers to offer assistance with the **preservation and seizure of Digital Evidence**.
- Able to be **abstracted with minimal impact** in order to assist on high-level enquiries looking for potential digital lines of enquiry.
- Allow the implementation of a **structured continuous professional development plan and mandatory portfolio**.
- Enable the Digital Media Investigators to be a **force/district resource** with their own in house Digital Media Investigator operating procedures.
- Enable a **formal Digital Media Investigator tasking process**, giving insight into performance and demand, to senior management.
- More **time and care** spent on digital enquiries due to less pressures from an officer's workload, providing a better public service.
- Allow Digital Media investigators to **learn** from one another and discuss duties/ideas with ease. At the moment Digital Media Investigators are spread out throughout different departments and districts.

6.3.2 A part-time Digital Media Investigator role

If the Digital Media Investigator role is kept part-time, the role must be purely in an advisory capacity that is reactive. This will allow officers the ability to manage their normal workload without additional enquiries. However, the research has shown us that by keeping the role purely advisory that

an officer workload will still suffer. This is due to the nature of an advisory role and not knowing how long advisory abstractions may take.

- The **role will remain reactive**, as the demands of an officer's workload make it difficult to take on additional duties.
- **Protected time for DMIs** in order to remain up-to-date and on top of the required continuous professional development, in order to be an effective Digital Media Investigator.
- **The role should be purely advisory** as the additional Digital Media Investigator duties add to the pressures of an existing officer's workload and is very difficult to manage.

6.4 Digital Media Investigator Role Profile

- Using the role-profile (see appendix) define what duties should be core Digital Media Investigator duties.
- Create a new role-profile based the duties identified and start implementing supporting training/equipment based on it.

6.5 Digital Media Investigator Support

- Technical roles and departments such as Cyber-Crime and Digital Forensics could prepare inputs and training around new techniques and skills for Digital Media Investigators.
- Digital Media Investigators would benefit from visiting other various departments within West Yorkshire Police. This has already been done with the Cyber-Crime unit and the Digital Forensics Unit however, it was reported that it would be very beneficial to mirror this with other departments, letting DMIs see how they work and where they could help one another.

6.6 Information sharing between Digital Media Investigators

- In-force refresher and networking days. This was proposed as a method of reinforcing skills that may not have been immediately utilised after DMI training and as a means of further DMI networking opportunities.
- Creating a system similar to POLKA in which in-force Digital Media Investigators can communicate on and offer advice to one another.

8.0 Bibliography

1. Research Forum, P. E. (2014) The Role of Local Law Enforcement Agencies in Preventing and Investigating Cybercrime 2014.pdf [Online]. pp. 27, 28. Available from: <http://www.policeforum.org/assets/docs/Critical_Issues_Series_2/the%20role%20of%20local%20law%20enforcement%20agencies%20in%20preventing%20and%20investigating%20cybercrime%202014.pdf> [Accessed 9 May 2016].

2. Research Forum, P. E. (2014) The Role of Local Law Enforcement Agencies in Preventing and Investigating Cybercrime 2014.pdf [Online]. p. 47. Available from: <http://www.policeforum.org/assets/docs/Critical_Issues_Series_2/the%20role%20of%20local%20law%20enforcement%20agencies%20in%20preventing%20and%20investigating%20cybercrime%202014.pdf> [Accessed 9 May 2016].

3. Research Forum, P. E. (2014) The Role of Local Law Enforcement Agencies in Preventing and Investigating Cybercrime 2014.pdf [Online]. pp. 16, 17, 18. Available from: <http://www.policeforum.org/assets/docs/Critical_Issues_Series_2/the%20role%20of%20local%20law%20enforcement%20agencies%20in%20preventing%20and%20investigating%20cybercrime%202014.pdf> [Accessed 9 May 2016].

4. Shekhar, R. (2016) Infotrac Newsstand - Document - As Cybercrime Soars, Police Get Ready to Byte Deep. *The Times of India* [Online], 26 January. Available from: <http://go.galegroup.com.ezproxy.leedsbeckett.ac.uk/ps/retrieve.do?sort=RELEVANCE&docType=Article&tabID=T004&prodId=STND&searchId=R2&resultListType=RESULT_LIST&searchType=AdvancedSearchForm&contentSegment=&currentPosition=1&searchResultsType=SingleTab&inPS=true&userGroupName=lmu_web&docId=GALE%7CA441436846&contentSet=GALE%7CA441436846> [Accessed 11 May 2016].

5. National Crime Agency (n.d.) *National Crime Agency - National Cyber Crime Unit* [Online]. Available from: <http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit> [Accessed 13 June 2016].

6. Her Majesty's Inspectorate of Constabulary (2014) *Policing the Crimes of Today with the Methods of Yesterday - Reinforcing Need for Cyber Trained Officers by HMIC.* [Online]. Available from: <https://www.justiceinspectorates.gov.uk/hmic/news/news-feed/policing-the-crimes-of-today-with-the-methods-of-yesterday/> [Accessed 7 April 2016].

7. College of Policing (2014) *Boost for Police Skills to Tackle Cyber Crime | College of Policing* [Online]. Available from: <http://www.college.police.uk/News/archive/2014may/Pages/Boost-for-police-skills-to-tackle-cyber-crime.aspx> [Accessed 4 April 2016].

8. Justice Inspectorates HMIC (2015) *Real Lives, Real crimes A study of digital crime and policing* [Online] Available from: <https://www.justiceinspectorates.gov.uk/hmic/wp-content/uploads/real-lives-real-crimes-a-study-of-digital-crime-and-policing.pdf> [Accessed 4 April 2016]

9. College of Policing (2014) *In focus: Giles Herdale talks on policing a new world of cybercrime* [Online] Available from: <http://www.college.police.uk/News/archive/2014nov/Pages/In-focus-Giles-Herdale.aspx> [Accessed 4 April 2016]

10. Schreuders, Z.C., Cockcroft, T., Butterfield, E., Elliott, J., Soobhany, A.R., and Shan-A-Khuda, M. (2017) *Needs Assessment of Cybercrime and Digital Evidence in a UK Police Force, The Cybercrime and Security Innovation (CSI) Centre, Leeds Beckett University.*

9.0 Appendix

Digital Media Investigator (DMI) role profile	
Purpose	The Digital Media Investigator (DMI) is embedded within major investigation or serious organised crime investigation teams, rape teams and, if required by the LEA, can be deployed locally to support local investigation teams on volume crime. DMIs will collate and coordinate on all matters related to CD and other technology media. The DMI will obtain contributions from SPoCs, Digital Forensics, Open Source and other technology teams and support the related elements of analysis and case preparation. They will author the technology and data component of the overall operational strategy and ensure execution of the strategy in partnership with other stakeholders.
Key Outcomes 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
Main Responsibilities	**Development of technology and data strategies** ▪ Lead the development of the technology & data strategy (developed in conjunction with Analyst, SPoC, Digital Forensics, Open Source and other relevant technology functions and channelled into the overall strategy managed by the SIO) ▪ Lead in the development of a digital profile for a victim, witness or suspect on an investigation **Coordination of expert inputs** ▪ Coordinate returned digital media products with related products from ANPR/CCTV/Financial Investigation teams ▪ Co-ordinate the input of expert witnesses such as cell site engineers or RF technicians to support work around communications data ▪ Provide guidance to SIOs / Investigators on the application of technology in investigations / operations ▪ Take guidance and input from experts in SPoC Unit, Open Source, Digital Forensics and other technology teams and feed this into the investigative process ▪ Use these inputs to prioritise workload to be passed to the SPoC Unit, Open Source and Digital Forensics teams ▪ Coordinate meetings, discussions, planning and review sessions between SPoCs, Analysts, Open Source, Digital Forensics and ANPR/CCTV functions as part of the investigative or intelligence gathering / analysis process, including maintaining minutes, actions and keeping a record of all technology and data lines of investigation

	CD acquisition and exploitation ▪ Manage delivery against the technology and data strategy ▪ Where required, prepare CD applications on behalf of investigations or operations, with guidance from SPoCs, for submission to the SPoC Unit and/or support advanced TLOs in doing this ▪ Discuss, analyse and evaluate returned CD with Analysts, SPoCs and Investigators feeding the result into the investigative process in line with the technology and data strategy ▪ Liaise with major incident rooms (Receiver and Action Manager) on appropriate technology and data actions **Prosecution and disclosure** ▪ Work closely with Prosecutors (as well as the Analyst and SIO where applicable) on the technology and data elements of the case and the preparation of evidence, drawing on SPoC, Digital Forensics, Open Source and ANPR/CCTV other technology team expertise to ensure evidential files and products are fit for purpose ▪ Handle excess data appropriately, assess its impact on the case and take relevant action to ensure that it is passed to the Disclosure Officer where required in accordance with CPIA **Knowledge sharing and continual improvement** ▪ Identify and action opportunities for continual improvement in the input of SPoCs, Open Source, Digital Forensics in investigations, sharing these ideas using provided processes and systems (via the DMI Lead where one exists) ▪ Use agreed processes and systems to share knowledge and experience gained with CD users both within and across LEAs
Reports Into	**Senior Investigating Officer (SIO)/Deputy SIO**
Skills	▪ Strong, competent investigative skills ▪ Ability to develop clear, concise articulate technology and data strategies ▪ Ability to complete a CD application form to the right level of detail for the type of request ▪ Ability to build strong working relationships with other teams e.g. Open Source, Digital Forensics, SPoC ▪ Basic skills in Excel and data manipulation / analysis e.g. filters and pivot tables ▪ Ability to use the LEA workflow system to submit applications ▪ Ability to present and communicate information clearly to all levels (both written and verbal) ▪ Ability to plan and prioritise high workloads with limited supervision ▪ Ability to challenge and influence the SIO, being able to successfully articulate the rationale behind the challenge ▪ Ability to apply RIPA and other legislation in practice to guide the acquisition of CD and other digital media ▪ Skills in management and coordination of multiple inputs from multiple individuals and teams
Knowledge	▪ Remain up to date on the techniques used by SPoCs, Analysts, Digital Forensics and Open Source teams through networking with these teams and other DMIs and

	understand how these techniques can be applied together and the possibilities / limitations of using them ▪ Understand the application of ANPR, CCTV and financial analysis to support digital media investigations ▪ A strong knowledge of RIPA and its applicability to investigations/intelligence operations ▪ Understanding of non-RIPA data available ▪ Knowledge of different technology and data types ▪ Strong understanding of investigative and prosecution processes and how to prepare cases / evidence ▪ Knowledge of disclosure procedures and CPIA ▪ Good understanding of the PII Process and procedures relating to sensitive methodology (not LI) ▪ Knowledge of the grading system for CD ▪ Understanding the implications of retaining CD and other media for intelligence purposes and the implications for its use as evidence in subsequent investigations and prosecutions ▪ Knowledge of how CD and other media can be used as evidence to show corroboration, correlation, common purpose, chronology, similar fact evidence, presence etc ▪ Knowledge of emerging technology, trends and how it impacts on data acquisition and media collection ▪ Knowledge of exhibits management and how to give evidence
Experience	▪ Practical experience of working on a broad range of investigations, including some with a data and technology focus (Essential) ▪ Experience of working in an environment where networking is critical (Desirable) ▪ Experience of influencing senior individuals (Desirable) ▪ Experience of working on a Major Investigation Team/Serious Organised Crime Investigation Team or local Criminal Investigation Team (Essential) ▪ Experience of utilising capabilities of SPoC / Open Source / Digital Forensics teams (Desirable) ▪ PIP Level 2 trained police investigator (or equivalent accreditation in other LEAs) (Desirable)
Special conditions	▪ An affinity and aptitude for communications technology ▪ Completion of relevant training relating to the role of DMI such as Core Skills in Communications Data training course, Open Source / Digital Forensics awareness training etc ▪ Attendance of any DMI CPD and refresher training, technology / media seminars / conferences and networking events ▪ The role requires receiving an appropriate level of clearance and can be a police or civilian officer ▪ The role may be full time for major crime cases, and will be a dedicated role within the team or part time alongside delivery of other responsibilities, depending on the LEA organisational model and resource availability