Perceptions of Money Laundering in Digital Crime Investigation

Michael Donegan

This dissertation is being submitted in partial fulfilment of the candidacy requirements for the degree of MSc Financial Investigation and Digital Intelligence

Department of Criminology and Social Sciences
College of Business, Law Social Sciences

Contents

Acknowledgements

I would like to assert my sincere appreciation to all of those that have guided and assisted me throughout my time at the University of Derby, without their support, it would not have been possible for me to complete my MSc Financial Investigation and Digital Intelligence.

To express my gratitude, I would first like to take the opportunity to thank my programme leader and dissertation supervisor, Dr David Hicks. Without David's understanding, patience and enthusiasm this dissertation would not have been achievable. Your commitment throughout the entire process, has been hugely appreciated

Secondly, my appreciation extends to Craig Hughes. Your passion and knowledge in respect of financial investigation has inspired this dissertation. The message that cyber crime doesn't exist is one I will be carrying forward!

Thirdly, I would like to display my appreciation to my wife, daughters, family and friends as they have all played a significant role in my success. At times of extreme stress when I have doubted my own ability, their words of reassurance have given me the confidence and optimism to achieve what I never thought I could. Your continuous support has helped me more than you will ever know, and I am forever in your debt. Thank you.

Finally, I would like to thank everyone that took part in my research project as without them this project would not have gone ahead.

Abstract

This dissertation presents an exploratory study on the perceptions of money laundering legislation within digital crime (DC) investigations. The data was drawn from twenty-eight (N=28) questionnaires completed by DC investigators from various ranks and forces throughout England and Wales.

DC or “cyber crime” is classed as a priority for many police forces. Significant budgets are spent on training officers and purchasing tools for investigating DC. This is a relatively new area of responsibility for law enforcement. In spite of this there is a plethora of research on DC. Much of this research is however based on the technical aspects of such criminality. Little attention appears to have been paid to tackling the financial motivation of digital criminals. In particular the application of the Proceeds of Crime Act 2002 (POCA) and money laundering offences in DC appears to be a gap in the literature.

This study will build upon existing literature by providing data and analysis on these concepts which appear to have received minimal research attention. The central research questions are:

1. Do digital investigators utilise POCA legislation relating to money laundering? (Central Research Question One - CRQ 1)

2. Do digital investigators perceive the legislation should feature in DC investigations? (Central Research Question Two - CRQ 2)

3. Do digital investigators feel they should be trained in financial investigation? (Central Research Question Three - CRQ 3)

Recommendations for policy and practice detailed in chapter five are based on results identifying minimal application of money laundering offences in DC investigations. The results also identified that a majority of DC investigators believed financial investigator training would be beneficial to their role.

Preface

DECLARATION

This work has not previously been accepted in substance for any degree and is not concurrently submitted in candidature for any degree.

STATEMENT 1

This dissertation is being submitted in partial fulfilment of the requirements for the degree of MSc Financial Investigation and Digital Intelligence.

STATEMENT 2

This dissertation is the result of my own independent work/investigation, except where otherwise stated. Other sources are acknowledged by explicit references.

STATEMENT 3

I hereby give consent for my dissertation, if accepted, to be available for photocopying and for inter-library loan, and for the title and summary to be made available to outside organisations.

Signed M Donegan (candidate) Date 11th February 2019

Figures and Tables

Glossary of Acronyms and Nomenclature

CDM	Confirm, Deny, Modify
CMA	Computer Misuse Act 1990
CPS	Crown Prosecution Service
CRQ	Central Research Question
DC	Digital Crime
DCon	Detective Constable
DI	Detective Inspector
DPA	Data Protection Act 2018
DS	Detective Sergeant
ERSOU	Eastern Region Special Operations Unit
FI	Financial Investigation
FIs	Financial Investigators
G	Supervisor rank in National Crime Agency
GDPR	General Data Protection Regulation
HMIC	Her Majesty's Inspectorate of Constabulary
IO	Immigration Officer
IPA	Investigatory Powers Act 2018
ISO	International Organization for Standardization
LE	Law Enforcement
ML	Money Laundering
MoJ	Ministry of Justice
N	Number
NCA	National Crime Agency
NCSC	National Cyber Security Centre
NPCC	National Police Chiefs Council
PC	Police Constable
POCA	Proceeds of Crime Act 2002
POLKA	Police OnLine Knowledge Area
RAT	Routine Activity Theory
SS	Sub sample
UK	United Kingdom
USA	United States of America
VC	Virtual Currency

Chapter One:
Introduction

Digital Crime (DC) or "cybercrime" is classed as a policing priority for UK law enforcement (LE) by the National Police Chiefs Council (NPCC, 2018). The terms DC or cybercrime has been defined in the UK by the Crown Prosecution Service (CPS) as referring *"to any type of criminal activity conducted through, or using, an Information and Communications Technology (ICT) device."* (CPS, 2018).

DC is seen to pose unique challenges for LE not present in non-digital offences (NPCC, 2018:3). One such challenge is technology facilitating international crime groups remotely targeting UK nationals (Saunders, 2017:4). The nature of these crime groups has seen an evolution in the motivations for DC (Dell, 2015). Literature highlights that early motivations were driven by curiosity, thrill-seeking and status (Kiger et al, 2004; Kremen, 1998). These appear to have now overwhelmingly been replaced by financial gain (Dell, 2015:2,3; Goldman and McCoy, 2016:595). The number of DC offences committed has increased significantly in recent years with a 9% rise in DC recorded between 2017 and 2018 (ONS, 2018). It could be inferred that this is partly driven by how lucrative the rewards are for digital criminals. Research has estimated that one particular DC incident earned the associated offenders $2.7 million a month (Goldman and McCoy, 2016:609).

Though the motivations for DC have been identified through research, the responses to combat them does not appear well documented. One particular gap in the literature appears to be how digital investigators within LE, utilise tools under the Proceeds of Crime Act (POCA) 2002, to effectively tackle the financial motivation. The objective of this research project is to identify and fill selected gaps within the subject area, whilst confirming, denying or modifying (CDM) the existing literature. To do so, this project focuses on the following research questions:

1. Do digital investigators utilise POCA legislation relating to money laundering? (CRQ 1)

2. Do digital investigators perceive the legislation should feature in DC investigations? (CRQ 2)

3. Do digital investigators feel they should be trained in financial investigation? (CRQ 3)

In chapter two a comprehensive literature review is outlined focusing on: the current state of DC, the CPS role, legislation and financial investigation in DC. These topics have been chosen to illustrate the limited available literature regarding digital investigator perceptions. Chapter three outlines the methodology used to design and conduct this research project. The techniques and rationale used to accomplish the research objectives are clearly explained in this chapter. This chapter contains details of the sample, the mixed methods approach, the data collection methods and ethical considerations. In Chapter four analysis and findings from the data collection are detailed. This is outlined in sections relevant to the CRQs above. The findings from the study will CDM those noted in chapter two, whilst critically

analysing the methodology identified in chapter three. Finally, chapter five, the conclusion, discusses the studies key findings and outlines recommendations and/or concerns for policy, practice and future research.

This studies research and data collection was completed prior to the introduction and effective implementation of the Criminal Finances Act 2017. Thus, this dissertation focuses on knowledge and implementation of POCA 2002 in DC investigations.

Chapter Two:
Literature Review

2.1 Introduction

In recent years considerable media attention has been paid to the subject of DC. The majority of this literature agrees that DC poses a significant threat and challenge for society as a whole. One article goes so far as to declare *"...Any modern state cannot remain secure and prosperous without securing itself in cyberspace"* (Reeve, 2016:1). The negative consequences of DC have a significant impact at a local community level in the UK. Research findings identify that those worse affected are groups already facing societal challenges, in particular women, the elderly and the economically disadvantaged (Homes Office, 2018:5).

LE is trusted by local communities *"to prevent and detect crime, …, and to provide assistance to those in need"* (Snell, 2015:2). Digital crime could challenge this position. The internet has driven criminal innovation with significant numbers of crimes being committed digitally (Europol, 2014:9). There were 3.6 million digital offences recorded by the police in 2016 (Muir,2016:1). Consequences arising from this are more people in need of assistance and a greater necessity for prevention and detection of crime. An argument could be made that if UK policing wishes to maintain the trust of local communities, it must respond to the technology changing their lives (HMIC, 2017:14) and become an integral element of combatting digital criminality.

There is not a universal acceptance of this consideration with arguments stating the challenges presented by DC are not best solved by LE (Muir, 2016). The police in the UK have embarked on developing an investigative and preventative DC capability. Policy documents on this, including the UK Cyber Security Strategy (2011) and the Serious and Organised Crime Strategy (2013) have focused on an "end-to-end national-regional-local response". The result is dedicated digital police investigators at local, regional and national agencies (NPCC, 2015:2). These officers receive technical training on how computer networks operate and how to obtain evidence from them (NPCC, 2015:30).

Digital offences in the UK have been split into two categories; cyber enabled which encompasses traditional crimes augmented with technology, and cyber dependant which covers offences which could not be committed without a computer (CPS, 2018). This latter category is governed by the Computer Misuse Act 1990 (CMA) and broadly involves unauthorised access to and impairing the operation of a computer (CMA, 1990: c18). This study will focus on CMA offences and those working on dedicated units investigating such offences. Cyber enabled offences will not be included as they cover a very broad range of offences and pieces of legislation, the scope of which is beyond this dissertation (McGuire and Dowling, 2013).

The current processes and tactics deployed by these agencies have been scarcely investigated **(CRQ1)**. This gap in the literature makes it difficult to identify the exact nature of the response to DC. Without this knowledge examining how LE are keeping pace with the development of DC becomes challenging. The author Bryant

(2008:87) commented directly on this development concluding that *"police are trying to keep pace with ...financially motivated, organised global criminal enterprises.".* This is corroborated by Maguire (2018) who highlights that the profits available from DC motivate bad actors to innovate and become early adopters of technology. If this research is accurate, it could be argued that to effectively challenge this motivation LE need strategies based on both digital and financial investigation. This would include utilising the Proceeds of Crime Act 2002 (POCA), particularly the offences around money laundering (ML) **(CRQ2)**. In doing so the criminal assets of DC offenders would be threatened with confiscation. The CRQs in this study are seeking to identify digital investigators perceptions on utilising POCA legislation to address the financial motivation outlined **(CRQ1,CRQ2,CRQ3)**.

ML can be defined as the concealment, acquisition, possession, retention or use of criminal property (POCA, 2002: c.29, pt. 7, Sec 327, 328, 329). Criminal property is that which constitutes a benefit from criminal conduct and the alleged offender knows or suspects it constitutes such a benefit (POCA, 2002: c.29, pt7, Sec 340). The definition of property is very broad allowing for a multitude of interpretations. It includes tangible, intangible and incorporeal property (POCA, 2002: c.29, pt7, Sec 340). Considering the DC perspective digital data could potentially be interpreted as criminal property within the purview of POCA.

2.2 Current state of DC

Research on the underlying causes for why individuals commit DC finds that economic factors (Okeshola and Adeta, 2013:99) play a major part. Many are confronting poverty or unemployment whilst others are simply on a quest for wealth (Hassan et al., 2012). These factors do not suggest that offenders are biologically pre-disposed to commit crime (University of Glasgow, 2016). External or sociological factors appear to have a more definite link to the commission of DC. Recognising why and how crime is committed allows theoretical concepts to be developed. These aim to improve the investigation and prevention of such criminality. Digital offending has been the subject of several studies reflecting this idea. The central question for many has been "*...to what extent theoretical concepts developed in relation to the "terrestrial world*" can be legitimately applied to the "*virtual environment*" (Leukfeldt and Yar, 2014:263).

One prominent sociological framework is Routine Activity Theory (RAT) (Cohen and Felson, 1979). It outlines prerequisites for crime occurrences. These are motivated offenders converging in space and time with suitable targets, in the absence of capable guardians. The implication is that the absence of either of the first two elements (offender and target) or the presence of the third (capable guardians) would be sufficient to prevent a potential criminal event (Miro, 2014:1). Some research findings have argued that RAT cannot apply to DC as it is in "*crucial ways discontinuous with the terrestrial world*" (Capeller, 2001). Others such as Grabosky (2001:248) have argued that the three tenets of RAT are as applicable to DC as any other crime type. Although its applicability is debated RAT has been used to positive effect in areas of criminality such as burglary (Adamson, 2005). For this reason, it will be used in this study when identifying the current empirical reality of DC and how the concepts proposed offer the potential to improve this reality.

Though research on the efficacy of the response to DC is very limited, it is possible to deduce some measure of effectiveness through the number of convictions for CMA offences. UK figures for cyber dependant crimes between October 2017 and March 2018 show 12,372 reported crimes (Action Fraud 2018). In all of 2017 there were 47 convictions for CMA offences, though not exactly the same time frame this equates to less than one per cent of the 12,372 crimes recorded (MoJ, 2017). DC is not alone in suffering a high attrition rate, in 2016 approximately one and a half percent of recorded frauds resulted in conviction (Blakeborough and Correia, 2017:6,21). Significantly though DC suffers a higher attrition rate which opens up a debate on whether LE are a capable guardian for DC **(CRQ1,CRQ2)**. It could be argued that as DC is a relatively new phenomena LE have only turned their attention to developing best practice in recent years (Gercke, 2006). As a result, the attrition rate could decrease in line with improvements in LE capability. Research findings undermine this argument stating that LE still have no effective training regime for the "*digital future*" (HMIC, 2017:15). If the conviction rate remains very low it could be argued that the number of motivated offenders will not decline. This is because the risk versus reward ratio is weighted in favour of reward (Shoshitaishvili et al, 2014) as the risk of LE action is minimal.

Answers to issues of this nature are often sought in new legislation introducing new powers for LE. The Investigatory Powers Act 2016 (IPA) is an example of efforts to improve the capacity of LE to tackle DC. Such measures are controversial as they can be seen as infringing human rights. A High Court (Carey, 2018) outlined that the IPA breached human rights through the collection of internet activity and phone records with no suspicion of serious crime. The introduction of new legislation also appears to direct attention away from whether the existing legislation was (or is) being used effectively. For example, the confiscation of the proceeds of crime through POCA legislation is believed to deter offending and symbolise that '*crime does not pay*' (Bullock 2014:45, POCA 2002). Unfortunately, cases detailed in CPS press releases cast some doubt on whether the proceeds of DC are being targeted for confiscation **(CRQ1,CRQ2)**. For example, in September 2017 the CPS highlighted that a defendant had been charged with a CMA offence involving the acquisition of data. No POCA offences or proceedings are mentioned (CPS, 2017) despite the defendant transferring and acquiring property, in this case data, of value. **(CRQ1,CRQ2)**

There appears to be no literature on why POCA has not been applied routinely to DC **(CRQ1)**. There are however some points from which an inference could be drawn. One argument is that the general approach to POCA by LE is inconsistent with applications of the law varying in terms of effectiveness (Sittlington and Harvey, 2018:1; House of Commons, 2016:31). The author Murray (2016:447) contends that investigation skills need an upgrade if LE are to prosecute ML offences effectively. Research by Chave (2017:437) corroborates this with findings that LE training in POCA is limited and inadequate **(CRQ1,CRQ2).**

Chave (2017:437) argues that the LE approach to POCA has failed to recognise the changing face of criminality. The separation of digital and financial investigators into distinct separate units may have contributed to this. For example, the National Crime Agency (NCA) includes an Economic Crime Unit which appears to have no place in its sub-structure for DC components (NCA, 2017). Rigid organisational

structures can limit innovative responses to problems (Brown and Sutton, 1997:22). Limited opportunities to gain skills from both subject areas could mean a narrow knowledge structure for investigators **(CRQ3)**. If LE do not utilise POCA effectively, then it could be argued that they are not using the full range of opportunities to undermine offenders' motivations in DC.

The case of an offender convicted in January 2018, can be used to gauge the current logic applied to ML within a DC context. Although convicted for CMA offences and ML the two counts were not directly related (BBC, 2018). The CMA offences appear to relate to unauthorised access and acts with intent to impair **(CRQ1,CRQ2)**. The offender was alleged to have unauthorised control over a large number of computers and to be using them to launch network attacks against a variety of businesses (BBC, 2018). The ML count related to an online commerce site set up to sell hacking tools for digital criminality (BBC, 2018). This does not appear to take data into consideration as criminal property even though the discussion above makes clear this connection. In the CMA offences, the unauthorised access to victims' computers was enabled through data, connection credentials, physically held on digital devices. This data has been obtained through criminality and was of significant (monetised) value to the offender. Such credentials can be used privately to facilitate further financially motivated DC or they can be sold through online criminal marketplaces to other digital criminals with the same motivation (Onaolapo et al., 2016).

Considering the broad definition of property within POCA the data in this circumstance could be used to substantiate any of the three ML offences. Though one might argue that this was not needed in this instance, the circumstances do provide a valuable insight to current practice and how it could be altered. The CRQs do not directly reference if data should be considered criminal property but the topic is covered in this studies research questionnaire (see Appendix A). The research will therefore be able to provide some insights to confirm or deny if DC investigators perceive data as criminal property. The researcher believes this concept has not been investigated which makes it an important gap in the literature to fill. **(CRQ1,CRQ2)**

2.3 CPS role

The key role in prosecuting DC offenders is held by the CPS as they ultimately decide the charges with which any suspect is charged. This results in CPS having a distinct impact on how legislation is applied to DC and how investigators perceive such legislation. In respect of ML the CPS guidance on the subject could negatively affect the perceptions of digital investigators **(CRQ1,CRQ2)**. This is due to the guidance potentially being seen as overly cautious with emphasis placed on considering public interest and *"careful exercise of prosecutorial discretion"* (CPS, 2017). Evidently it is in societies interest for legislation to be utilised proportionately, but this still means that it can be used proactively in the right circumstances. The guidance could be viewed as corroborating research findings identifying a reluctance by CPS to charge ML offences (Transparency International, 2014:3; Chave 2017:437) **(CRQ1)**. Institutionalised reluctance to use applicable law could account for the perceived low number of ML prosecutions and confiscations (Fitzpatrick, 2017:449; House of Commons, 2016:35,36) **(CRQ1,CRQ2)**.

If it is perceived that such offences generate few successful prosecutions it could undermine the motivation of digital investigators to utilise the legislation **(CRQ1,CRQ2)**. By not using the legislation to "*prevent and detect crime"* (Snell, 2015:2) the status of LE as a capable guardian for DC could diminish. Such an outcome would potentially lead to a greater number of motivated offenders as they perceive little threat from LE. To combat this the use of POCA legislation in digital investigations could be given positive attention and this could encourage CPS to utilise it for prosecutions. There appears to be little research on how the current limited use of POCA ML offences affects investigators. Data collected from CRQ 1 and 2 could help to fill this gap in the literature. Confirming a positive or negative perception of ML legislation may provide insight into a wider judgement LE have made. **(CRQ1,CRQ2)**

The CPS guidance does however have some positive points. One in particular, being the clear directive that ML offences are not confined to cases involving money (CPS, 2017). **(CRQ1,CRQ2)**

2.4 Legislation

Current research on DC appears focused on its technical aspects such as computer forensics (NPCC, 2015:30; Parliament Street, 2018:3) Concepts such as what legislation could be used to tackle DC receive little attention. Such a focus could lead to a binary viewpoint where improvement is measured in technical capability. The potential negative here is it could make it difficult to keep sight of improving the service offered to victims. Developing technology can become a case of what can be technically achieved rather than focusing on the benefits brought to society (Leonhard, 2016:ii). In policing this should mean a focus on developing a DC capability which serves local communities (Snell, 2015:2). By LE not expanding the focus beyond technical improvements it is possible that insights into best serving the community will be restricted. As an example, research findings assert that criminals in DC are *"financially motivated, organised global criminal enterprises."* (Bryant 2008:87). This statement could be interpreted as implying that POCA legislation may be central to effectively tackling the motivation for DC. However, the literature reviewed for this dissertation appears to contradict this point.

When authors reference legislation relevant to DC investigation, few highlight POCA offences (Bryant 2008:33,34,35; Walden 2016:65). Recent research considering how to improve digital policing in the UK demonstrates a similar pattern. It referred to working with "tech giants" and police hackathons but at no point made any consideration around FI and POCA (Hitchcock et al, 2017). Broadening the perspective to include financial considerations appears to be an important gap in the literature. CRQ 2 and CRQ 3 will identify data which can be used to help fill this gap.

The focus of the literature on the technical aspects of DC may be influencing the training and resources provided to investigators **(CRQ2).** Private training providers such as Firebrand (2017) do extensive work with LE training digital investigators.

Their syllabus focuses on the technical protocols and live forensic recovery of digital artefacts (Firebrand, 2017) **(CRQ2)**. The positive impact this has on DC outcomes is open to argument. One study found no link between technical training and an increase in positive investigative outcomes (Marcum et al. 2010:523). No other research could be found by the author measuring this correlation. Though it is an older piece of literature given the fast pace at which technology progresses, the correlation is worth consideration. Research evidence shows that communities within the UK have *"a strong concern for punishment and protection of the public"* (Victim Support, 2012:NP). If technical training is not addressing these concerns it corroborates the need to broaden the focus for DC investigation **(CRQ 2,CRQ3)**. Doing this could increase the number of positive investigative outcomes. Considering the RAT theory (Cohen and Felson, 1979) this could mean fewer instances of DC through positive outcomes lowering the number of motivated offenders.

The definition of criminal property outlined in the introduction is very broad. In spite of this most literature appears to only reference money and does not explore the concept of what constitutes criminal property. Harrison and Ryder (2016:9) detail that ML is the process of converting the *"dirty money"* linked to the proceeds of crime into *"clean money*". The NCA risk assessment on ML (2017:22) could be seen to reinforce an over-emphasis on money with risks from cash being a predominant theme. The literatures focus on money could be detrimental to the perceptions of how ML fits DC. This is because in digital offences the property of value is often data. Studies which do show data as a gateway to financial gain frequently do so inadvertently. For example, research by the author Ramage (2012:279) highlights data as a target of DC offenders, but draws no link to it being criminal property. **(CRQ2)**

Data is one of the most valuable commodities in the world today and has been referenced as the "new currency of the digital world" (Feijóo et al., 2017:248). McGuire (2018:125) concurs with the paradigm of data being seen as currency. Specifically referencing DC, the author McGuire (2018:15) finds that data is a major driver for criminal profits. Digital footprints have allowed for valuable information to be collected on all aspects of life (Feijoo et al., 2014:248). The literature does not go so far as to identify data as criminal property within ML legislation. This remains a gap in the literature but the concept of viewing data more as "traditional currency" is poignant. It could assist in highlighting the argument for data to be considered criminal property within the confines of POCA. **(CRQ2)**

Defining data as criminal property could change the LE approach to DC. It would allow greater use of ML legislation, which would more suitably account for the motives of DC offenders. POCA confiscation orders could also factor in the value of data when arriving at criminal benefit figures **(CRQ2)**. Such actions could positively affect the RAT principles (Cohen and Felsen, 1979), as LE would be recognising and seeking to undermine the primary motivation of offenders in DC.

2.5 Financial investigation in DC

Contrary to studies on UK LE, research in the United States of America indicates that LE there are utilising FI to deter cyber criminals. This appears to be targeted

towards the intermediaries facilitating the financial gains obtained from the digital offences. ML is not the focus of the research but it does highlight that denying access to financial intermediaries can be an efficient deterrent. This is corroborated in research detailing the important role financial intermediaries and money mules play in DC (Leukelfdt and Ruger, 2015) **(CRQ2)**.

One possible conclusion to draw from the above is that DC would reduce if access to financial intermediaries was limited. Relating this to the RAT principles (Cohen and Felson, 1979), LE could be a more capable guardian if DC investigators made efforts to disrupt financial intermediaries in the UK. The available literature does not however substantiate a concerted effort in DC to limit access to financial intermediaries. In fact, a report by CIFAS (2018:2) highlights that the money mule threat in the UK continues to grow, up approximately 13% in a year. In comparison the CPS news resource appears to have one report of convictions for money mules involved in DC (CPS, 2018) **(CRQ1,CRQ2,CRQ3)**.

Co-ordinated responses from LE to the threat also seem to be missing from the literature. Minutes from the Joint Fraud Taskforce (Home Office, 2017:2) reference *"The continued development of the Money Mules and Repatriation of Funds scheme"* but provide no mention of what response LE is providing to the problem. Most of the literature appears to put private enterprise such as banks on the frontline of mitigating the issue. One LE unit, Eastern Region Special Operations Unit (ERSOU, 2017), does reference a focus on "money mules from international crime" but gives no practical details on what this means. The lack of clear response may have prompted an enquiry set up by the All-Party Parliamentary Group on Financial Crime (House of Commons, 2018). This enquiry directly seeks to address the financial intermediaries' issue and the role LE plays in mitigating the problem.

LE focusing on FI opportunities and ML legislation could be seen as an important part of an effective response to the problem. There is some evidence to corroborate this point. An article in the Financial Times (2016) detailed that international LE requests to the UK relating to DC had jumped by 12%. The focus for this was the financial elements of the digital criminality not the technical. This is because of London being seen as an attractive centre for laundering "*the ill-gotten gains of cyber crime*" (Financial Times, 2016). **(CRQ3)**

Almost uniquely in the literature identified, McGuire (2018:124) concludes that LE should equip digital investigators with a range of "*cyber specific*" and "*financial*" skills **(CRQ3)**. Though not explicitly outlined in the literature it becomes clear why McGuire draws this conclusion. DC revenues identified in the study originated from crimes covering all of the CMA offences. Not only this but DC offenders are reported to be constantly re-investing profits to ensure the continuity of cashflows (NCSC,2017). This potentially opens up a wide range of traditional FI opportunities for DC investigators (McGuire, 2018). These range from interactions with financial institutes to contacting services for payment information. If this proved effective it could positively impact the capable guardian principle in RAT (Cohen and Felson, 1979). **(CRQ2,CRQ3)**

It is important to note that the conclusion drawn by McGuire (2018:124) was not based on the perceptions of DC investigators. This means that practitioners have

not corroborated the conclusion. This is an important gap in the literature. Those who are actively investigating such matters could be best placed to identify how relevant FI skills are for DC investigation. At present no study appears to have directly addressed this issue. The closest is a study into the perceptions of a broad range of LE officers into DC (Schreuders et al, 2018:15,20). Participants were not however asked directly about FI. **(CRQ3)**

The conclusion posed by McGuire (2018:124) is also open to being undermined due to potential research limitations in identifying strong evidence to substantiate arguments. For example, two authors, Anand (2015) and Fahmy (2010), are used to corroborate FI opportunities to disrupt digital criminality (McGuire, 2018:110). Unfortunately, these are news articles rather than academic sources. This maybe due to a lack of specific research in the area and highlights the importance of further studies into the subject **(CRQ1,CRQ2,CRQ3).** CRQ 3 is aimed at identifying if DC investigators perceive a benefit in FI training. None of the literature searched by the author outlined that the current DC investigation training regime included a financial element. The training roadmap published in NPCC (2015:30) guidance lists courses for DC investigators. No FI inputs are present in any of the courses detailed. This makes the perception of current DC investigators very relevant **(CRQ3)**. Confirming or denying whether they see a benefit could help modify the current training opportunities available.

There are alternatives to incorporating FI training **(CRQ3)**. For example, digital and financial investigators could be co-located so they could readily access skillsets. This is potentially corroborated by literature outlining the future challenges for LE as the rapid growth of technology and need for constant focused training to keep pace with this (Westera et al, 2014:197,202). DC investigators could be perceived as being at the forefront of this challenge and therefore should be left to specialise on DC.

Being left to specialise could though have an unintended consequence. Constant focused training on DC (Westera et al, 2014:202) is not guaranteed for non-DC investigators. Findings in a recent survey of UK LE officers highlighted that digital training was inadequate and that e-learning was ineffective (Tatham, 2017:26,43). This could isolate DC units and make it difficult for other units to engage with them effectively. For example, a financial investigator may not understand the context of a request made in a digital financial enquiry. This could mean significant time is spent explaining the context prior to the enquiry being progressed. Equipping investigators with financial and digital investigation skillsets could significantly streamline enquiries as they would have knowledge of both sides **(CRQ3)**

2.6 Conclusion

The literature clearly outlines that LE face significant challenges in effectively tackling digital criminality. Previous studies have outlined that the UK public perceive that "*the police will not/cannot do anything about online crimes*" (McGuire and Dowling, 2013:4). In light of this DC could be seen as a threat to the ability of LE to meet the needs of local communities (Snell, 2015:2). To counter this threat the options and powers available to digital investigators need examining. One of the options to improve DC investigation is utilising ML legislation. The researcher is

aware of only one study commenting on this option, it states that financial and digital skillsets should be combined (McGuire, 2018:121). This study did not go into detail over what elements of FI were important or how the legislation should be applied in a digital context. This is a gap in the literature which needs attention. It seems important that those actually working as DC investigators help to fill this gap. They can provide unique insight based on experience in the field. This study can contribute to this gap in the literature as it seeks the perceptions of DC investigators on FI and ML. The findings generated could also contribute to confirming, modifying or denying (CDM) the broad argument made by the author McGuire (2018) above.

One pressing theme from the literature is the focus on technical skills for digital investigators. It is widely agreed that technology is growing exponentially. New developments such as artificial intelligence and quantum computing are rapidly progressing and infiltrating society (Inglesant et al, 2018). These new emerging technologies are quickly exploited by criminal actors (Oreku and Mtenzi, 2017). This in turn means DC is changing rapidly and to remain relevant capable guardians police forces must respond. Improving the technical skills of digital investigators is vital (Hitchcock et al, 2017). Importantly though there is an argument technical DC training alone does not automatically lead to more positive outcomes (Marcum et al. 2010: 523).

Findings from other studies detail that DC needs a more holistic approach if the challenge is to be fully understood (McGuire, 2018:121). Evidence to corroborate this can be found in research commissioned by the College of Policing (CoP) (McDowell et al, 2015:4) which found a multi-pronged approach to aspects of policing could improve practice. The findings from central research questions 2 and 3 directly address whether FI should be part of the holistic approach suggested. This is important as the literature agrees almost unanimously that the primary motivation for DC is financial gain. This finding does not however translate into combined skillsets in the current DC investigation arena. In fact, how LE perceive this motivation and how they tackle it is not clear within the literature. Considering the RAT principles (Cohen and Felson, 1979), it seems that clearly understanding the challenge of DC would present opportunities to positively affect the three aspects.

Chapter Three:
Methodology

3.1 Introduction

This chapter will outline and explain the methodology utilised in this study to add value to the literature. The starting point is the ontological and epistemological considerations on which the study is built. These are important elements of social research (Bryman and Bell, 2003:29), and the philosophical position of the researcher needs to be clear.

There are two main contrasting positions when considering ontology. These are objectivism and constructionism. Both focus on whether or not social phenomena has an existence independent of social actors (Bryman, 2008:18). Objectivism implies that social phenomena is beyond the influence of social actors (Bryman, 2015:29). Constructivism reasons that social actors directly influence social phenomena (Robson and McCarten, 2016:25) leaving it in a constant state of revision. It could be argued that phenomena relating to LE have aspects of both ontologies. There are elements, such as legislation, which are external facts beyond the reach or influence of police officers. Pressure is applied by LE organisations for individuals to "*conform to the requirements of the organisation*" (Bryman, 2008: 18). Examples of this can be found in the police regulations which govern police officers in the UK (Police Federation, 2018). These points would indicate an objectivist ontology within LE social phenomena.

The scope of policing responsibilities is wide and not always clearly defined potentially making the role of LE unique (Roycroft, 2017: vii). If this is accurate it does challenge the objectivist standpoint. Fulfilling these responsibilities means that LE officers are involved in social interchange with a wide range of people. This makes social interactions difficult to predict and thus subjective in character (Guillot, 2016). Such a viewpoint allows the argument that social actors are going to be relevant to how social phenomena play out. The author Finanne (1990:218) provides some corroboration for this noting, *"Every level of police work, especially at the micro level, involves choice on the part of the police officer".* Based on the argument that subjective choice is available to social actors (Bronitt and Stenning, 2011:320) this research will posit that constructionism is a more suitable ontology for the social phenomena under examination.

In terms of epistemology, a significant central issue is whether the social world can and should be studied according to methods of the natural sciences (Bryman, 2008:13). Positivism focuses on the explanation of human behaviour, and interpretivism seeks to understand it (Bryman, 2008:15). This latter position requires researchers to interpret the subjective meaning of social action (Bryman, 2008:16). Positivism is not amenable to such concepts as it details that phenomena and hence knowledge can only be confirmed by the senses (Bryman, 2008:12). Several recent studies into LE perceptions of DC have utilised an interpretivist approach (Cockroft et al, 2018: Schreuders et al, 2018).

These studies sought a broad spectrum of perceptions and provided findings on the qualitative data provided by participants. It could be argued that the interpretivist

epistemology allowed the research to reflect the meanings people bring to phenomena and how they use it to make sense of their world (O'Donoghue, 2007: 16-17). It is important to add that these studies placed no dedicated focus on digital investigators, as such there is still a gap in the literature (Cockroft et al, 2018: Schreuders et al, 2018).

The CRQs in this study are seeking to identify the subjective meaning of social action (Bryman, 2008:16). Interpretivism therefore could be a potential epistemology for this research project. There is however a further consideration. Interpretivism seeks to develop objective science to describe social action (Andrews, 2012:39). Applying an objective interpretation to the unpredictable and arguably subjective nature of LE social interactions (Guillot, 2016) could limit the research findings. Some LE agencies recognise constructivism and social constructivism as major elements of how officers attain knowledge (Hong Kong Police College, 2011; Shipley, 2017). These theories perceive the learner as a unique individual, who constructs meaning and knowledge through cultural and social communities of discourse (Fosnot, 2005:1).

In essence the individual forms their perceptions and actions from the nature of the experiences they encounter (Guidere, 2006:4). The varied and unpredictable social interactions faced by LE officers (Guillot, 2016) could lead to the development of individual and unique knowledge constructs. This could manifest itself in many different situational responses from officers even when faced with the same circumstance. Recognising that digital investigators could believe in many versions of reality (Guba and Lincoln, 1994:111) was a key consideration to the research design. The reason for this is that in social constructivist theory all such differing views of reality are to be or could be considered valid (Guba, 1990:41; Hugly and Sayward,1987:278). This is the epistemological position adopted in present study as it is believed that each participant will provide a potentially unique input to the data generating new or novel insight into the CRQs. This epistemology has been used by other studies into LE phenomena (McComas, 2017; Chavez, 2012) though they have not focused on investigators perceptions into their professional practice.

The CoP outline that evidence-based policing is "*the use of best available evidence to inform and challenge policies, practices and decisions"* (CoP, 2018). This could be taken as focusing on a positivist epistemology particularly as the CoP input talks of testing new initiatives (CoP, 2018). Testing hypothesis, in this case new initiatives, is a principle of positivism (Bryman, 2008;13). The application of evidence-based methods in other professions such as social work, has caused some concerns over restricting the variety of research approaches used to understand relevant phenomena (Drisko and Grady, 2012;19). These concerns could be exasperated by DC whose investigation is impacted by the continual progressive development of technology (Schreuders et al, 2018). As a result, digital investigation could be seen as a social phenomenon in a constant state of revision (Bryman, 2008:19) dictated by technological developments and their influence on social actors. Restricting research methods into DC may neglect to accurately reflect a phenomena where social actions could be difficult to measure using natural sciences (Bryman, 2008:697). Considering this one could argue that constructionism and social constructivism will more accurately reflect the constant state of revision affecting the phenomena and accordingly give a greater insight.

The other sections in this chapter will provide effective signposting to the methodological approaches deployed to address the CRQs. This includes the participant sample, data collection method, data analysis, ethical considerations and conclusion. Critical analysis is utilised to justify why particular methods positively contributed to the project with strengths and weakness documented for the readers benefit.

3.2 Sampling frame

Generating data on the perceptions of a particular subset of individuals meant the target population had explicit criteria for inclusion. The reason for minimising the available population were based on the current issues LE face with DC. The HMIC findings (2017:15) that LE still have no effective training regime for the "digital future" outline that frontline policing is still not equipped to effectively deal with DC. As such the insights these officers could provide to the study may not be so great as those working on specialist DC units who receive dedicated training (NPCC, 2015). The other consideration was that without inclusion criteria insights from many different cultures within LE could be obtained. This could introduce sources of error into the research. Studies have outlined that LE has a distinct culture that it is potentially socially constructed (Dick and Jankowicz, 2001:183). There is not however one overarching culture, Holdaway and Parker (1998) found that certain specialist posts within LE have their own unique culture.

Obtaining knowledge and insight into these various cultures would be necessary to effectively interpret results. Unfortunately, the broad responsibilities of LE (New Statesman, 2014), may have created numerous distinct cultures. Accounting for all of these was not deemed practical or achievable in this study. Considering these points, it was believed that those working in a LE digital crime culture would be the most suitable participants. They are the individuals working within the current system and best placed to provide insight into its mechanics. The conditioning of the distinct culture they work within may also have provided them with unique perceptions which would provide new or novel data for the studies CRQs. This meant the target population comprised of digital investigators from local, regional and national LE agencies who dealt with cyber dependant (Action Fraud, 2018) criminality in dedicated DC units.

Strategically applying the sample criteria to ensure participants were *"selected because of their relevance to understanding a social phenomenon"* (Bryman, 2008:415) meant a purposive sampling method was employed. Purposive sampling has been utilised in several other qualitative research studies on DC and policing (McGuire, 2018; HMIC, 2017; Hitchcock et al, 2017). Purposive samples do restrict the generalisation of results to a population (Bryman, 2008:415), potentially limiting the impact of research findings. Elements of this studies research design could still allow for the sample to be viewed as logically representative of the target population (Lavrakas, 2008: 645). For example, the researcher being involved in the field of DC investigation by LE allowed for greater access to the target population. This ensured that a cross section of local, regional and national DC investigators contributed to the research.

Snowball sampling techniques (Bryman, 2008: 184) were utilised in the research. Contact was made with a small group of known digital investigators to request they engage as participants. As part of this they were asked to establish contact with other relevant individuals to request they become participants. Attendance at digital investigator conferences were also used as opportunities to reach out to the target population. Paper copies of links to the research were handed out to those identified as meeting the sampling frame. An invitation to participate was also posted on a LE forum called the Police OnLine Knowledge Area (POLKA). These efforts helped to ensure that the target population was effectively engaged and had the maximum opportunity to participate.

3.3 Sample

The definitive target population size is not known. Finding this out would have involved enquiries with every LE agency in the UK, it was felt that this would take too much time so was not carried out. Estimates were made instead based on National Police Chiefs Council guidance (2015). This report provides an input on staffing levels for local force based cyber crime units. It recommends two investigators per local unit. There are 45 local police forces (Police, 2017) which allows an estimate of 90 digital investigators. There are 10 regional cyber crime units (Justice Inspectorates, 2015), in 2015 it was outlined in the guidance that there were 69 officers at this level (NPCC, 2015:3). There are two national units, the NCA and the National Cyber Security Centre (NCSC) (NCA, 2017:3), but insight into their staff numbers has not been gained. The figures detailed allow for the argument that the number of digital investigators is relatively low, the estimation being 150 - 300. It was based on this consideration that the researcher aimed for 50 participants. It was believed that the number was high enough for findings to be largely representative of the population but manageable in terms of time and resources.

Taking the above into account the anticipated number of completed data collection instruments was fifty (N=50). The total number of responses collected was 73 (N=73) though not all were completed. Of this number 45 (N=45) were only partially completed responses. The reasons for this partial completion rate and low overall response rate will be explored in the data collection section. Only having 28 completed responses does negatively impact on the how generalisable the research findings will be. This is a small sample and thus the research findings only represent a small percentage of the target population. The sample would have had to have been bigger or randomised for more positive claims to be made on its generalisation across the target population (Bryman, 2008:180).

From the background data taken from participants it was possible to identify how many digital investigators from local, regional or national level participated. There were 14 (N=14) who identified with local policing, 10 (N=10) at regional level and 7 (N=7) at national. The figures appear inaccurate, however, 2 participants associated with multiple levels of policing. Given that regional and national levels do share some structures and processes (Justice Inspectorates, 2015:6) it is plausible for a participant to associate with multiple levels. The actual agency participants worked for has not been collected. This was a design feature to safeguard the participants anonymity. Details on this are discussed in the Ethical Considerations section. All participants, given they were working for law

enforcement agencies, were over the age of 18 which is the minimum age to join these agencies (NCA, 2018, CoP 2018).

3.4 Data collection

An online questionnaire was deemed by the researcher to be the most appropriate method for obtaining relevant data for the CRQs outlined in chapter one. Online questionnaires benefit from being economical; relatively easy to arrange and, dependent on their format, can facilitate accessibility (Denscombe, 2014: 181). Further to this, questionnaires still allow for the collection of rich qualitative and quantitative data (Henn et al., 2013, Bryman, 2008:653).

In this research project these benefits assisted the researcher in a number of ways. The target population works for LE agencies across the United Kingdom. This makes the practicalities of approaching and engaging with them face to face difficult. One of the only ways of doing this is in a time and cost-effective manner is through digital means (Bryman, 2008:653). The use of a digital questionnaire also works well in this research as it suits the target populations skillset (Yun and Trumbo, 2000). Being time and cost effective allowed for the collection of data at an early stage in the project. This assisted in allowing the researcher to work within the time constraints of the project. Ethics approval was issued on the 21st February 2018, efforts to obtain the desired number of responses were exhausted by July and project completion is scheduled for December 2018.

It is important to note that questionnaires do have a number of limitations. Bryman (2016:192) details two particular disadvantages; one being that they almost always result in lower response rates and the second is they do not make it easy to ask a lot of questions. The implications for this research were limited opportunities to describe the perceptions prevalent in the target population. The limitation noted on response rate was corroborated in this study with only 28 completed questionnaires. Unfortunately, it is not possible to explore the low response rate in more depth. This would have necessitated further engagement with the target population which was beyond the scope of this research. The only further insight which can be offered is the limitations outlined are long standing issues which have featured in other research (Sheehan, 2001; Crawford et al., 2001).

Several other methods of data collection were considered for this research. Interviews have a number of benefits for data collection. They allow for a depth of information to be obtained (Ragin and Amoroso, 2010:123), have a high response rate and produce data based on participants priorities (Denscombe, 2014: 231-233). Despite these positives, interviews can take a long time to complete (Ragin and Amoroso: 2010:3) which leads to practical implications such as timescales and finances (Edwards and Holland, 2013:66). For these reason interviews were not deemed appropriate for this research. Observations are a great way of verifying what people actually do, as opposed to what they say they do (Denscombe, 2014: 212). In spite of this, they were deemed unsuitable for this project. They suffer from the same drawbacks as interviews in that the time taken to collect sufficient data can be prohibitive (Cooper, Lewis, Urquhart 2004:7). Secondary data analysis was also considered particularly as this would provide data without the need for expending time and resources (Crow and Semmens, 2008). Unfortunately, as

outlined in the literature review there are no secondary data sources outlining the perceptions being sought.

The questionnaire completed by participants was designed using an online service called Smart Survey. There were 24 questions detailed with the majority being open questions and the minority being closed. It was felt that a largely qualitative approach was required to add value to the literature within the epistemological framework. The rationale for this was that qualitative data better reflects participants interpretations through providing a rich depth of detail (Denscombe, 2014: 302). As a result, 16 open questions were posed. It was hoped that this would allow participants the maximum number of opportunities to answer in their own terms (Bryman, 2008:232) as per their perceptions.

The remaining 8 questions were closed in nature and served to collect quantitative data. Though closed questions inhibit the participants ability to answer in their own terms (Bryman, 2008:232), they are straightforward to comprehend and answer, as well as being quick to code during the analysis process (Henn et al., 2013; Bryman, 2008:235). In this research it was thought that the collection of quantitative data focused on the practical usage of ML legislation could be beneficial. The use of POCA legislation is believed to be valuable in identifying factors which have influenced investigators perceptions.

The use of closed questions was also used to help mitigate researcher basis. It is argued that all social research is biased since the values of the researcher are always present (Holloway 1997). This is considered to be accurate in this instance as the researcher sees ML legislation as being of potentially great benefit to digital investigators. Certain questions were multiple choice offering yes or no options followed by a why question for context. Leading the participant to a limited number of answers goes against the aims of truly reflecting their perceptions. It does however provide a potential benefit. Clear positive or negative responses and insight into the participants response rationale, helps to prevent a gross misinterpretation of data to fit the values of the researcher.

The quantitative data gathered will be subjected to statistical and content analysis (Weber, 2004). Utilising this transparent research method (Bryman, 2008:288) will assist in identifying any researcher bias. Elements of Grounded theory (Corbin and Strauss, 2008) will be utilised. The researcher's interpretation of the data will influence the coding (Charmaz, 2000: 515) and any theories outlined will be grounded in the data collected. This decision is due to the suitability of grounded theory to exploring subjects where there has been little exploration of contextual factors (Crooks 2001). In subjecting the qualitative and quantitative data to these analysis approaches this research has a mixed methods approach (Hesse-Biber, 2010; Golder et al., 2017). In merging and connecting the qualitative and quantitative data when analysing results, a better understanding of investigators perceptions could be obtained (Creswell, 2006:7). There are potential drawbacks to this approach, difficulties can arise if the quantitative and qualitative results do not agree. If this occurs it poses a particular challenge as often further data collection is required (Cresswell, 2006:66). This would be beyond the scope of this research and could only be considered as a future research consideration.

Unfortunately, any disagreement only becomes apparent during the analysis so this will be discussed in the following chapter.

Identifying some measure of the participants knowledge of ML and its application to DC was deemed important. The findings in the literature review relating to POCA allowed the argument that a lack of knowledge on the subject may be affecting perceptions (Chave, 2017: 437). As such several questions were designed to provide insight into participants knowledge of ML. These questions were posed as content specific scenarios which asked participants to respond to the circumstances laid out (Brush and Saye, 2008:7). This design decision was based on the difficulty in measuring knowledge of problem-based inquiry with standard collection instruments such as observation forms (Brush and Saye, 2008:7). To counter this difficulty scenario-based assessment has been successfully implemented in fields such as business (Callanan and Perri, 2006), ethics (Snow and Bloom, 1996), and technology (Barrett at al., 2006). None of the studies identified in chapter two utilised scenario-based questions though it has been applied by recent studies into digital social phenomena (Jafarkarimi et al., 2016). Utilising scenario-based questions in this research will potentially generate new and novel insight into the CRQs.

The research findings outlined by Bryman (2016:192) informed several design decisions. To counter the two negatives highlighted, low response rate and difficulty in asking a lot of questions (Bryman, 2016:192), the questionnaire was kept concise asking just those questions crucial to the research (Denscombe, 2014: 172). By keeping the questionnaire concise the mental burden of answering the questions was reduced. It was hoped this would minimise participants offering "satisficing" answers which could negatively affect the data collected (Krosnick, 1991). Corroboration for this decision can be found in research results which identified that response rates were lower for longer questionnaires (Rolstad at al., 2011:1101). In asking a minimum number of questions it could be argued that insight will be limited due to a lesser volume of available data. To counter this argument the aim was to obtain a significant number of completed responses.

The questionnaire has been designed to be completed by participants without oversight from the researcher. The validity of self-completion data collection has been called into question as there is a difficulty in verifying the responses given (Ong and Weiss, 2000:1691). Despite this issue self-completion questionnaires can be a valid data collection method when gathering a breadth of information (Ozer and Reise, 1994) as this research seeks to do. Self-completion questionnaires have been in used in research on DC (Marcum et al. 2010) though it is important to note the studies referred to in Chapter 2 predominantly utilise other methods. Efforts were made in the design of this study to respond to concerns over validity. Factoring in participant anonymity was done for ethical reasons, covered in the next section, and to facilitate the collection of more accurate data by minimizing social desirability pressures (Lelkes et al., 2012:1291; Paulhus and Vazire, 2007).

Question content was considered carefully to reduce potential sources of error. The wording of questions needed to be appropriate and focused to prevent confused or unsuitable responses. Data arising from unsuitable responses could distort the

findings and analysis in chapter four (Henn et al., 2013). Part of being appropriate was ensuring the nature of questions minimised any risk of embarrassment or sensitivity. Numerous studies have found that the quality of questionnaire data is especially worrisome where questions are likely to be perceived as sensitive or embarrassing (Armacost at al., 1991; Becker and Bakal, 1970; Bradburn et al., 1978). To minimise concerns on this issue no questions required participants to critique their agencies response to DC and ML. Such questions could have been interpreted as being sensitive in nature. The consequences of the decisions made in regards to question content will be discussed in Chapter 4. It is only after the data collection that possible ambiguity or issues are revealed.

The questionnaire content was designed to add value to the findings presented in the literature review. For a complete list of the questionnaire that was distributed to the participants, please refer to appendix A.

3.5 Ethical Considerations

The ethical considerations in this dissertation ensure the research is compliant with the University of Derby Policy and Code of Practice on Research Ethics (2013). The control and processing of personal data has been carried out as per the requirements set out in the Data Protection Act (DPA) (2018) and the General Data Protection Regulations (GDPR) (European Parliament, 2016).

All participants were provided, at the beginning of the questionnaire, with an information briefing and informed consent form. No deception or misrepresentations were desirable so the information provided was clear and thorough. This helped ensure that participants were suitably informed of the research intentions and what would be done with the data collected. With these measures in place it was felt that participants should be capable of providing informed consent (Curtis and Curtis, 2011). Before being able to proceed to the questionnaire all participants were required to tick a box confirming they had read and understood the consent sheet.

Safeguarding confidentiality was deemed essential and so participants identity was not revealed at any point of the research. Such a disclosure was felt to violate the right to private and family life outlined by the European Convention on Human Rights (Article 8, 1950). Providing anonymity also reduced the risk of potential harm to participants. This was an important consideration in proving compliance with the University of Derby Policy and Code of Practice on Research Ethics. Protecting the rights, dignity, safety and privacy of participants through non-malfeasance and beneficence is an essential element of the policy.

To uphold confidentiality the privacy policy of the Smart Survey website was reviewed. It was outlined in the policy that user specific data was collected (Smartsurvey, 2017). To prevent such measures leaving participants at risk of being deanonymized, they were advised to read the privacy policy and engage tactics which could prevent identifying data being collected (See appendix B for list of tactics). This advice was provided to potential participants in emails, on POLKA and in paper copies.

It was made explicitly clear that participants were volunteers who could withdraw at any time up until project completion. There no incentives offered for participation. Within the questionnaire, participants were asked to create their own unique identifier of two letters and two numbers. It was explained that this should be something meaningful to the participant but not personal information. In doing this the participant was still able to withdraw from the study if they so wished. This did not compromise the anonymity of the participant as there was no possibility of the researcher drawing links to participants unless they elected to withdraw.

If a participant did choose to withdraw the identifier was used to highlight the relevant data. This would then be destroyed and cease to form part of the research. This was compliant with the GDPR directive around individuals right to be forgotten (European Parliament, 2016).

The security of the research data has been considered. The service provider smart Survey will host the data generated. They are ISO 27001 and Cyber Security Essentials Plus certified. ISO 27001 is the best-known standard for an information security management system. To achieve this an entity must demonstrate stringent processes for safeguarding data (ISO, 2017). The Cyber Essentials certification is a government initiative to certify companies which have taken measures to safeguard their computer network (Cyber Essentials, 2017). Smart Survey also ensure that all data is encrypted during transit and at rest. These measures are robust and provide a reassurance to participants that data is being handled responsibly.

Throughout this process the researcher will retain their role as the “Data Controller” and the primary data collection will be conducted through the recognised “Data Processor” (DPA, 208). In this case that is Smart Survey who are compliant with UK/EU government and industry standards. None of the data is utilised for marketing or resale value. This is detailed in their privacy policy (Smart Survey, 2017). Therefore, it is possible to assure participants that the data they generated will only be used for the research proposed. All of the research data gathered will be securely destroyed once the research product is complete.

3.6 Conclusion

Most of the studies identified in the literature review use analysis of secondary data (Leukfeldt and Yar, 2014; McGuire, 2018; Hassan et al. 2012). There is evidence though of surveys also being a suitable medium for data collection in respect of DC (Okeshola and Adeta, 2013). Considering the time constraints of this project and the geographic nature of the sample, the researcher believed that an online questionnaire was the most appropriate data collection tool.

The use of a mixed methods approach has been identified in other studies relating to DC (Cockcroft et al. 2018). Its use does however appear limited with many of the studies identified utilising qualitative methods (HMIC, 2015; Schreuders et al., 2018). Utilising mixed methods is hoped to enhance explanations of significant findings (Onwuegbuzie and Leech, 2004) relating to the same social experiences (Pope and Mays, 2006). This was believed to be important in identifying new and

novel insight into the CRQs, even when considering the potential drawbacks detailed in the data collection section.

The decision on the sampling frame differs from the other literature identified in chapter 2. None apply the inclusion criteria detailed in this study. In spite of being different this inclusion criteria was considered necessary to provide accurate and appropriate data for the CRQs. It is believed to have done this by targeting the appropriate sample population. Utilising scenario-based questions is another departure from research methodologies identified in chapter 2. However as identified they have been successfully utilised in non-DC studies (Snow and Bloom, 1996). The methodological approaches outlined in this chapter will ensure this research offers new and novel data aimed at adding value to what was presented in the literature review.

Chapter Four:
Analysis and Findings

4.1 Introduction

This chapter seeks to add empirical value to the findings from chapter two, the literature review, through analysis of the primary data collected in this research. The impact of the methodology, discussed in chapter three, on this analysis will also be referred to. The three CRQs, referred to in chapter one, have been devised based on the literature review and methodology. To reiterate, the research questions are:

1. Do digital investigators utilise POCA legislation relating to money laundering? (CRQ 1)

2. Do digital investigators perceive the legislation should feature in DC investigations? (CRQ 2)

3. Do digital investigators feel they should be trained in financial investigation? (CRQ 3)

4.2 Participant overview

The respondents in this study numbered 28 (N=28). In this chapter when referring to the source of a response, participants will be referred to by a unique identifier. This will be made up of their self-reported rank and a number reflecting the order in which the questionnaire was completed (after removal of partial questionnaire completions). Rank will be abbreviated as per the glossary of acronyms in the front matter.

4.3 Digital investigators use of money laundering (CRQ1)

No literature could be found on whether POCA legislation is utilised to tackle any financial motivation relating to DC. This section therefore seeks to address this important gap by exploring the use of ML legislation by digital investigators.

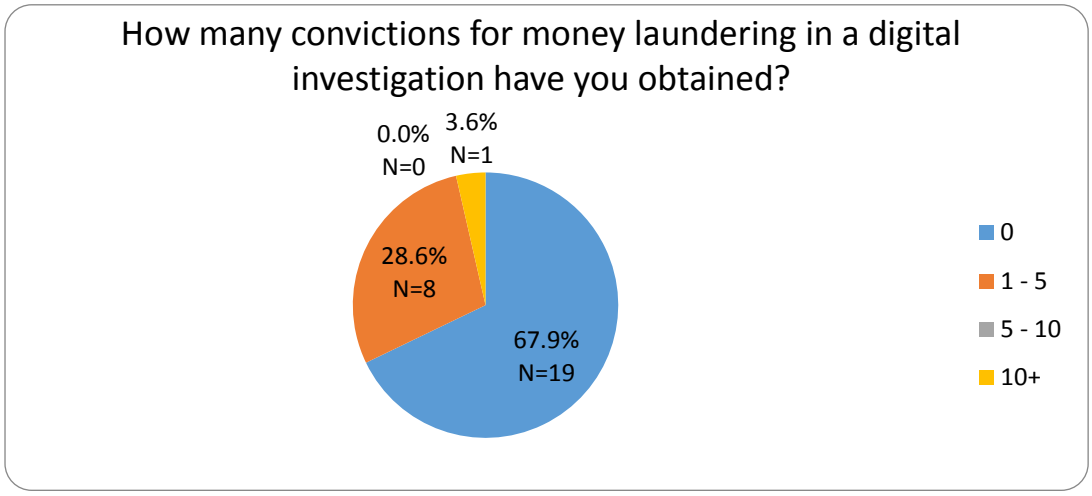
Usage was interpreted from data relating to application of ML legislation in respect of DC, convictions for ML relating to DC and knowledge outlined in scenario-based questions. In respect of applying ML legislation 53% (N=15) of the full sample stated they had, with the remaining 47% (N=13) detailing they had not used it. This finding allows for several potential conclusions. Just over one in two investigators applying the legislation may be seen as a positive. Not every investigation will necessitate the application so 53% could be seen as proportionate to this fact. Another interpretation is that 47% having never applied it is quite high, and thus a negative reflection on its application in DC. Identifying corroboration for these interpretations is not clear cut. No exact figures were available in the literature reviewed to clearly highlight how much DC is financially motivated.

The literature review did however provide qualitative corroboration for the negative interpretation outlined. It highlighted that financial gain was a key motivating factor in DC (Bryant 2008: 87). Other literature supports this assertation stating that

money is a prime motivator for DC (Saunders, 2017:4). Estimates by the NCA put the cost of digital crime to the UK economy in the billions of pounds (NCA, 2016). Reviewing this literature, it is possible to argue that ML offences would apply in the clear majority of DC investigations. As such the number applying the legislation should be significantly higher. Greater insight into this CRQ could have been achieved by asking two further questions. First, where applicable, why a participant had not applied the legislation. Secondly, where applicable, how many times had a participant applied ML. Not obtaining a greater depth of data in relation to this was a negative in respect of the research design. Some mitigation of this was possible through other aspects of the methodology. Primarily this was achieved through analysis of participants examples of utilising the legislation.

From the Sub Sample (SS=15) who did provide an application example, 40% (SS=6) related to cyber dependant criminality. The remaining 60% (SS=9) referenced fraud offences with a digital component. The reason for the answers detailing frauds may be a misinterpretation of the phrase “digital crime”. It was defined in the participants information briefing as referring to Computer Misuse Act 1990 offences. This definition was provided at an early stage and was succinctly outlined to prevent any confusion. Given this it is not clear why the misinterpretation occurred. Removing the data relating to frauds significantly changes the initial application data. As per the definition of DC provided to participants, ML had been applied by 21% of the full sample (N=6). This increases the number not applying ML to 79% (N=22). This re-evaluation of the data draws more support to the negative interpretation in respect of usage of the legislation.

Table 1 below illustrates the data obtained from the question on convictions achieved for ML:



The results appear to show 32% (N=9) of participants have secured at least one conviction. Nearly one third achieving a conviction could be considered quite high given the potentially limited application (21%) identified. Unfortunately, the misinterpretation of DC affected this analysis with only 3 participants relating their experience of a ML conviction to a CMA offence. As such a more accurate representation in respect of the question asked would be 10% (N=3) of participants had obtained a conviction utilising the legislation. The exact number of convictions is not known as the questionnaire did not ask for this information. This is a limitation

of the research design, greater accuracy in regards to the precise figure would have allowed a more definite demonstration of value added to the literature in respect of CRQ1. The best possible interpretation from the data collected in this research is a lower and upper range in terms of number of convictions. All three participants indicated that they had between 1 and 5 convictions. The range of potential offences is therefore between 3 and 15.

The findings outlined above allow for a strong argument outlining that ML legislation and thus financial strategies are utilised infrequently in DC. In particular the data suggests a significant attrition rate between application and conviction. DC does not appear unique in this context. Literature identifies that ML offences are not prosecuted effectively in the UK across all crime types even in fraud instances where ML is intrinsically linked (Blakeborough and Correia, 2017:4; Button, Shepherd and Blackbourn, 2016:8; Murray, 2016). This allows the contention that high attrition rates between application and conviction are common to all crime types relating to ML.

If ML legislation is utilised infrequently and not prosecuted effectively, calls for further legislation to combat DC are open to scrutiny. Without correctly identifying what options existing legislation provides, the logic in calling for more powers may be flawed. There is no guarantee that new legislation will be implemented any more effectively than that which already exists. Issues with the implementation of legislation are detailed in chapter two with numerous authors criticising the ineffective application of POCA (Sittlington and Harvey, 2018:1; House of Commons, 2016:31; Murray, 2016: 447; Chave, 2017: 437). Consideration needs to be given to analysing the application of existing powers. Such analysis should investigate whether the terms of existing legislation inhibit DC investigation, or if there has been a failure by LE to effectively utilise it. Further data collection beyond the scope of this research would be needed to provide this insight.

Analysis of qualitative data obtained from the scenario questions, allowed for examination of participants perceptions in regards to CRQ1. The analysis firstly focused on whether participants felt ML offences could be considered in the DC circumstances outlined. The second focus was if they believed ML offences should actually be utilised as opposed to just considered.

In scenario question one 57% (N=16) of participants, the lowest of the three scenarios, outlined they would consider ML offences. Potential reasons for why it was the lowest will be discussed when considering CRQ2. One quick insight into this may be the theme of financial gain. Many of the answers provided by the sample highlighted a focus on obvious instruments of financial gain, cash being one example. The first scenario did not mention any obvious financial gain as it sought to obtain participants perception of criminal property. This design decision may account for the low figure considering ML offences. This logic could also apply to the scenario having the lowest number of participants utilising ML offences. Only 39% (N=11) deemed such offences appropriate with the remaining 61% (N=16) not employing the legislation.

For the remaining scenario questions the same number of participants (N=23) indicated that they would consider ML offences. Although a higher number

considered the offences, on both occasions a significant drop was seen in those committing to utilise the legislation. In scenario question 2 50% (N=14) detailed they would utilise it and in scenario question 3 the figure was 46% (N=13). The financial gain theme may also have played a part in these findings. None of the scenarios directly referenced money or other financial mechanisms being obtained. It is apparent in the sample data that many participants perceived an obvious financial gain as an important factor when considering utilising ML. This links in with the literature gap identified in chapter two regarding criminal property. Investigators perceptions could be interpreted as reflecting the financial focus provided in the literature (Harrison and Ryder, 2016:9). As a consequence, investigators may be inhibiting use of the legislation by not utilising the broad definition of criminal property (POCA, 2002: c.29, pt7, Sec 340) discussed in chapter two.

Across three scenarios the mean number (MN) considering the legislation was 74% (MN=20), for going on to utilise it the number was 45% (MN=12). These results bring to bear the issue highlighted with mixed methods in chapter three, the qualitative and quantitative data do not appear to agree (Cresswell, 2006:66). More than double the number (MN=12) utilised the legislation in the scenarios than applied it in real life DC investigations (N=6). There are possible reasons for this discrepancy. One could be the questionnaires focus on ML may have tuned participants in to considering the application of the legislation more carefully. As such the scenario data cannot be seen as a completely accurate representation of how ML is utilised. There is also a consideration that the discrepancy is not as great as first thought. Both figures represented less than half of the sample and allow for the interpretation that ML is not applied to DC frequently.

4.4 Perceptions on whether the legislation should feature in DC investigations (CRQ2)

Analysis in respect of CRQ2 focused on the qualitative data provided in the scenario questions. Data from the questions on barriers to usage and words associated with ML was also utilised. The scenarios were designed to reflect DC situations and sought to explore the broad definition of criminal property (POCA, 2002) outlined in chapter two. The idea of data being property was prominent in the scenario questions. Explanation for this exploration of data as criminal property is outlined in chapter two. The consequences of this decision are evident in the themes identified in the sample data.

A prominent theme throughout was an inconsistent perception of what constitutes criminal property. It was possible to interpret this as a result of the research design. The scenario questions were broken down into three parts. Firstly, participants identified if ML legislation could be considered. After this they quantified what was criminal property and finally, they highlighted if they would utilise the legislation. Qualitative data was sought for each of these questions, as a result an in-depth insight into the participants rationale was captured. This revealed that across a scenario the sample often answered the three questions in a contradictory fashion.

In scenario one, 42% (N=12) did not believe money laundering could be considered. The main reason provided for this was a lack of overt financial benefit being identified by participants. This rationale could be interpreted as participants

equating criminal property with overt financial benefit articles such as cash. If this interpretation was accurate it would be logical to expect the same 42% (N=12) of the sample to have not identified any criminal property. The data does not however corroborate this interpretation. When asked in the second part of scenario one to identify what represented criminal property, the overwhelming majority, 82% (N=23), identified data. This was not where the inconsistencies ended, in spite of the majority identifying a ML offence by detailing data as criminal property, only 39% (N=11) stated they would utilise ML offences.

It is not possible to fully clarify why these inconsistencies occur. Further data collection would have been needed on participants definition of criminal property. Not seeking this is a limitation of the research design and would be something to explore in future research. Despite this limitation insight into these results can be potentially found in chapter two. The literature identifies that an environment of confusion exists in respect of ML offences (Murray, 2016:447). Further to this the general approach of LE to POCA is highlighted as inconsistent with varying applications of the law (Sittlington and Harvey, 2018:1; House of Commons, 2016:31). The inability of LE to effectively utilise the legislation is seen to be caused by a limited knowledge base in respect of ML (Murray, 2016:447).

Evidence that the inconsistencies outlined by the sample are not confined to DC can be seen in further analysis of the data. Several participants identified as having FI backgrounds, being accredited FIs, Financial Intelligence Officers or deployed on a fraud investigation unit. Given this background in POCA legislation, it is possible to argue that the responses provided by this group would be fairly consistent. This argument was found to be flawed when the data from these participants was scrutinised. Though some agreed on criminal property being present and the use of ML offences, others did not. Several did not consider ML offences applicable for any of the scenarios. If inconsistencies are present in responses from those with FI training, the data provides some support for literature identified in chapter two. Research by Chave (2017: 437) outlined that LE training in POCA is limited and inadequate. This has implications for CRQ3. Any perceived advantages identified by DC investigators may be flawed if the training is inadequate. Exploration of how adequate FI training currently is was beyond the scope of this research. It does however appear that it could be a worthwhile subject for future research.

Sample participants experience in FI and the barriers they perceived to utilising ML legislation, highlighted several significant findings. One quarter of participants detailed a limited experience in FI and subsequent lack of knowledge. This was also a theme in the barriers to utilising the legislation. Over half the sample, 57% (N=16), felt a lack of knowledge inhibited their application of ML offences. The lack of knowledge was perceived as not just indicative of DC investigators, but the criminal justice system as a whole. Several references are made to CPS lacking the requisite knowledge and not wanting to charge ML offences. This provides some corroboration for the argument made in chapter two that the actions of CPS could be negatively affecting utilisation of ML offences. Both the literature (Fitzpatrick 2017: 449, Gale and Kelly, 2018:31) and the sample data highlight concerns over the ability of CPS to support charges for ML offences.

Limited access to FIs as a barrier to utilising ML offences, is a prominent theme within the sample data. This provides some corroboration for the consideration in chapter two that separate FI and DC units could be detrimental to ML application. For example, one response outlined "*the ability to freely use ML offences in the NCA was limited"* to do so *"required the sign off from a separate FI department"* (G24). This could be seen as restricting DC investigators ability to effectively challenge criminality. Literature identified in chapter two highlighted that rigid organisational structures could negatively impact problem solving (Brown and Sutton, 1997:22). Limited access to FIs may provide corroboration for this finding.

No explanation was provided in the data collected for why access to FIs was limited. It was not known that this would arise as a theme so therefore was not factored into the research methodology. The literature identified in chapter two offers some possible insights. One limitation to how LE approach POCA is detailed as a failure to recognise the changing face of criminality (Chave 2017: 437). This may be why LE have not recognised the potential benefits of applying the legislation to DC. The data gathered in this study offers some evidence to support this. Responses from the sample identified a failure by senior officers to recognise POCA opportunities (DS13) and a lack *"of awareness of POCA legislation for digital investigators*" (DCon10).

The perceptions of some participants appear to have been affected by negative experiences of utilising FI. One participant stated that in their experience ML investigations grew in size quickly and *"become disproportionate to the original offence leading to cases being closed."* (DS5). These negative perceptions appear deep rooted in some participants. It was outlined that proactive financial investigations were virtually unheard of *"due to a lack of interest in the development of financial intelligence pictures" (PC22).* Investigations which did take place were slow and cumbersome (PC22). ML was *"difficult to investigate, overwhelming to law enforcement" (IO15)* and "*Prevelant, Boring, Protracted" (DCon17).* These negative perceptions appear to go beyond DC investigators, one study details that FIs themselves feel financial investigation is used ineffectively (Gale and Kelly, 2014:30). One potential reason for these negative feelings is that FI does not appear to be core to LE investigative practice (Wood, 2017). This could lead to a misunderstanding of its possibilities (Gale and Kelly, 2014:30).

The themes identified thus far in this section suggest DC investigators have a negative perception in respect of utilising ML. There is though a prominent theme in the data which strongly suggests DC investigators perceive ML should feature. This theme focuses on virtual currencies (VC) perceived link to both financial and digital investigation (for a full explanation of VC please see European Parliament document (2018)). Across the questionnaire there were 24 references to VC. Broken down this was made up of 9 participants associating it with ML, 6 referencing it in application examples, 1 in both knowledge of financial and digital investigation, 5 in barriers to utilising ML and 2 in why FI training would be beneficial. With no single concentration of answers its possible to interpret the theme as being a broad and consistent concern for DC investigators. Referencing it in the context of ML also allows for the argument that DC investigators link the subject to FI. The potential conclusion being that DC investigators do perceive ML

should feature in their investigations. Whilst this could be the case there are some points which need further examination.

The threat of criminality utilising VC is believed by the researcher to be an important consideration. Interpreting the qualitative data as outlined above allows for the assertion that the threat is perceived to be substantial. If accurate then a possible argument is that the perception is based on participants regular exposure to VC in investigations. In this study participants were not asked to identify how regular the experience had been, to gain some insight inferences had to be drawn from other questions. The sample data on utilising ML legislation was one source which was used to corroborate if VC were being dealt with on a regular basis. This identified 14% (N=4) of the whole sample had utilised ML legislation in a DC investigation where VC had been a factor. The examples in respect of convictions were analysed, none of these referenced VC. The sample is too small to be fully representative of DC investigators as a whole, however the limited usage and no conviction examples suggest that VC may not be as significant a risk as perceived. If accurate then it is possible to argue that concentrating ML considerations on the low risk posed by VC is flawed. It may even be inhibiting innovative thinking around applying ML legislation to DC investigations, for example the concept of data as criminal property detailed in chapter two.

Studies into the criminal threat posed by VC provide some corroboration for the risk being low. The UK national risk assessment (NCA, 2017:38) on ML concluded there was little evidence of VC being used as a tool for ML. As a result, the risk from VC was categorised as low. Specific to DC estimates suggest only around 4% of money laundered is in Bitcoin or other cryptocurrency (Maguire, 2018: 19). Between 2013 – 2016 separate research identified only 1% of Bitcoin transactions as being criminal in nature (Fanuasie and Robinson, 2018). Focusing on Bitcoin is appropriate as it is the dominant VC and is seen as "*the gold standard*" (Recorded Futures, 2018) in DC accepted by the greatest number of services (Foley et al., 2018:6).

Reviewing the number of overall transactions on the Bitcoin blockchain and utilising the 4% figure allows a very rough estimate of how many transactions are linked to DC. Over a 24-hour period from the 13th to the 14th September 2018 there were 225,537 transactions globally (Blockchain, 2018). This means that during the 24-hour period referenced, there were an estimated 9,021 DC related transactions globally. Narrowing this down to the UK is very difficult as the available evidence on the subject is limited, there is one report which details that 11% of overall bitcoin transactions are UK based (Totalcrypto, 2018). Employing this figure of 11% against the DC related transaction gives 992 UK based DC related transactions.

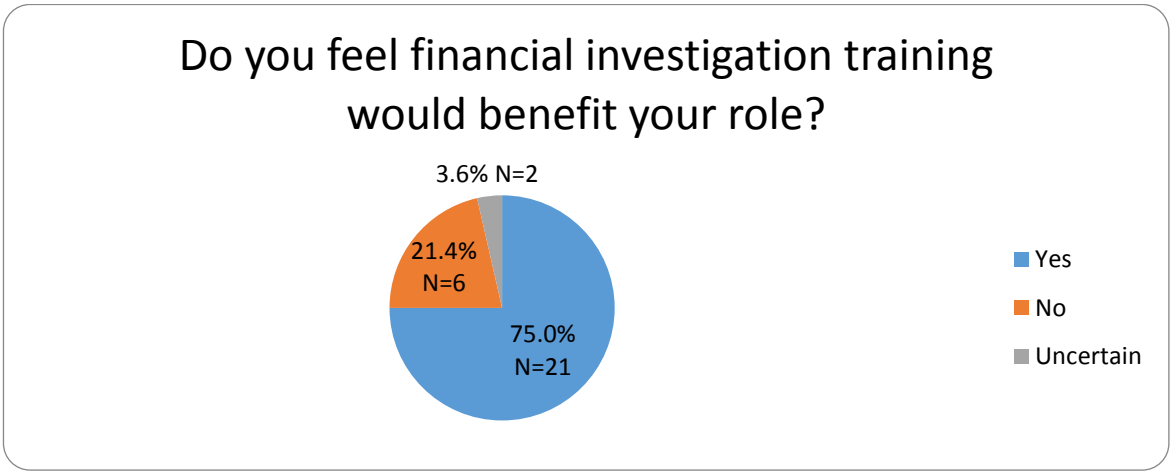
To put this into perspective we can use physical cash as a comparison. This is seen as high risk in the UK national risk assessment due to its inherent anonymity (NCA, 2017:65). In 2017 13.1billion transactions in the UK were carried out in cash (Koellwe, 2017). No evidence of how many transactions related to DC were identified. It is important to note that research findings identify cash as an important part of DC (Van Wegberg et al, 2018: 420). Therefore, the comparison can be argued to be relevant. The 4% principle highlighted above will be applied for this comparison. It is acknowledged that this is not based on direct evidence, but given

the lack of literature it seems appropriate to consider that a mechanism deemed "high risk" (NCA, 2017) and an "important part" of DC, would be used at least as often as Bitcoin. The result shows that an estimated 1.4 million transactions a day in the UK are potentially associated with DC. Analysing this comparison, it is possible to argue that cash poses the greater threat in DC.

There is a need to consider how VC affects criminality as some literature argues that the overall number of criminal bitcoin transactions is substantial (Van Wegberg et al, 2018: 420; Foley et al., 2018:1). From a DC point of view though, the evidence identified does not corroborate the samples strong focus on VC being the link between DC and ML. The reason for this strong focus was not explored in the questionnaire. Negative press on VC may have affected perceptions, for example its use on dark net markets (Foley et al., 2018:1). To really gain insight though further research would be worthwhile.

4.5 Perceptions on FI Training (CRQ3)

Utilising mixed methods greatly aided insight into this CRQ. This was a result of the qualitative and quantitative data agreeing with each other (Creswell, 2006:7). As a result, a greater depth of data was available to provide insight into CRQ3. The qualitative data provided a strong argument to state that DC investigators perceived FI training would benefit their role. Table 2 below identifies that three quarters (N=21) of the sample identified the training would be beneficial.



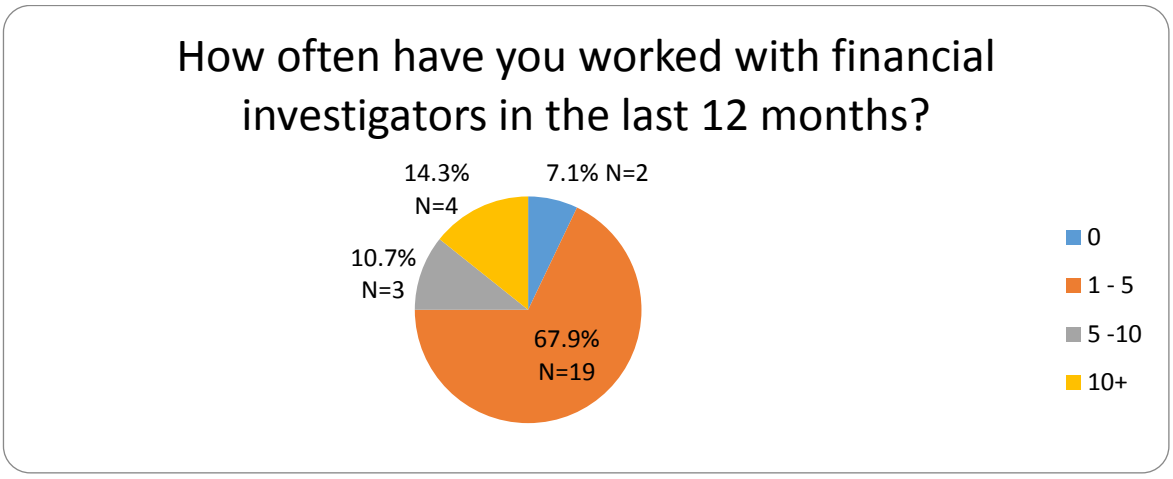
Several prominent contextual themes emerge from the qualitative responses to support the descriptive statistics. Approximately a third (N=9) identify that DC is predominantly financially motivated agreeing with literature identified in chapter two. In a response very similar to that identified in the literature (Bryant, 2008:87) one participant outlines *"the motivation of cyber criminals is increasingly, and now overwhelmingly focused on profit. The days of mischief hacking are gone"* (DCon01). It is possible to interpret another third (N=9) of responses find a direct connection between financial and digital investigation, for example DCon04 stated FI was "*directly linked to a number of our investigations*." and DCon08 detailed FI was a "*complimentary skillset*". Those stating it would not benefit them largely

identified that their knowledge was sufficient (PC07, DS12). These perceptions may not be representative of the sample. As referenced earlier in this section lack of knowledge on FI is a prominent theme throughout the data. It is important to note that some participants saw FI as distinct from DC investigation. As a result, they did not believe FI training was beneficial. In a slight contradiction such perceptions highlighted that they just needed *"an understanding of the issues and legislation"* (DI27). By outlining this need it is possible to argue that FI training would be beneficial despite the perception to the contrary.

Another theme arising from the data was a perception that FI training would improve efficiency in DC investigations. It was detailed that currently there was a reliance on FIs to "*access specific investigative routes and databases*" (IO15). Other responses corroborated this highlighting that every time FI skills were needed the work had to be handed on (DCon18). The findings suggest that LE see the world in fragments corresponding to organisational siloes. In this instance financial investigation skillsets have not been provided to DC investigators as that responsibility lies in another organisational silo. Thus, one possible interpretation of the data is DC has not been viewed objectively by LE undermining its ability to apply appropriate skillsets in response.

Research does suggest there are alternatives to providing FI training to DC investigators. Locating FIs with the investigative teams they assist raises awareness and understanding of financial investigation. It also prevents FIs from being isolated from the organisations within which they worked (Gale and Kelly, 2018:29). This could go some way towards positively affecting perceptions on FI. The sample were not however asked about how this approach would affect their perception in respect of CRQ3. The researchers bias in this matter may have impacted this decision. In believing FI training to be beneficial other approaches were not considered. As a result, further research on this would be beneficial for further insight into CRQ 3.

The current usage of FIs was thought to be a good insight into whether DC investigators would use the training if available. The results are detailed below in Table 3:



A design flaw outlined earlier in this chapter also affected this question. The exact number of interactions was not asked for. As a result, analysis is restricted to an estimate based on the minimum number of interactions. The minimum figure is 74 with only two participants detailing no interactions. As outlined in the methodology although small the sample could be seen as logically representative of the target population (Lavrakas, 2008: 645). Considering the sample as being logically representative, and that LE provide a year-round response, a rough estimation outlines that FIs are used at least once a week (365/74=4.93) in DC investigations. The findings outlined earlier in this chapter on limited access to FIs, make it possible to argue that usage would be higher if the skillset was more accessible. Taking these two points into consideration the data could be interpreted as FIs play a significant role in DC investigations. As a result, the data may corroborate that DC investigators would utilise FI training on a consistent basis.

4.6 Conclusion

The evidence in respect of CRQ1 indicates that ML legislation is utilised by DC investigators. Predominantly this usage appears to relate to cyber enabled crime with limited application identified in respect of cyber dependant offences. The data did highlight a potential misinterpretation of the definition of DC. The findings are still accurate though as the qualitative data analysis allowed for the identification of misinterpretations. Reasons were considered for the misinterpretation but none are obvious as the research design factored in a clear definition of DC. The findings highlighting DC investigators limited utilisation of ML legislation, are the first contribution to the subject matter the researcher could find. As such they help to fill the gap in the literature identified in chapter two.

In CRQ2 the data indicates that DC investigators may be encountering significant barriers to utilising ML legislation. In spite of this the themes emerging identify a wish by investigators to overcome the barriers. For example, building a better knowledge base to make the legislation more accessible. Greater access to financial investigators is also prominent in the data. Significant evidence is present to argue that DC investigators perceive ML legislation should feature in investigations involving VC. No literature was found in chapter two directly referencing DC investigators perceptions of ML. The findings outlined therefore adds to the literature on the subject by helping to fill this gap. They also provide supporting evidence for some of the literature identified in chapter two. In particular the conclusion outlining that across the board LE training in POCA is limited and inadequate Chave (2017: 437).

The data collected on CRQ3 validated the research design decision in respect of mixed methods. As a result, it was possible to make a strong argument that DC investigators did feel they should be trained as financial investigators. This finding provides potential confirmation for the literature in chapter two stating that financial and digital skillsets should be combined (McGuire, 2018: 121). Participants perceptions of the drawbacks of not having the combined skillset offered further support for this finding. Utilising a mix of closed, open and scenario-based questions, as outlined in chapter three, is believed to have allowed for a depth of data which minimised researcher bias potentially distorting findings and analysis (Henn et al., 2013). The depth of data achieved can be seen in participants

providing full and appropriate answers to questions. It is believed that the research decision not to ask any questions likely to be perceived as sensitive or embarrassing was a contributing factor in this.

This is the first study, as far as the researcher is aware, that has attempted to fill the gaps in the literature identified. The findings, though on a small-scale, do offer new and novel insight into the perceptions of DC investigators in regards to ML legislation. The use of questionnaires has provided data of value in this research. In spite of this it is acknowledged that the need to minimise the number of questions asked (Denscombe, 2014: 172) can inhibit analysis and insight. As such future researchers may wish to consider further exploration of the subject through interviews.

Chapter Five:
Conclusion

The main focus of this study was to critically analyse the perceptions of DC investigators in regards to ML legislation. Mixed methods were utilised to explore and address the CRQs:

1. Do digital investigators utilise POCA legislation relating to money laundering? (CRQ 1)

2. Do digital investigators perceive the legislation should feature in DC investigations? (CRQ 2)

3. Do digital investigators feel they should be trained in financial investigation? (CRQ 3)

As far as the researcher is aware this is the only study that has produced empirical data concerning DC investigators perceptions of ML legislation. As a result, this study adds new and novel data to the existing literature. It is however important to note though this study is not without limitations.

Reflecting on the research design several participant questions did not yield data directly specific to CRQs. As identified in chapter four there were a number of occasions where further questions on a subject would have provided more precise analysis. Those questions not directly contributing to the CRQs should have been eliminated and more pertinent questions inserted. The definition of DC also caused some misinterpretation of certain questions. The research design ensured a clear definition was provided, as such it is not felt it was possible to have foreseen this issue. Misconceptions were mitigated by the analysis of follow up questions so it is not believed they distorted the findings.

The main focal points for analysis were the CRQs outlined above. The findings in respect of CRQ1 identified that utilisation of ML is arguably minimal when going by a strict DC definition. One potential reason for this and the response inconsistencies identified in chapter four, is many participants self-identified lack of knowledge on ML. This provides some confirmation for literature arguing that inconsistent approaches to POCA are negatively impacting its utilisation (Sittlington and Harvey, 2018:1; House of Commons, 2016:31). The findings could be seen to add to the secondary data identifying a failure within the criminal justice system, to provide an effective response to the proceeds of crime (Fitzpatrick, 2017: 449; Chave, 2017: 437). Further confirmation of this literature is provided by the studies finding that CPS were perceived to be a barrier to utilising ML legislation.

Greater insight into CRQ1 could have been gained through follow up interviews. These would have been beneficial in clearing up any misconceptions and asking the questions highlighted in chapter four. In respect of CRQ1, the use of mixed methods was undermined by the misinterpretation of DC. Despite this the analysis carried out is believed to have assisted in at least partly answering CRQ1.

The findings for CRQ2 brought out a number of important themes. Perceptions appear to have been impacted by negative experiences with FI. It was highlighted in some responses to be overwhelming and difficult to investigate. This potentially confirms the literature identifying that LE need to upgrade investigation skills if they are to utilise ML offences effectively (Chave, 2017: 437; Murray, 2016: 447). There was however evidence in the data that ML legislation should feature in DC investigations. Only 18% (N=5) of the sample did not consider ML in any of the scenarios. Close to half of the sample for each scenario also outlined ML offences as being applicable.

As outlined in chapter four particular emphasis was placed on VC and their connection to DC. This was a strong theme identifying that the sample perceived ML legislation did apply to DC. Research into this perception casts doubt on VC being the main driver for applying ML legislation to DC (NCA, 2017:38). Focusing on VC could be inhibiting thought processes around how to implement ML in DC. As an example, in chapter two data was identified as a major driver for criminal profits in respect of DC. This evidence could be seen as identifying that data, not VC, should currently be considered as the prominent link between DC and ML legislation.

As outlined above the sample did perceive that ML legislation applied to DC. What was however clear in the data was a confusion on how it applied. This is most apparent in participants often contradictory identification of criminal property. The emergence of this issue around the concept of criminal property was not expected and not catered for in the research design. Follow up interviews to clarify answers would have assisted in providing more data to give greater analysis on the theme. No other research could be identified on the perceptions of ML in DC, as such the findings for CRQ2 provide new and novel data on the subject.

The inclusion of mixed methods in the research design was validated in the findings for CRQ3. The correlation of quantitative and qualitative data highlighted strong evidence to suggest DC investigators see value in FI training. Three quarters confirmed they would benefit from such training and provided details of the investigative inefficiencies arising from not being FI trained. Such strong evidence confirms the literature outlining that a holistic approach, such as joint financial and digital skillsets, is required to fully understand the challenge of DC (McGuire, 2018: 121; McDowell et al, 2015:4). The limited literature identified on this subject utilised secondary data, as such it is believed that this is the first study to gather primary data which means the findings offer new and novel insights on the subject.

The research design decision to utilise scenario questions (Brush and Saye, 2008:7) is believed by the researcher to have greatly aided insight into the CRQs. By giving participants a situation in which they could choose if ML legislation was appropriate, more data was generated on the nuances of participants perceptions. For example, in scenario one the overwhelming majority (N=23) considered data could fit the criminal property definition. This corroborated the literature highlighting the value of data (Feijóo et al., 2017: 248) and challenged that which only focused on overt financial mechanisms in ML offences (Ramage (2012: 279).

This subject area would benefit from further research in the future. This project was only on small scale, though unsuccessful efforts were made to attract a larger sample. Given this the results need CDM by projects with a larger sample to be considered generalizable to all DC investigators across England and Wales.

5.1 Recommendations

The recommendations below are grounded in the data produced by this research. This is in line with the research design which identified that elements of grounded theory would be utilised.

Numerous sources in the literature identify that the motivation for DC is financial and thus financial strategies are required to tackle this (McGuire, 2018; Goldman and McCoy, 2016:595; Bryant 2008:87). The research findings highlighted numerous barriers to DC investigators utilising financial strategies. Two significant themes were rigid organisational structures restricting access to accredited FIs, and a lack of knowledge on POCA legislation by DC investigators.

To overcome these barriers the first move could be to accept within LE the findings that DC is financially motivated. It could be argued that this is not currently the case as the DC training roadmap focuses only on digital elements (NPCC, 2015:30). By accepting the findings, the focus could be changed to consider how best to tackle both the digital and financial elements of DC. This could potentially lead to a commitment to increase DC investigators knowledge of POCA legislation. By doing this the utilisation of ML by DC investigators might increase. If this led to a more effective response to DC, LE could be seen as a more capable guardian in this area. Going by the RAT principles (Cohen and Felson, 1979) outlined in chapter two, this could reduce the number of motivated offenders and thus result in fewer instances of DC.

There are several further points which would need to be considered in respect of the above. Firstly, the lack of knowledge around POCA is not restricted to DC investigators. As outlined in the project findings and literature CPS are also struggling with the concept. Any improvement in LE capabilities would be undermined if CPS are not part of any increase in knowledge on the subject.

Restricting DC investigators access to accredited FIs also needs to be resolved. Several participants identified that they could not complete enquiries which could only be done by accredited FIs. The decision to be made in respect of this appears to be one of two choices. Firstly, improve the accessibility DC investigators have to those suitably qualified. Alternatively provide DC units with their own capability through accredited FI training. Whether this requires every DC investigator to be an accredited FI was beyond the scope of the research. It would however be an interesting topic for future research.

References

Action Fraud (2018). *Cyber Profile October 2017 – March 2018* [pdf] London: Action Fraud (Unpublished in public domain) [Accessed 3rd Jun. 2018].

Adamson, S. (2005). Burglary Reduction in Action: The Hartlepool Experience. Crime Prevention and Community Safety, 7(2), pp.41-52. Available at http://dx.doi.org/10.1057/palgrave.cpcs.8140217http://dx.doi.org/10.1057/palgrave.cpcs.8140217 [Accessed 28th August 2018]

Anand, P. (2015). *18 most popular things fraudsters buy with your credit card.* Available at: https://www.marketwatch.com/story/18-most-popular-things-fraudsters-buy-with-your-credit-card-2015-11-24 [Accessed 3 Jun. 2018].

Andrews, T. (2012). What is Social Constructionism? *Grounded Theory Review*. Vol. 11(1). pp.39-46. Available at http://groundedtheoryreview.com/2012/06/01/what-is-social-constructionism/ [Accessed 20th August 2018]

Armacost, R. L., Hosseinio, J. C., Morris, S. A., & Rehbein, K. A. (2012). An empirical comparison of direct questioning, scenario, and random response methods for obtaining sensitive business information. *Decision Sciences, 22(5),* pp.1073-1090 Available at http://dx.doi.org/10.1111/j.1540-5915.1991.tb01907.x [Accessed: 17 October 2018].

Barrett, M., Garrety, K., & Seberry, J. (2006). *ICT professionals' perceptions of responsibility for breaches of computer security.* [pdf] Australia: Proceedings of the Australian and New Zealand Academy of Management Conference. Available at https://ro.uow.edu.au/cgi/viewcontent.cgi?referer=http://scholar.google.co.uk/&httpsredir=1&article=1382&context=infopapers [Accessed 5th November 2018]

BBC News. (2018). *Hacker jailed for cyber crime offences*. Available at: http://www.bbc.co.uk/news/uk-england-42733638 [Accessed 22 May 2018].

Becker, G., & Bakal, D. (1970). Subject anonymity and motivational distortion in self-report data. *Journal of Clinical Psychology, 26,* pp.207-209. Available at: https://doi.org/10.1002/1097-4679(197004)26:2%3C207::AID-JCLP2270260224%3E3.0.CO;2-6 [Accessed 25th September 2018]

Birmingham City University (BCU), (2011). How to Write References. [pdf] Birmingham: BCU. Available at: http://library.bcu.ac.uk/references.pdf [Accessed 15 Dec. 2017]

Blakeborough, L. and Correia, S. (2017). *The scale and nature of fraud: a review of the evidence*. [pdf] London: Home Office, p.4. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/720772/scale-and-nature-of-fraud-review-of-evidence.pdf [Accessed 9 Sep. 2018].

Blockchain.com. (2018). *Bitcoin Charts & Graphs - Blockchain.* Available at: https://www.blockchain.com/en/charts [Accessed 15 Sep. 2018].

Bradburn, N., Sudman, S., Blair, E., & Stocking, C. (1978). Question threat and response bias. *Public Opinion Quarterly, 42(2),* p221-234. Available at: https://academic.oup.com/poq/article-pdf/42/2/221/5290267/42-2-221.pdf [Accessed 25th September 2018]

Bronitt S., Stenning P., (2011) Understanding discretion in modern policing, *Criminal Law Journal.* pp320 Available at https://research-repository.griffith.edu.au/handle/10072/44249 [Accessed 17th September 2018]

Brown M. and Sutton A., (1997) "Problem Oriented Policing and Organisational Form: Lessons from a Victorian Experiment," *Current Issues in Criminal Justice* vol. 9, no. 1 p. 21-33. Available at http://classic.austlii.edu.au/au/journals/CICrimJust/1997/11.pdf [Accessed on 26 Jun. 2018]

Brush, T., & Saye, J. (2008). *How do preservice social studies teachers implement problem-based historical inquiry strategies: A scenario-based survey study.* [pdf] Annual conference of the American Educational Research Association*,* New York, United States of America 5th – 9th April 2008. Available at: https://www.researchgate.net/profile/Thomas_Brush2/publication/254061919_How_Do_Pre-service_Social_Studies_Teachers_Implement_Problem-based_Historical_Inquiry_Strategies_-_A_Scenario-based_Survey_Study/links/570638d108ae0f37fee15b12/How-Do-Pre-service-Social-Studies-Teachers-Implement-Problem-based-Historical-Inquiry-Strategies-A-Scenario-based-Survey-Study.pdf [Accessed 30th October 2018]

Bryant, R. (2008). *Investigating digital crime.* Chichester: J. Wiley & Sons. [Accessed 9 Dec. 2017]

Bryman A. (2015) *Social Research methods*, Oxford: Oxford University Press [Accessed 23rd September 2018]

Bryman, A. (2016) 4th edn. *Social Research Methods*. Oxford: Oxford University Press. pp.192 [Accessed 13 Jan. 2018]

Bryman, A. and Bell, E., (2003) *Breaking down the quantitative/qualitative divide. Business Research Methods*, Oxford: Oxford University Press pp.465-478. [Accessed 21st September 2018]

Bullock, K. (2014). Criminal benefit, the confiscation order and the post-conviction confiscation regime. *Crime, Law and Social Change*, 62(1), pp.45-64. Available at: http://dx.doi.org/10.1007/s10611-014-9517-7 [Accessed 18 Nov. 2017].

Button, M., Shepherd, D. and Blackbourn, D. (2016). *The Fraud 'Justice Systems': A Scoping Study on the Civil, Regulatory and Private Paths to 'Justice' for Fraudsters*. [pdf] Portsmouth: University of Portsmouth Centre for Counter Fraud Studies, pp.8,70,76. Available at: http://www2.port.ac.uk/media/contacts-and-departments/icjs/ccfs/Fraud-Justice-Systems-2016---Final-Report.pdf [Accessed 9 Sep. 2018].

Cabinet Office (2011). *The UK Cyber Security Strategy*. Available at: https://www.gov.uk/government/publications/cyber-security-strategy [Accessed 19 May 2018].

Callanan, G. & Perri, D. (2006). Teaching conflict management using a scenario-based approach. *The Journal of Education for Business, 81(3),* pp.131-139. Available at https://doi.org/10.3200/JOEB.81.3.131-139 [Accessed 30th October 2018]

Capeller, W. (2001). Not Such a Neat Net: Some Comments on Virtual Criminality. *Social & Legal Studies,* 10(2), pp.229-242. Available at https://doi.org/10.1177/a017404 [Accessed 22 Oct. 2018].

Carey, S. (2018). *Investigatory Powers Act: What you need to know.* Available at: https://www.computerworlduk.com/security/draft-investigatory-powers-bill-what-you-need-know-3629116/ [Accessed 7th Jun. 2018].

Charmaz K (2000:515) "Grounded Theory: Objectivist and Constructivist Methods" in N.K. Denzin and Y.S. Lincoln (Eds.), *Handbook of Qualitative Research*, 2nd Edn. Thousand Oaks, CA:Sage publications [Accessed 20 Oct. 2018].
Chave, D (2017). Proceeds of crime training: bringing it up to date, *Journal of Financial Crime,* Vol. 24 Issue: 3, pp.437-448, https://doi.org/10.1108/JFC-04-2017-0028 [Accessed 18 Nov. 2017].

Chávez, T. G. G. (2012) *Perspectives on community policing: a social constructivist and comparative analysis*, Ph.D Thesis. University of Birmingham. Available at: http://etheses.bham.ac.uk/3459/ [Accessed 20th August 2018]

Cockcroft, TW and Trevorrow, PA and Shan-A-Khuda, M and Schreuders, ZC (2018) Police Cybercrime Training: Perceptions, Pedagogy and Policy*. Policing: A Journal of Policy and Practice,* Available at https://doi.org/10.1093/police/pay078 [Accessed 7th September 2018]

Cohen, L. and Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, 44(4), pp.588 - 608. Available at https://www.jstor.org/stable/2094589 [Accessed 22 Oct. 2018].

Coinmarketcap.com. (2018). *Global Charts* | *CoinMarketCap.* Available at: https://coinmarketcap.com/charts/ [Accessed 15 Sep. 2018].

College of Policing (2017), *Crime Reduction Research,* Available at: http://whatworks.college.police.uk/Pages/default.aspx [Accessed 13 Jan. 2018]

College of Policing (2018) *Police Officer*. Available at: http://recruit.college.police.uk/Officer/Pages/default.aspx [Accessed 1st August 2018]

College of Policing (2018) *What is evidence-based policing?"* Available at http://whatworks.college.police.uk/About/Pages/What-is-EBP.aspx [Accessed 21st September 2018]

Computer Misuse Act 1990 c.18. London: The Stationery Office. [Accessed 10 Dec. 2017].

Cooper, B., Shepardson, D., & Harbor, J. (2002). Assessments as teaching and research tools in an environmental problem-solving program for in-service teachers. *Journal of Geoscience Education, 50(1),* 64-71. Available at: http://dx.doi.org/10.5408/1089-9995-50.1.64 [Accessed 5th November 2018]

Cooper, J., Lewis, R., & Urquhart, C. (2004). Using participant or non-participant observation to explain information behaviour. *Information Research*, 9(4). Available at http://www.informationr.net/ir/9-4/paper184.html. [Accessed 10th November 2018]

Corbin, J., and Strauss, A. (2008) *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. 3rd edn. London: Sage Publications Ltd.

Council of Europe (1950), Article 8, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950 [Accessed 13 April 2018]

Crawford, S.D., Couper, M.P., and Lamias, M.J. (2001), Web Surveys: Perceptions of Burden, *Social Science Computer Review*. 19(2) pp.146-162 Available at http://dx.doi.org/10.1177/089443930101900202 [Accessed 18th August 2018]

Creswell, J. (2006). *A concise introduction to mixed methods research*. California: Sage Publications, p.7. [Accessed 10th October 2018]

Crooks DL (2001) The importance of symbolic interaction in grounded theory research on women's health, *Health Care for Women International*, *22:1-2*, pp.11-27, Available at http://dx.doi.org /10.1080/073993301300003054 [Accessed 9th August 2018].

Crow, I. Semmens, N. (2008), *Researching Criminology.* Maidenhead: Open University Press. [Accessed 13 Jan. 2018]

Crown Prosecution Service (2017), *Hacker who targeted US military systems receives suspended prison sentence.* Available at: http://www.cps.gov.uk/news/latest_news/hacker-who-targeted-us-military-sys/index.html [Accessed 9 Dec. 2017].

Crown Prosecution Service (2017). *'Money mules' in a nationwide scam sentenced* | *The Crown Prosecution Service.* Available at: https://www.cps.gov.uk/mersey-cheshire/news/money-mules-nationwide-scam-sentenced [Accessed 22 May 2018].

Crown Prosecution Service (2017). *Proceeds of Crime Act Money Laundering Offences: Legal Guidance*, Available at: http://www.cps.gov.uk/legal/p_to_r/proceeds_of_crime_money_laundering/ [Accessed 13 Dec. 2017].

Crown Prosecution Service (2018). *Cybercrime - prosecution guidance* | *The Crown Prosecution Service.* Available at: https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance [Accessed 29 Sep. 2018].

CryptoSlate. (2018). *DEA: Criminal Activity Drops 80 Percent in Bitcoin Transactions*. Available at: https://cryptoslate.com/dea-criminal-activity-drops-80-percent-in-bitcoin-transactions/ [Accessed 15 Sep. 2018].

Curtis, B. & Curtis, C. (2011), *Social Research : A practical Introduction.* Los Angeles: London. Sage Publications. [Accessed 13 Jan. 2018]

Data Protection Act 1998 c.29 London: The Stationary Office [Accessed 10 Dec. 2017]

Data Protection Act 2018. London: The Stationary Office. Available at: http://www.legislation.gov.uk/ukpga/1998/29/contents [Accessed: 17 October 2018].

Dell SecureWorks (2015). *The Next Generation of Cybercrime: How it's evolved, where it's going.* [pdf]. Available at: http://www.allstream.com/wp-content/uploads/2015/11/white-paper-cybercrime.pdf pp.2, 3 [Accessed 8 Oct. 2018].

Denscombe, M. (2014). *The Good Research Guide: For small scale research projects*. 5th ed. Milton Keynes: Open University Press. [Accessed 13 Jan. 2018]

Eastern Region Special Operations Unit (2017). *About Us - Eastern Region Special Operations Unit - ERSOU ROCU*. Available at: https://www.ersourocu.org.uk/about.aspx [Accessed 20 Oct. 2018].

Edwards, R. and Holland, J. (2013). *What is qualitative interviewing?.* 1st ed.

London: Bloomsbury Academic, p.66. [Accessed 5th September 2018]

Europol (2014). *The Internet Organised Crime Threat Assessment*. [pdf] The Hague: Europol, pp.9. Available at: https://www.europol.europa.eu/sites/default/files/documents/europol_iocta_web.pdf [Accessed 25 Jun. 2018].

Fahmy, D. (2010). *Crooks Love Shopping at Best Buy, Target.* Available at: https://abcnews.go.com/Business/credit-card-theft-crooks-shop-best-buy-target/story?id=9931006 [Accessed 3 Jun. 2018].

Feijóo, C., Gómez-Barroso, J. and Voigt, P. (2014). Exploring the economic value of personal information from firms' financial statements. *International Journal of Information Management*, 34(2), pp.248-256. Available at https://doi.org/10.1016/j.ijinfomgt.2013.12.005 [Accessed 13 Jan. 2018]

European Parliament (2018) *Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion* [pdf] Brussels: European Parliament. Available at: http://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf [Accessed 15 Sep. 2018].

Financial Times (2016). *Overseas requests soar for UK help with cyber crime*. Available at: https://www.ft.com/content/257b599a-3a2f-11e7-821a-6027b8a20f23 [Accessed 15 May 2018].

Firebrand (2017) BBC report on Firebrand's police force cyber crime training. *Firebrand*. [blog] 12 May. Available at: http://blog.firebrandtraining.co.uk/2017/05/bbc-cybercrime.html [Accessed 17 Oct. 2018].

Firebrand (2017), *Cyber Investigator Course Phase One and Two*, Available at http://www.firebrandtraining.co.uk/courses [Accessed 13th Jan. 2018]

Fitzpatrick, D. (2017). A "think piece" on intelligence, investigation and prosecution. *Journal of Financial Crime*, 24(3), pp.449-460. Available at https://doi.org/10.1108/JFC-03-2017-0018 [Accessed 13 Jan. 2018]

Foley, S., Karlsen, J., Putnins R., Talis J., Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies? *SSRN Electronic Journal,* Available at SSRN: https://ssrn.com/abstract=3102645 or http://dx.doi.org/10.2139/ssrn.3102645 [Accessed 29th September 2018]

Gale E. and Kelly J. (2018), *Exploring the Role of the Financial Investigator Report Home Office Research Report 104* [pdf] Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/753212/exploring-the-role-of-the-financial-investigator-report-horr104.pdf [Accessed 8 Oct. 2018].

Gemalto (2018). 2017 The Year of Internal Threats and Accidental Data Breaches report. *Gemalto Enterprise Security* [blog] 13th April. Available at: https://blog.gemalto.com/security/2018/04/13/data-breach-stats-for-2017-full-year-results-are-in/ [Accessed 8 Oct. 2018].

Gercke, M. (2006). The Slow Wake of a Global Approach Against Cybercrime. *Computer Law Review International,* 7 (5). Available at: http://www.unafei.or.jp/english/pdf/RS_No79/No79_05VE_Gerke.pdf
Golder, S., Ahmed, S., Norman, G., and Booth, A. (2017) 'Attitudes Towards the

Ethics of Research Using Social Media: A Systematic Review', *Journal of Medical*

Internet Research, 19(6), Available at: https://doi.org/10.2196/jmir.7082.

[Accessed 30th October 2018]

Goldman, Z. K., & McCoy, D. (2016). Economic Espionage: Deterring Financially Motivated Cybercrime. *Journal of National Security Law & Policy, pp.595-621*. Available at: http://jnslp.com/wp-content/uploads/2017/10/Deterring-Financially-Motivated-Cybercrime_2.pdf [Accessed 8th October 2018]

Grabosky, P. (2001). Virtual Criminality: Old Wine in New Bottles. *Social & Legal Studies*, 10 (2) pp. 243 – 249 Available at http://journals.sagepub.com/doi/pdf/10.1177/a017405 [Accessed 21st April 2018].

Guba, E. G. (1990). *The Paradigm Dialogue*. Thousand Oaks, CA: Sage Publications pp.44 [Accessed 7 September 2018]

Guba, E. G., and Lincoln, Y. S. (1994). Competing paradigms in qualitative research. In N. K. Denzin & Y. S. Lincoln (Eds.), *Handbook of qualitative research*, Thousand Oaks, CA: Sage Publications, pp. 105-117 [Accessed 1st August 2018]

Guidere, M. (2006). *The clash of perceptions. Defense Concepts*. [pdf] Center for Advanced Defense Studies, p.4. Available at: http://cogprints.org/4838/1/CADS_pubs_clash_0306_final.pdf [Accessed 15 Jul. 2018].

Guillot, M. (2016). I Me Mine: on a Confusion Concerning the Subjective Character of Experience. *Review of Philosophy and Psychology*, 8(1), pp.23-53. Available at https://doi.org/10.1007/s13164-016-0313-4 [Accessed 13 Jan. 2018]

Harrison, K. and Ryder, N. (2016). *The law relating to financial crime in the United Kingdom*. London: Routledge. pp.9 [Accessed 18 Nov. 2017]

Hassan, A., Lass, F. and Makinde, J. (2012). Cybercrime in Nigeria: Causes, Effects and the Way Out. *ARPN Journal of Science and Technology*, 2(7), pp.626-

631. Available at http://www.ejournalofscience.org/archive/vol2no7/vol2no7_11.pdf [Accessed 22 Oct. 2018].

Henn, M., Weinstein, M., and Foard, N. (2013) *A critical introduction to Social Research*. 2nd edn. London: SAGE Publications Ltd. [Accessed 10th November 2018]

Her Majesties Inspectorate of Constabularies (2015). *Real lives, real crimes: A study of digital crime and policing*. [pdf] London: Her Majesties Inspectorate of Constabularies. Available at: https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/real-lives-real-crimes-a-study-of-digital-crime-and-policing.pdf [Accessed: 17 October 2018].

Her Majesty's Inspectorate of Constabulary (HMIC), (2017). *PEEL: Police effectiveness 2016 A national overview.* [pdf] pp.4-5, 8-10, 12-15. Available at: http://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/peel-police-effectiveness-2016.pdf [Accessed 8 Dec. 2017].

Her Majesty's Inspectorate of Constabulary, (2015). *Regional Organised Crime Units - A review of capability and effectiveness*. [pdf] Available at: https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/regional-organised-crime-units.pdf [Accessed 21st August 2018]

Hesse-Biber, S. (2010). Qualitative Approaches to Mixed Methods Practice. *Qualitative Inquiry*, 16(6), pp.455-468. Available at https://doi.org/10.1177/1077800410364611 [Accessed 10th October 2018]

Hitchcock, A., Holmes, R. and Sundorph, E. (2017). *Bobbies on the net*. [pdf] London: Reform. Available at: http://www.reform.uk/wp-content/uploads/2017/08/Bobbies-on-the-net.pdf [Accessed 19 May 2018].

Holdaway, S. and Parker, S.K. (1998), ``Policing women police: uniform patrol, promotion and representation in the CID'', *British Journal of Criminology*, Vol. 88 No. 1, pp. 40-64, Available at https://doi.org/10.1093/oxfordjournals.bjc.a014227 [Accessed 13 Jan. 2018]

Holloway, I. (1997). *Basic Concepts for Qualitative Research*. Oxford: Blackwell Science. [Accessed 13 Jan. 2018]

Home Office (2013). *Serious and organised crime strategy.* London: Home Office Available at: https://www.gov.uk/government/publications/serious-organised-crime-strategy [Accessed 19 May 2018].

Home Office (2017). *Joint Fraud Taskforce – Oversight Board Minutes*. [pdf] London: Home Office. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attac

hment_data/file/652665/170911__JFT_Oversight_Board_Minutes.pdf [Accessed 22 May 2018].

Home Office (2018). *Understanding the costs of cyber crime - A report of key findings from the Costs of Cyber Crime Working Group.* [pdf] London: Home Office Science Advisory Council. Available at: https://www.techuk.org/images/understanding-costs-of-cyber-crime-horr96.pdf [Accessed 16 May 2018].

Hong Kong Police College (2011). *Learning and Development for Talent Management. Police Training Series. [pdf]* Wan Chai: Hong Kong Police College, p.6. *[Accessed 17th Jun. 2018]*

House of Commons (2018). *APPG Financial Crime and Scamming Young People Inquiry Terms of Reference.* [pdf] London: All Party Parliamentary Group. Available at: http://www.appgfinancialcrime.org/uploads/files/Internal-Young%20People%20Inquiry%20Terms%20of%20Reference%20Draft.docx.pdf [Accessed 22 May 2018].

House of Commons (2018). *Home Affairs Committee, Proceeds of crime, Fifth Report of Session 2016–17* [pdf] London: Home Office. Available at: https://publications.parliament.uk/pa/cm201617/cmselect/cmhaff/25/25.pdf [Accessed on 26 Jun. 2018]

Hugly, P. and Sayward, C. (1987). Relativism and Ontology. *The Philosophical Quarterly*, 37(148), pp.278, Available at https:doi.org/10.2307/2220398 [Accessed 13 Jan. 2018]

Inglesant, P., Hartswood, M. and Jirotka, M. (2018). *Thinking Ahead to a World with Quantum Computers. The Landscape of Responsible Research and Innovation in Quantum Computing.* [pdf] Oxford: UK National Quantum Technologies Programme, p.4. Available at: https://nqit.ox.ac.uk/sites/www.nqit.ox.ac.uk/files/2016-11/RRI%20Landscape%20Report%20November%202016.pdf [Accessed 3 Jun. 2018].

International Organization for Standardization (2017), *ISO 27001*, Available at https://www.iso.org/isoiec-27001-information-security.html [Accessed on 13 January 2018]

Investigatory Powers Act 2016, London: Stationary Office [Accessed 7th Jun. 2018].

J. W. Drisko and M. D. Grady (2012), *Evidence-Based Practice in Clinical Social Work*, New York :Springer, pp.19 [Accessed 21st September 2018]

Jafarkarimi H., Sim A.T.H., Saadatdoost R., Hee J.M. (2016) Designing a Scenario-Based Questionnaire to Assess Behavioral Intention in Social Networking Sites' Ethical Dilemmas. In: D'Ascenzo F., Magni M., Lazazzara A., Za S. (eds) *Blurring the Boundaries Through Digital Innovation. Lecture Notes*

in Information Systems and Organisation, vol 19. New York: Springer

[Accessed 30th October 2018]

Kiger, M. Arkin, O. and Stutzman, J. (2004). *In The Honeynet Project Know Your Enemy: Learning about Security Threats*, 2nd edn. Boston: Addison Wesley.

Kollewe, J. (2018). *UK debit cards transactions overtake cash for the first time*. Available at: https://www.theguardian.com/business/2018/jun/18/uk-debit-cards-transactions-overtake-cash-for-the-first-time [Accessed 15 Sep. 2018].

Kremen, S. H. (1998). *Apprehending the Computer Hacker: The Collection and Use of Evidence,*
Computer Forensics Online. Available at: http://www.shk-dplc.com/cfo/articles/hack.htm [Accessed 8 Oct. 2018]

Krosnick, J. A. (1991). Response strategies for coping with the cognitive demands of attitude measures in surveys. *Applied cognitive psychology*, 5(3), pp.213–236. [Accessed on 13 January 2018]

Lavrakas P.J., (2008), *Encyclopedia of survey research methods*, Thousand Oaks: Sage Publications, pp. 645 [Accessed 19 July 2018]

Lelkes, Y., Krosnick, J., Marx, D., Judd, C. and Park, B. (2012). Complete anonymity compromises the accuracy of self-reports. *Journal of Experimental Social Psychology, 48(6)*, pp.1291-1299. Available at: https://doi.org/10.1016/j.jesp.2012.07.002 [Accessed 30th September 2018]

Leonhard, G. (2016). *Technology vs. Humanity*. Tonbridge: Fast Future Publishing Ltd, p.ii. [Accessed on 26 Jun. 2018]

Leukfeldt, E. (2014). Phishing for Suitable Targets in The Netherlands: Routine Activity Theory and Phishing Victimization. *Cyberpsychology, Behaviour, and Social Networking*, 17(8), pp.551-555. Available at http://dx.doi.org/10.1089/cyber.2014.0008 [Accessed 28th April 2018].

Marcum, C., Higgins, G., Freiburger, T. & Ricketts, M. (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, pp.516 – 525. Available at https://doi.org/10.1350/ijps.2010.12.4.201 [Accessed 30 May 2018].

McCartan K., and Robson C., (2016) *Real World Research*, New Jersey: Wiley [Accessed 23rd September 2018]

McComas, H. (2017) *An investigation into learning for ethical leadership in a law enforcement environment,* MSc. Thesis. University of South Australia. Available at:
http://search.ror.unisa.edu.au/record/UNISA_ALMA11160048340001831/media/di

gital/open/9916192209901831/12160048330001831/13160048320001831/pdf [Accessed 21st September 2018]

McDowall, A., Quinton, P., Brown, D., Carr, I., Glorney, E., Russell, S., Bharj, N., Nash, R. and Coyle A. (2015) *Promoting ethical behaviour and preventing wrongdoing in organisations: A rapid evidence assessment*. [pdf] Ryton-on-Dunsmore: College of Police. Available at http://whatworks.college.police.uk/Research/Documents/150317_Integrity_REA_FINAL_REPORT.pdf [Accessed 29th September 2018]

McGuire, M. (2018). *Into the Web of Profit: An in-depth study of cybercrime, criminals and money*.[pdf] London: Bromium. Available at https://www.bromium.com/wp-content/uploads/2018/05/Into-the-Web-of-Profit_Bromium.pdf [Accessed 27 August 2018].

McGuire, M. and Dowling, S. (2013). Cyber crime: A review of the evidence. Research Report 75. [pdf] London: Home Office, p.4. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246756/horr75-chap4.pdf [Accessed 13 July 2018].

Ministry of Justice (2017). *Criminal Justice System Statistics publication: Outcomes by Offence 2007 to 2017: Pivot Table Analytical Tool for England and Wales* [pdf] London: Ministry of Justice.Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/614418/cjs-outcomes-by-offence-tool-2017.xlsx [Accessed 6th Jun. 2018].

Ministry of Justice (2017). *Criminal Justice System statistics quarterly: December 2017*. [pdf] London: Ministry of Justice. Available at: https://www.gov.uk/government/statistics/criminal-justice-system-statistics-quarterly-december-2017 [Accessed 6 Jun. 2018].

Miro, F. (2014). Routine Activity Theory. *The Encyclopaedia of Theoretical Criminology*. pp.1 Available at http://dx.doi.org/10.1002/9781118517390.wbetc198 [Accessed 19th April 2018].

Muir, R. (2016). It's time to face up to the challenge of policing in a digital age. *The Police Foundation* [Blog] 8th December. Available at: http://www.police-foundation.org.uk/2016/12/its-time-to-face-up-to-the-challenge-of-policing-in-a-digital-age/ [Accessed 17 May 2018].

Murray, K. (2016). In the shadow of the dark twin – proving criminality in money laundering cases. *Journal of Money Laundering Control*, 19(4), pp.447-458. Available at https://doi.org/10.1108/JMLC-02-2016-0009 [Accessed 13 Jan. 2018]

National Crime Agency (2015), Financial Investigator (FI) Pre-course reading V4.2, London: National Crime Agency Proceeds of Crime Centre. (Unpublished in public domain) [Accessed 9th August 2018].

National Crime Agency (2016) "*Cyber Crime Assessment 2016 – Need for a Stronger Law Enforcement and Business Partnership to Fight Cyber Crime."* Available at: http://www.nationalcrimeagency.gov.uk/publications/709-cybercrime-assessment-2016/file. [Accessed 9th August 2018].

National Crime Agency (2016b). *National Strategic Assessment of Serious and Organised Crime 2016*. London: National Crime Agency. Available at: http://www.nationalcrimeagency.gov.uk/publications/731-national-strategic-assessment-of-serious-and-organised-crime-2016/file [Accessed 3 Jun. 2018].

National Crime Agency (2017a) *National Crime Agency Annual Report and Accounts 2016–17.* Available at: http://www.nationalcrimeagency.gov.uk/publications/814-national-crime-agency-annual-report-2016-17/file [Accessed 1st August 2018]

National Crime Agency (2017b) *National Strategic Assessment of Serious and Organised Crime.* Available at: http://www.nationalcrimeagency.gov.uk/publications/807-national-strategic-assessment-of-serious-and-organised-crime-2017/file

National Crime Agency (2017c), *Economic Crime Command*, Available at: http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime [Accessed 9 Dec. 2017].

National Crime Agency (2017d), *National Cyber Crime Unit,* Available at: http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit [Accessed 9 Dec. 2017].

National Crime Agency (2018) *Careers.* Available at: http://www.nationalcrimeagency.gov.uk/careers [Accessed 1st August 2018]

National Cyber Security Centre (2017a), *Cyber Essentials,* Available at: https://www.cyberessentials.ncsc.gov.uk/ [Accessed on 13 Jan. 2018]

National Cyber Security Centre (2017b). *Cyber crime: understanding the online business model*. [pdf] London: National Cyber Security Centre, p.10. Available at: https://www.ncsc.gov.uk/content/files/protected_files/news_files/Cyber%20crime%20-%20understabnding%20the%20online%20business%20model.pdf [Accessed 3 Jun. 2018].

National Police Chiefs Counil (2015), *Force based Cyber Crime Units*. London: National Police Chiefs Council [Accessed 10 Jan. 2018]

New Stateman (2014), *The role of policing has become too broad.* Available at: https://www.newstatesman.com/politics/2014/04/role-police-has-become-too-broad [Accessed 25th September 2018]

O'Donoghue. T. (2007), *Planning Your Qualitative Research Project: An introduction to Intrepretivist Research in Education* Abingdon: Routledge [Accessed 1st September 2018]

Office for National Statistics (2017), *Crime in England & Wales, year ending June 2017* [pdf] Titchfield: Office for National Statistics. Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/june2017 [Accessed 26th Dec. 2017]

Office for National Statistics (2018), *Crime in England & Wales, year ending March 2018* [pdf] Titchfield: Office for National Statistics. Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/march2018 [Accessed 29th September 2018]

Office of the police and crime commissioner Northamptonshire (2014). *Northamptonshire's Police and Crime Plan 2014 – 2017, Making Northamptonshire the Safest Place in England.* [pdf] Available at: https://cmis.northamptonshire.gov.uk/cmis5live/Document.ashx?czJKcaeAi5tUFL1DTL2UE4zNRBcoShgo=evy6e0TzG077xZK3LP5ECyO97v3ghczOW%2BNUaemEtlC%2FbVS%2BLR5fqA%3D%3D&rUzwRPf%2BZ3zd4E7Ikn8Lyw%3D%3D=pwRE6AGJFLDNlh225F5QMaQWCtPHwdhUfCZ%2FLUQzgA2uL5jNRG4jdQ%3D%3D&mCTIbCubSFfXsDGW9IXnlg%3D%3D=hFflUdN3100%3D&kCx1AnS9%2FpWZQ40DXFvdEw%3D%3D=hFflUdN3100%3D&uJovDxwdjMPoYv%2BAJvYtyA%3D%3D=ctNJFf55vVA%3D&FgPlIEJYlotS%2BYGoBi5olA%3D%3D=NHdURQburHA%3D&d9Qjj0ag1Pd993jsyOJqFvmyB7X0CSQK=ctNJFf55vVA%3D&WGewmoAfeNR9xqBux0r1Q8Za60lavYmz=ctNJFf55vVA%3D&WGewmoAfeNQ16B2MHuCpMRKZMwaG1PaO=ctNJFf55vVA%3D [Accessed 8 Oct. 2018].

Office of the police and crime commissioner Staffordshire, Police and Crime Panel (2018). *Update from the PCC on the Safer, Fairer, United Communities for Staffordshire 2013-18: Focus Priority: Modern Policing.* [pdf] Available at: http://moderngov.staffordshire.gov.uk/documents/s103938/PCP%2029%2001%2018%20SFU%20Modern%20Policing%20Update%20rept.pdf [Accessed 8 Oct. 2018].

Okeshola, F. and Adeta, A. (2013). The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria. *American International Journal of Contemporary Research*, 3(9), pp.98-114. Available at http://www.aijcrnet.com/journals/Vol_3_No_9_September_2013/12.pdf [Accessed 22 August 2018].

Onaolapo, J., Mariconti, E. and Stringhini, G. (2016). What Happens After You Are Pwnd; Understanding the Use of Leaked Webmail Credentials in the Wild, *Proceedings of the 2016 Internet Measurement Conference.* Available at: http://dx.doi.org/10.1145/2987443.2987475 [Accessed 26 Jun. 2018].

Ong, A. and Weiss, D. (2000). The Impact of Anonymity on Responses to Sensitive Questions. *Journal of Applied Social Psychology, 30(8), pp.1691-1708*. Available at: https://doi.org/10.1111/j.1559-1816.2000.tb02462.x [Accessed 30th September 2018]

Onwuegbuzie, A.J., and Teddlie, C. (2003) 'A Framework for Analysing Data in Mixed Methods Research', in Tashakkori, C., and Teddlie, C. (eds) *Handbook of Mixed Methods in Social and Behavioural Research.* Thousand Oaks, CA: Sage Publications Ltd, pp. 351-383.

Oreku G.S., Mtenzi F.J. (2017) Cybercrime: Concerns, Challenges and Opportunities. In: Alsmadi I., Karabatis G., Aleroud A. (eds) *Information Fusion for Cyber-Security Analytics. Studies in Computational Intelligence, vol 691*. Cham: Springer, [Accessed 22 May 2018].

Palmer, D. (2018). Ransomware: *Why the crooks are ditching bitcoin and where they are going next | ZDNet.* Available at: https://www.zdnet.com/article/ransomware-why-the-crooks-are-ditching-bitcoin-and-where-they-are-going-next/ [Accessed 15 Sep. 2018].

Parliament Street (2018). *Policing and Cybercrime*. [pdf] London: Parliament Street, p.3. Available at: http://parliamentstreet.org/wp-content/uploads/2018/03/Parliament-Street-Policing-and-Cybercrime.pdf [Accessed 2 Jul. 2018].

Paulhus, D.L., and Vazire, S. (2007) 'The Self-Report Method', in Robins, R.W., Fraley, R.C., and Krueger, R.F. (eds) *Handbook of Research Methods in Personality Psychology.* New York, London: The Guildford Press, pp. 224-239 [Accessed 13 Jan. 2018]

Penny Dick, Devi Jankowicz, (2001) "A social constructionist account of police culture and its influence on the representation and progression of female officers: A repertory grid analysis in a UK police force", *Policing: An International Journal of Police Strategies & Management*, Vol. 24 Issue: 2, pp.181-199, Available at https://doi.org/10.1108/13639510110390936 [Accessed on 13 Jan. 2018]

Police Federation (2018) *Quick reference guide – A basic summary of your main terms and conditions*. Available at: http://www.polfed.org/aboutus/3638.aspx [Accessed 5th October 2018]

Police Foundation (2018) More than just a number. Computer Fraud & Security, 2018(12), p.4. Available at https://doi.org/10.1016/S1361-3723(18)30116-7 [Accessed 4th January 2019]

Police.uk, (2018). *List of UK Police Forces* Available at: https://www.police.uk/forces/ [Accessed 21st August 2018]

Pope, C., and Mays, N.B. (2006) *Qualitative Research in Health Care.* 3rd end. Oxford: Blackwell Publishing. [Accessed 13 Jan. 2018]

Proceeds of Crime Act 2002 c.29, Pt 7, Sec 327, 328, 329, 340. London: The Stationery Office. [Accessed 13 Jan. 2018]

Ragin, C. and Amoroso, L. (2010). *Constructing social research*. 2nd ed. London: Sage Publications, pp.3,123. [Accessed 5th September 2018]

Ramage, S. (2012). "Information technology facilitating money laundering." *Information & Communications Technology Law,* 21(3), pp.269-282. Available at https://dx.doi.org/10.1080/13600834.2012.744226 [Accessed 13 Jan. 2018]

Recorded Future. (2018). *Litecoin Emerges as the Next Dominant Dark Web Currency*. Available at: https://www.recordedfuture.com/dark-web-currency/ [Accessed 15 Sep. 2018].

Reeve, T (2016). *UK Government launches new National Cyber Security Strategy. SC Media UK, 1 November.* Available at: https://www.scmagazineuk.com/uk-government-launches-new-national-cyber-security-strategy/article/570116/ [Accessed 15 Oct. 2017].

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [Accessed 25th September 2018]

Rolstad, S., Adler, J. and Rydén, A. (2011). Response Burden and Questionnaire Length: Is Shorter Better? A Review and Meta-analysis. *Value in Health, 14(8),* pp.1101-1108. Available at: https://doi.org/10.1016/j.jval.2011.06.003 [Accessed 30th September 2018]

Roycroft M. (2017) *"Police Chiefs in the UK: Politicians, HR Managers or Cops?". In: Police Chiefs in the UK.* Palgrave Macmillan:Cham p.vii [Accessed 21st September 2018]

Saunders J. (2017) Tackling cybercrime – the UK response, *Journal of Cyber Policy, (2) 1*, pp.4-15, Available at: http://dx.doi.org/10.1080/23738871.2017.1293117 [Accessed 9th August 2018].

Schreuders, Z.C., Cockcroft, T.W., Butterfield, E.M., Elliott, J.R.. Soobhany, A.R. and Shan-A-Khuda, M. (2018) Needs Assessment of Cybercrime and Digital Evidence in a UK Police Force *(Unpublished journal, Leeds Beckett University)* pp.*15,20* Available at http://eprints.leedsbeckett.ac.uk/5076/ [Accessed 7th September 2018]

Fanusie Y. and Robinson T., *"Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services"* [pdf] Foundation for Defense of Democracies and Elliptic, January 12, 2018. https://s3.us-east-2.amazonaws.com/defenddemocracy/uploads/documents/MEMO_Bitcoin_Laundering.pdf [Accessed 7th September 2018]

Sheehan, K. (2001), 'E-mail Survey Response Rates: A Review', *Journal of Computer-Mediated Communication*, 6, Available at: http://ascusc.org/jcmc/vol6/issue2/sheehan.html [Accessed 5th September 2018]

Shipley, P. (2017). Coaching and evidence-based learning. *Journal of Community Safety and Well-being, 2(3),* pp.116-118. Available at https://journalcswb.ca/index.php/cswb/article/view/54/116 [Accessed 7 August 2018]

Shoshitaishvili, Y, Invernizzi, L, Doupe, A & Vigna, G 2014, Do you feel lucky? A large-scale analysis of risk-rewards trade-offs in cyber security. *Proceedings of the ACM Symposium on Applied Computing*, pp. 1649-1656 Available at https:dx.doi.org/10.1145/2554850.2554880 [Accessed 22 Oct. 2018].

Sittlington, Samuel and Harvey, Jackie (2018) Prevention of Money Laundering and the Role of Asset Recovery. *Crime, Law and Social Change*. 70(4) pp.421-441 Available at https://doi.org/10.1007/s10611-018-9773-z [Accessed 2 Jul. 2018].

Smartsurvey.co.uk. (2017). *Privacy Policy* | *SmartSurvey,* Available at: https://www.smartsurvey.co.uk/privacy-policy [Accessed 26 Nov. 2018].

Snell, E. (2015). *Policing Cybercrime*. [pdf] London: Royal Holloway University. Available at: https://www.royalholloway.ac.uk/isg/documents/pdf/technicalreports/2016/computer-weekly-articles/esthersnellcw.pdf [Accessed 16 May 2018].

Snow, R. & Bloom, A. (1996). A survey-based pedagogical approach to ethics in the workplace. *The Journal of Applied Behavioral Science, 32(1)*, pp.89-100. Available at: https://doi.org/10.1177%2F0021886396321006 [Accessed 30th August 2018]

Tatham, N. (2017). *Viewpoint Survey 2017 - Full group report* [pdf] Derby: Derbyshire Constabulary (Unpublished in public domain) pp.26, 43 [Accessed 8 Oct. 2017]

Theregister.co.uk. (2018). *Dixons Carphone: Yeah, so, about that hack we said hit 1.2m records? Multiply that by 8.3*. Available at: https://www.theregister.co.uk/2018/07/31/dixons_carphone_breach_10m_records/ [Accessed 16 Sep. 2018].

Totalcrypto (2018) *Bitcoin Adoption: Trading Volume by Country* Available at: https://totalcrypto.io/bitcoin-adoption-trading-volume-country/ [Accessed 20 Oct. 2018].

Transparency International UK (2014 pp.3.). *National Risk Assessment of Money Laundering and Terrorist Financing.* Available at:

https://www.transparency.org.uk/wp-content/plugins/download-attachments/includes/download.php?id=1392 [Accessed 27 Jun. 2018].

University of Derby. (2013) *Policy and Code of Practice on Research Ethics*.

Derby: University of Derby. [Accessed 16 Oct. 2018].

University of Glasgow (2016). *Theories and causes of crime*. [pdf] Glasgow: Scottish Centre for Crime & Justice Research, pp.1-9. Available at: http://www.sccjr.ac.uk/wp-content/uploads/2016/02/SCCJR-Causes-of-Crime.pdf [Accessed 24 Jun. 2018].

Van Wegberg R., Oerlemans J., Van Deventer O., (2018) "Bitcoin money laundering: mixed results?: An explorative study on money laundering of cybercrime proceeds using bitcoin", *Journal of Financial Crime, Vol. 25 Issue: 2,* pp.419-435 Available at: https://doi.org/10.1108/JFC-11-2016-0067

Victim Support (2012). Out in the open What victims really think about community sentencing. [pdf] Victim Support, p.14. Available at: https://www.victimsupport.org.uk/sites/default/files/Out%20in%20the%20open%20-%20what%20victims%20really%20think%20about%20community%20sentencing.pdf [Accessed 20 May 2018].

Walden, I. (2016). *Computer crimes and digital investigations.* 2nd ed. Oxford: Oxford University Press [Accessed 22 Nov. 2018].

Weber, R. (2004) 'The Rhetoric of Positivism Versus Interpretivism: A Personal View', *MIS Quarterly, 28(1),* pp. 3-12. Available at: https://misq.org/misq/downloads/download/editorial/25/ [Accessed 13 April 2018]

Westera, N., Kebbell, M., Milne, B. and Green, T. (2014). The prospective detective: developing the effective detective of the future. *Policing and Society*, 26(2), pp.197-209. Available at: http://dx.doi.org/10.1080/10439463.2014.942845 [Accessed 14th August 2018]

Wood, H. (2017) Every transaction leaves a trace: The role of financial investigation in serious and organised crime policing. [PDF] Royal United Services Institute for Defence and Security Studies: London. Available from: https://rusi.org/sites/default/files/201709_rusi_everytransactionleavesatrace_wood_web.pdf [accessed 2/10/2018] [Accessed 15th December 2018]

Yun, G.W. and Trumbo, C.W. (2000), 'Comparative Response to a Survey

Executed by Post, E-mail and Web Form', *Journal of Computer-Mediated*

Communication, 6, Available at http://www.ascusc.org/jcmc/vol6/issue1/yun.html

[Accessed 1st August 2018]

Appendix A

1. Please create a unique identifier below of two digits, two letters and a special character. This will be used to identify the data you generate if you wish to withdraw from the study at a later point in time. Please remember the ID you create.

2. Describe your experience and knowledge of digital investigation

3. What impact does social interaction with colleagues have on your role?

4. Describe your experience and knowledge of financial investigation

5. What level of law enforcement agency do you work for?

- Local
- Regional
- National

6. What rank do you hold?

7. What words do you associated with money laundering?

8. Have you ever applied money laundering to a digital investigation?

- Yes
- No

9. If so, what were the brief circumstances? (If you have not please move to the next question)

10. How many convictions for money laundering in a digital investigation have you obtained?

- 0
- 1 - 5
- 5 - 10
- 10+

11. What barriers do you perceive to utilising money laundering offences in digital investigations?

12. Do you feel financial investigation training would benefit your role?

- Yes
- No
- Uncertain

13. Why do you feel this way?

14. How often have you worked with financial investigators in the last 12 months?

- 0
- 1 - 5
- 5 -10
- 10+

15. Scenario 1

An offender gains unauthorised access to a corporate database containing customer data. They take a screenshot of the customer data held within and log off.

Can money laundering offences be considered?

- Yes
- No

16. Why?

17. What is criminal property within the scenario?

18. What offence/s would you deem appropriate in the scenario?

19. Scenario 2

An offender uses a credit card purchased on a darknet market to fund access to a botnet.

Can money laundering offences be considered?

- Yes
- No

20. Why?

21. What is criminal property within the scenario?

22. What offence/s would you deem appropriate in the scenario?

23. Scenario 3

An offender in Germany distributes malware which includes installing a backdoor. A number of victim computers (including those belonging to UK nationals) are infected and herded into a botnet. This is then made available for rental in a darknet marketplace. The offender visits the UK a short time after this and is arrested.

Can money laundering offences be considered?

- Yes
- No

24. Why?

25. What is criminal property within the scenario?

26. What offence/s would you deem appropriate in the scenario?

Appendix B

The following information was provided to participants in order to make them aware of the privacy policy of Smart Survey. Tactics to prevent this policy from undermining their anonymity were then detailed.

“To uphold the participant's confidentiality, it is necessary to make it clear that certain data which could identify the participant may be collected online. Smart Survey have a privacy policy which lists the data they collect.

The main items of concern for privacy are summed up in the policy:

“We may also collect data from the device and application that you use to access our services, including your IP address (from which we may infer your geographic location), login information and browser type. If you arrive at our website from an external source (such as a link on another website or in an email) we record information about that source.” (Smartsurvey.co.uk, 2017).

If this causes any concern the following tactics could be employed to prevent identifying data being collected:

- Don’t use a LE computer to access the survey
- Consider clearing the browser cache before visiting the survey web page.
- Employ a Virtual Private Network, Proxy or TOR prior to accessing the survey to mask the IP.
- Mask the user agent string
- Clear the browser cookie cache once the survey is complete”