THE POLICE FOUNDATION
The UK's policing think tank

UNLEASHING THE VALUE OF DIGITAL FORENSICS

RICK MUIR and STEPHEN WALCOTT

JANUARY 2021

UNLEASHING THE VALUE OF DIGITAL FORENSICS

Acknowledgements

The Police Foundation is very grateful to the Transforming Forensics programme for funding this research. The authors would like to thank Beverley Nutter and Winnie Jandu for their support and guidance throughout the project, and for their useful feedback. Thank you also to the 18 practitioners and stakeholders across England and Wales who took part in interviews to share their experiences.

About the Police Foundation

The Police Foundation is the only independent think tank focused exclusively on improving policing and developing knowledge and understanding of policing and crime reduction. Its mission is to generate evidence and develop ideas which deliver better policing and a safer society. It does this by producing trusted, impartial research and by working with the police and their partners to create change.

CONTENTS

1. Introduction **2**

2. Digital forensics in England and Wales **3**

2.1 What is digital forensics? 3

2.2 How is forensics capability currently organised in England and Wales? 3

3. The value of digital forensics **5**

3.1 Case studies 5

3.2 Wider technological advances 6

4. Challenges **8**

4.1 Demand and Capacity 8

4.2 Skills and knowledge 9

4.3 System weaknesses 9

4.4 Technology 10

4.5 Law and ethics 11

5. Conclusion **13**

Appendix **14**

List of interviewees 14

References **15**

1. INTRODUCTION

The digital revolution has transformed the ways in which people commit crime. Digital technology has created new opportunities to commit long established forms of crime such as child sexual abuse and fraud. It has also created the space for wholly new types of criminal activity such as phishing scams and denial of service attacks. Moreover, the ubiquity of digital devices and the centrality of the internet to most people's way of life mean that almost any crime will now generate a trail of digital evidence that is relevant to the work of the criminal justice system.

The volume of digital evidence now potentially relevant to criminal cases is such that it threatens to overwhelm the police, prosecutors and the courts. For example, a single mobile phone is estimated to be able to contain one terabyte of data, which is equivalent to around 78 million pages of a written document (House of Lords 2019). The technical challenge of retrieving, storing, analysing and interpreting such large volumes of data is considerable.

Moreover, technology changes quickly, meaning that police investigators and the wider criminal justice system need to continually adapt as criminals develop new ways of committing crime and covering their tracks. This poses a major challenge for organisations like police forces that have not prioritised investment in information technology. The police also use public sector procurement processes, which means that it can take months and even years to purchase new technology, leaving them generally behind the curve of technological change.

The challenges are not just technical, but also ethical. The creation of vast amounts of data in the course of everyday life means that a person's whereabouts, their behaviour and their private conversations are now traceable by police agencies and potentially subject to scrutiny in court in a way that was simply not possible in the past. At the same time, our attitudes to privacy are only just adapting to this new reality, leaving agencies such as the police unsure as to how far they should go in the surveillance of citizens or the examination of personal data. Because the law has tended to lag even further behind the reality of technological change the police are often making decisions about the balance between liberty and security in the absence of clear legal frameworks.

These challenges are particularly acute in the field of digital forensics, which is the subject of this report.

There is widespread concern within policing and beyond about the state of digital forensic capability in England and Wales. Indeed, the House of Lords Science and Technology Select Committee said in 2019 that "*the rapid growth of digital forensic evidence presents challenges to the criminal justice system. We were not presented with evidence of any discernible strategy to deal with them*." (House of Lords, 2019).

This Police Foundation report, commissioned by the Transforming Forensics Programme, is intended to help inform the development of a new national Digital Forensics Strategy for the police service. It has two aims: first to present evidence of the potential value that could be added to the work of policing and the wider criminal justice system from investment in digital forensics capability and, second, to set out the main challenges that need to be overcome if we are to make the most of these opportunities.

The report is based on research carried out by the Police Foundation between October 2019 and April 2020, including:

- 18 interviews with a range of digital forensics stakeholders, including digital forensic examiners, senior police managers with responsibility for forensics, prosecutors and academics (the full anonymised list can be found in the Appendix to this report).
- A literature review drawing together the findings of relevant secondary sources on the state of digital forensic capability in England and Wales.
- A discussion dinner held in partnership with KPMG bringing together a range of relevant stakeholders to discuss our emerging findings.

The report comes in three main parts. First, we describe the context for this report, defining what we mean by digital forensics and setting out how capability is currently organised in England and Wales. Second, we describe the importance of digital forensic work as a core part of the modern criminal justice system, highlighting examples from our interviews where digital forensic techniques have made a significant difference to criminal cases. Third, we identify a number of challenges that need to be overcome if we are to realise the potential of digital forensics, as well as recommendations for decision makers throughout policing and beyond.

2. DIGITAL FORENSICS IN ENGLAND AND WALES

In this section we define what we mean by digital forensics and describe how digital forensic services are currently organised in England and Wales.

2.1 WHAT IS DIGITAL FORENSICS?

The recent inquiry into the quality and delivery of forensic science in England and Wales, by the House of Lords Science and Technology Select Committee (House of Lords 2019), defined forensic science, of which digital forensics forms a part, as the application of "*scientific methods to the recovery, analysis and interpretation of relevant materials and data in criminal investigations and court proceedings"'* Forensic science encompasses a whole spectrum of sub disciplines such as DNA analysis, fingerprint examination, digital or computer forensics, forensic anthropology and ballistics.

Interpol defines digital forensics as "*a branch of forensic science that focuses on identifying, acquiring, processing, analysing and reporting on data stored on a computer, digital device or other digital storage media*" (INTERPOL, 2019). It has also been defined as "*The discipline that combines elements of law and computer science to collect and analyse data from computer systems, networks, wireless communications and storage devices in a way that is admissible as evidence in a court of law*" (US CERT, 2008).

For many years digital forensics was seen as a niche discipline, relevant mainly in so-called "hi-tech crime". However as digital evidence has become a core part of almost any criminal case, the use of digital forensics has now become a core criminal justice function. Under the general umbrella of digital forensics there are many sub disciplines including mobile, network, cyber, email, web, system and data forensics (Lopez et al,. 2016). As digital technology develops further the number of technical specialisms within digital forensics will most likely multiply.

2.2 HOW IS FORENSICS CAPABILITY CURRENTLY ORGANISED IN ENGLAND AND WALES?

Prior to 2012, the market leader in the provision of forensic science in the UK was the Forensic Science Service, a government agency funded by the Home Office. Following its abolition in 2012, police forces have commissioned forensics from the private sector or provided them in-house. The private sector predominates in some areas of forensics such as toxicology, whereas the police tend to provide other services such as digital forensics and fingerprint examination in-house. The House of Lords Science and Technology Select Committee describes the overall pattern of provision as follows:

> *"the forensic marketplace accounts for about 20% of service provision for law enforcement in forensic services by value, with the remaining 80% of forensic science work conducted by in-house employees of police forces."*

There are three major companies providing forensic science services: LGC Forensics (owned by Eurofins Forensic Services), Key Forensic Services (KFS) and Orchard Cellmark Ltd. KFS went into liquidation in 2018 and a package of investment was agreed to support the delivery of existing police casework in progress at the time and future investment. KFS was bought out and still provides a wide range of services. Alongside these large providers is "a cottage industry" of small firms "some of which employ only one or two people" (House of Lords, 2019).

Since 2008, oversight of this mixed economy has been provided by the Forensic Science Regulator, Dr Gillian Tully, whose role is to ensure that forensic work meets the best scientific standards. The Regulator monitors compliance with quality standards, although she does not have any statutory enforcement powers.

Both the Forensic Science Regulator and the House of Lords Science and Technology Select Committee, among others, have criticised the current pattern of forensic science provision. In particular, they have

voiced the concern that provision is too fragmented, meaning that each police force makes their own decisions as to how to commission forensic science, sometimes making decisions more on grounds of cost than quality. The Regulator has criticised police forces for commissioning private companies who do not currently meet international quality standards.

The financial difficulties Key Forensic Services faced in 2018 demonstrated the fragility of some of the major players in the forensics market. That fragility is explained in part by a major reduction in police force spending on forensic science services. Andrew Rennison, a Commissioner at the Criminal Cases Review Commission and former Forensic Science Regulator, told the House of Lords Science and Technology Select Committee that in 2008, "*there was probably £120 million being spent on forensic science. That is now down to about £50 million or £55 million*". This reduction is in the context of significant cuts of around 20 per cent to police force budgets over the last decade (NAO, 2018).

The fragility of the major players in the market, alongside the challenge of rapid technological change, have led many, including the Forensic Science Regulator, to argue that a strategic approach to forensics is lacking in England and Wales (Tully 2017, 2018, 2019). It was to address these concerns, at least on the policing side, that the National Police Chiefs' Council (NPCC) established the Transforming Forensics Programme in 2018 with £30 million funding from the Police Transformation Fund. The Programme aims to develop a more strategic approach to forensics across policing, facilitating collaboration across police forces, tackling operational fragmentation, improving compliance with standards, and improving capability in areas of rapidly changing technology such as digital forensics and DNA.

The Transforming Forensics Programme has led to the development and launch of the Forensic Capability Network, a network of police forces that will work collaboratively on a national basis to strengthen their forensic capability. The network is intended to stabilise the forensics marketplace by providing a more coherent structure for procurement, to ensure that police forces meet accreditation to international standards in their delivery of forensics, to benefit from greater economies of scale, to meet changing demands and to provide a stronger foundation for the development of the forensic science workforce (Forensic Capability Network, 2020).

In conclusion, the way in which forensics is delivered in England and Wales is changing, in recognition of the widespread concern that the existing model is fragmented, lacks a strategic approach and is unable to keep pace with the speed of technological change. In Section 4 below we explore how these challenges manifest themselves in the arena of digital forensics, but before that we turn to the potential value digital forensics can bring to the criminal justice system.

3. THE VALUE OF DIGITAL FORENSICS

The importance of digital forensics as a core capability within policing and criminal justice cannot be overstated. According to one senior police manager, digital evidence plays a role in 90per cent of criminal cases (House of Lords, 2019). What was once a niche sub-discipline mainly deployed in investigations of "high end" cybercrime is now a core competency required to meet demand across all forms of crime investigation.

It is not easy to assess the public value delivered by digital forensics for a number of reasons. First, there is no consolidated picture of the value generated by digital forensics. The fragmented nature of delivery, broken up into 43 police forces, some working through regional collaborative arrangements, alongside a cottage industry of private providers, means that it is hard to both develop a clear picture as to the extent of provision and to assess its impact. Second, establishing impact is not straight forward because much of it is located in outcomes which do not happen (for example, future crimes not committed by a prolific offender jailed due to digital forensic evidence) and which are not recorded or measured. Third, in part because this is an area of considerable change and flux, there is little academic research on the impact of digital forensic work.

From the literature and our interviews with stakeholders and practitioners, we identify the following types of public value generated by digital forensics capability:

- Swifter justice through the early identification of offenders, and speedier exoneration of innocent suspects.
- The prevention of potentially large numbers of future crimes by supporting the identification and conviction in court of prolific offenders.
- Reductions in investigation times allowing the police to move on to other cases and solve more crimes.
- Reductions in court costs, with digital forensic evidence potentially leading to more early guilty pleas and quicker trials.

Indeed, given the prevalence of digital evidence in almost all forms of crime investigation, without proper digital forensic capability we are likely to see a deterioration in performance across all of those metrics. It is widely believed across policing that a lack of investment in digital forensics is already resulting in prolonged investigations, lost opportunities to bring offenders to justice and costlier prosecutions.

Given the exponential increase in the volumes of digital data we are seeing, there was widespread agreement among those we interviewed that unless there is a significant uplift in digital forensics provision the police service could be overwhelmed and the criminal justice system unable to function effectively.

3.1 CASE STUDIES

In this section we draw on our interviews with digital forensic practitioners and stakeholders to highlight a number of examples of digital forensic techniques that they believe have had, or are having, a major impact on police investigations. In all of these cases the techniques hold great potential but are not yet widely used across policing.

Case study 1: Software to extract telematic data from vehicles

Software can extract telematic data from vehicles, providing tracking logs, attached devices and event logs. For example, it can track GPS waypoints from a sat nav to plot a journey, show when doors or windows open and identify erratic driving. A case report is assembled along with witness accounts and other digital evidence, such as CCTV footage. Such telematic data has enormous value, as realised in the successful prosecution of the Anglesey crossbow murderer in 2019. In that case the now convicted killer's precise movements on the night of the killing were tracked by data from "black box" technology in a Land Rover, which belonged to his partner and which he had borrowed (BBC News, 2020). While vehicles are not always the subject of the crime, they are very often an enabler and so this software offers enormous value across a whole range of cases.

We were told that this software is available to a majority of forces, but uptake has been slow due to resource pressures and a lack of understanding of what it can do. We were told that when new software like this is released it takes a long time and a lot of interest from

an individual practitioner to understand its value and how it can be used. Police forces are often reluctant to spend money on a new licence when they are uncertain about its value.

One specific challenge which may prove to be a barrier with extracting telematic data from vehicles is that it requires some dismantling of a vehicle and there is no guarantee that it can be put back together again. We should also note that the software is not suitable for all vehicle models.

Case study 2: Forensic capture of open-source internet data

Some forces use tools to capture open-source data in internet investigations, some of which can be downloaded for free. These enable the filing of screenshots, video captures and webpage downloads, including from the "dark web". These are automatically timestamped and hashed, enhancing the accuracy of evidence.

Challenges to its use include a lack of technical ability and the threat of malware. However, we were told that a bigger challenge is confusion over the legal authority required and interpretation of the applicable policies, regulations and legislation in this area. Some forces have looked to gain legal authority to use these tools while others have avoided them for fear of breaking surveillance laws.

A further challenge lies in the fact that some live data now simply disappears. For example, Snapchat data is automatically deleted after a given time. We were told that policing needs to adapt to the speed at which potential digital evidence comes and goes on the internet.

Case study 3: Wifi analysis

Various analytical techniques using wifi router data have been reported. Wifi surveying involves an assessment of the wifi networks that are visible and available to be connected to, when visiting a specific location.

Router examination tools can reveal all devices that have connected to a specific wifi network based on the router logs. This can be used to expose hidden or undeclared devices upon, for example, a house search and is sophisticated enough to tell the investigator the distance a connected device is from them.

Examination of a mobile device to reveal the wifi networks it has connected to, in conjunction with the above wifi analysis techniques, is a powerful investigatory tool. Findings would enable the inference of a suspects' whereabouts, corroborating a hypothesis and/or assist in finding additional suspects. However, we were told that forces are often unaware that these are tactics they can use.

Case study 4: Analytics software

Analytics software allows the data of numerous devices to be imported at one time. Some specific tools can use artificial intelligence to analyse and identify all communication links between the devices of suspects and/or victims and have the capability to search numerous devices simultaneously using a list of keywords. While saving significant time, it also solves problems with disclosure in court; the defence can request keywords to be added to the search which can be run easily and the recording of keyword searches reduces the likelihood of evidence being missed. It can be particularly useful in largescale child sexual exploitation, terrorism and street grooming investigations, by large forces, where various devices can be involved.

However, analytics software is not used across forces nationally for numerous reasons such as its high cost, the challenges of implementing new technology in forces and the potential ethical concerns with the wider data sharing that is involved. Its expense poses a problem for smaller forces that may only need to use it infrequently. Practitioners suggested that if it could be technically deployed alongside a cloud solution, so that licences and data could be shared, police investigations across the nation would benefit. It has been acknowledged that the ethical issues around such a cloud solution would need thorough consideration and clarity beforehand.

3.2 WIDER TECHNOLOGICAL ADVANCES

Beyond these examples of the value of specific digital forensic techniques our interviewees also highlighted wider technological advances that could enhance digital forensic work in the future.

Automation

The volumes of data requiring analysis mean that automation is critical. One of our interviewees estimated that with scripted or automated conversion and movement of data between systems, about a third of examiners' time would be saved. Automation is also one way of handling the issues of privacy highlighted in Section 4 below. If automated systems are able to identify what is and what is not likely to be relevant this

makes the investigator's task easier and should avoid examiners having to trawl through all of a person's photos, emails or text messages.

For example, if software could flag up when there is movement in a CCTV clip, this would enable examiners to go straight to the most relevant footage. The Crown Prosecution Service is currently trialling a system where photos are presented as thumbnails on a screen, eliminating the need to click into every separate file.

If more of the cumbersome manual tasks can be automated this means that highly skilled examiners can spend more of their time analysing and drawing inferences rather than processing data. As one senior police manager told us, "*it would allow examiners to actually do their job*".

Cloud-based storage

Cloud computing has now become the norm, with both business and personal users adopting this as the new form of data storage. Cloud storage enables large amounts of data to be stored and accessed remotely, which enables users to work flexibly and disposes of the need for organisations to have on-site servers.

There are obvious benefits from using the cloud to store digital evidence. Having to store vast amounts of digital data, including imagery and video footage, is a daunting challenge. Moreover, if a police force uses its own data storage system, this prevents other forces from accessing data they may require. From the point of view of scale, accessibility and flexibility the case for cloud-based storage is strong. There are however concerns that need to be overcome. Chief among these is data security, with a concern that storing police data remotely may make it vulnerable to hacking. However, given the pressing need to find storage capacity for the volumes of data that will need to be held now and, in the future, it is likely only a matter of time before policing embraces cloud storage for digital evidence.

4. CHALLENGES

In recent years, a number of reports have highlighted the weakness of digital forensics provision. In March 2019, the Forensic Science Regulator released her annual report which described the level of compliance to standards as "woeful".[1] (Tully 2017 and 2018). Similarly, in May 2019 the House of Lords Science and Technology Select Committee report on forensic science argued that the rapid growth of digital forensics creates an enormous challenge for the entire criminal justice system. The evidence presented to the select committee "*pointed to failings in the use of forensic science in the criminal justice system and these can be attributed to an absence of high-level leadership, lack of funding and an insufficient level of research and development*"(House of Lords, 2019). These reports echoed the findings of other such reports over the last ten years, specifically that forensic science, and in particular digital forensics, face significant challenges which if not addressed will mean that the criminal justice system cannot function effectively and could lead to serious miscarriages of justice (House of Lords, 2019; The Law Commission, 2011).

In this section we describe the range of challenges facing digital forensics that were identified in our literature review and in our interviews with practitioners and stakeholders.

4.1 DEMAND AND CAPACITY

> *"It's very difficult to think of a case that potentially doesn't have a digital element"*
>
> (Police digital forensics adviser)

> *"There is a digital witness in every case"*
>
> (Police digital forensics adviser)

> *"Entire digital lives are being extracted"*
>
> (Digital forensics practitioner)

Demand for digital forensics is growing; digital evidence is now relevant in most crime investigations and the volumes of data stored on devices which is potentially relevant to a criminal enquiry is also expanding. At the same time, the supply of digital forensics resources in the form of people and technology has been constrained. This is partly explained by the fact that the amount of money spent by police forces on forensics over the last decade has almost halved (House of Lords, 2019.)

One interviewee told us that staff numbers would have to increase by between a third and a half to meet current demand. Staff shortages have been made more acute by the so-called "brain drain" of digital expertise within policing due to digital forensics examiners leaving the public sector for private sector salaries. We were told that the ideal digital forensics examiner would have both computer skills and investigatory skills, but it is understood that a mixture of these competencies is hard to find.

One solution has been to supplement the work of examiners with Digital Media Investigators who advise on the strategy of an investigation, making the digital examiner's work more streamlined.

The lack of resources is also a concern. Many forces will be using poor and outdated technology while criminals innovate with new and more sophisticated ways of committing crime. Police forces also find themselves struggling with a very limited number of software licences. This means staff must wait for machines to become available and cannot operate flexibly across workstations.

This technology lag will only worsen as evidence in the future will be found on a whole range of new devices and in a bewildering range of novel formats. As one senior police manager told us: *"We are slow to revamp, technology is changing faster than us".*

Interviewees told us that backlogs for investigators waiting for data to be extracted and examined from devices range from a few weeks to six months, with waiting times of up to one year for some specialist services. If evidence for a case is urgent this can be fast-tracked and greater triage capability is now being rolled out, which should help. As part of triage, some police forces use a scoring matrix to prioritise and determine the urgency of a case prior to analysis.

[1] We should note that the same report did recognise improvements across all aspects of digital forensics and acknowledged that Digital Forensic Units were not the root of the problem.

Recommendation

There is a clear case for increased investment in digital forensic capability as part of the next Spending Review. This should lead to an increased number of specialist staff, an uplift in technology across policing and a pay and recruitment model that allows policing to attract and retain expertise.

4.2 SKILLS AND KNOWLEDGE

> *"If you don't understand the technology and you're an investigator, there's no way you're going to solve the crime"*
>
> (Digital forensics practitioner)

> *"It's now mainstream policing and not a specialism"*
>
> (Digital forensics practitioner)

There is a consensus among digital forensics stakeholders that the digital knowledge of frontline police officers involved with forensics needs to be improved. This is not only includes specific software but also digital forensic procedures. We were told that officers can at times ask for too much information and consider it to be urgent or they cannot explain why they need what they are requesting. We were told that sometimes inexperienced investigators do not understand what a reasonable line of enquiry is nor how to preserve digital evidence.

Training should enable more officers to use frontline kiosks for low-level examination. Enabling and trusting police officers to do this would give early access to intelligence and would free up capacity in the specialist labs to be more proactive, enhancing the efficiency of the evidence-gathering process.

To deepen officers' understanding of digital forensic investigators' capabilities, it has been suggested that officers spend a day in a lab to see how they operate and build a more communicative relationship. Interviewees also suggested that digital forensics skills and knowledge should be incorporated into mandatory officer training. This should involve teaching on what is achievable, the different data formats and the various software packages available. We were told that for officers that have already had their training, the materials they can refer back to, to refresh their knowledge need to be modernised.

Recommendations

All frontline officers should receive digital investigative training and as part of this some basic training in digital forensics, so that they are able to do more of the less complicated examinations themselves.

Training could usefully include frontline officers spending time in the lab with specialist staff to promote greater mutual understanding.

There should be greater investment in digital forensic practitioners' learning and development including more accessible and more frequent conferences on new software and techniques and dedicated staff whose role is to understand what different software tools can do.

4.3 SYSTEM WEAKNESSES

There is a strong belief among stakeholders that the whole system that sits behind digital forensics capability needs reform.

A fragmented police service

> *"Everybody thinks their processes are the best, but actually someone else might be able to give you a different, better, quicker, higher quality process"*
>
> (Digital strategy adviser)

> *"Everyone values their autonomy"*
>
> (Academic expert)

There is overwhelming agreement that the way in which the police service is organised is ineffective for the purposes of digital forensics. The 43 police forces have different leaders, governance and priorities, while also using different tools and processes. We were told that each police force or each regional collaboration works in its own silo and is reluctant to share best-practice, which has an impact on quality. By not sharing ideas on how jobs are solved, each investigator will start from scratch each time. It is precisely to build a better learning system in forensics that the new Forensic Capability Network has been conceived.

A lack of interoperable IT is an important consequence of organisational fragmentation. This means that data cannot always be shared because of different formats and systems. This chronic lack of inter-operability means that practitioners end up burning data onto CD-ROMS, which we were told is normal practice in at least one large force.

There are some areas of digital forensics where inter-operability is growing. For example, one force has linked their kiosk systems to CAID, the Child Abuse Image Database. It flags up where an image on a device has a matching hash-value to an image already on the database. This means that the police can better understand the circulation of images and potentially can help to identify victims.

Recommendations

There should be much greater joint national procurement of digital forensics tools through the Forensic Capability Network and all forces should be part of this. Ministers should mandate co-operation if necessary.

The Forensic Capability Network should create an on-going learning environment for digital forensic practitioners to share knowledge, including regular conferences to ensure people's knowledge of the field is up to date.

The lack of common quality standards

> *"When trying to work to ISO accreditation, we're not being smart enough with how we implement it"*
>
> (Senior police manager)

Page et al. (2018) compare the current quality management procedures in the UK for forensic science disciplines and report that digital forensics operates with the least robust quality management procedures. International standards (ISO) provide a credible framework for ensuring that the evidence submitted to the courts is reliable. However, police forces have generally struggled to attain accreditation, which we were told has been hampered by a lack of national guidance on how this ought to be done.

There is some debate around the use of accreditation in digital forensics. For example, Sommer (2018) states that a whole crime scene may be on one device and may contain large volumes of data types that need to be handled in different ways. On top of this, he suggests that the pace of change creates a problem when considering the speed that it takes to study, publish and present on the reliability of methods or artefacts. Sommer (2018) concludes that there is no "one size fits all" approach to accreditation and that a mixture of accreditation and good practice guidance is the most suitable way forward.

Private providers

> *"We are heavily reliant on external private companies that make the tools"*
>
> (Police frontline technical lead)

> *"We've got five or six men in control of over half the stuff ever written. Wherever you are politically or forensically, it's quite a… dystopian position to be in"*
>
> (Senior police manager)

Due to their lack of capacity to cope with increasing demand, forces are contracting cases out to private forensic providers. However, our interviewees told us that there is a lack of collaboration between policing and these private providers, meaning that different tools are being used that may affect the results of extraction and examination. For example, this can be a problem in a case where the defence hires a private company to do an examination and after some time a new version of software generates evidence that the police did not originally discover.

It was suggested to us that a national digital forensics body should support a more collaborative approach to software/hardware development, such that private providers better understand what the police need, and the police service can act as a more intelligent customer. Iterative design involving police input should lead to the development of better tools more suited to investigative needs.

Recommendation

There should be a joint working-group involving law enforcement, forensic service providers and resource developers to facilitate greater collaboration and user-led design.

4.4 TECHNOLOGY

Inevitably the work of digital forensics units is complicated by technological challenges.

> *"I think everyone accepts we will always be a little behind the curve in relation to being able to access data on devices"*
>
> *(Digital strategy adviser)*

The diversity of data

With an increase in the range of devices and data formats, the technical challenges of carrying out digital forensic work become ever greater. Raghavan (2013) identifies complexity, volumes, consistency and diversity as some of the significant issues for digital forensics. The internet of

things, along with the number of devices that are currently in use, generate a diverse range of operating systems, data types and file formats (Lillis et al., 2016). The proliferation of device types and data formats makes it harder to generate consistency in the outputs of digital forensic work.

This problem is exacerbated by the lack of any kind of systematic communication between the police and the device or app manufacturers. For example, we were told that a recent iPhone update resulted in the complete alteration of file systems which investigators had to work around. While this is beneficial for the security of Apple devices, it causes considerable problems for efficient digital forensic examination. Keeping up with changing operating systems, millions of changing applications and security patches can delay work by months.

The problem of diverse data is complicated further by the lack of interoperability of police force IT systems already discussed. This also results in data being presented in different formats making it difficult to compare forensic outputs.

Encryption

> *"If you don't want to be caught, you won't"*
>
> (Frontline technical lead)

> *"Manufacturers hold the key. It's their devices and their technology"*
>
> (Digital strategy adviser)

Encryption, as an anti-forensic tool, is by far the biggest challenge facing digital forensics. While some have called for encryption to be banned, this seems unlikely because of the consumer benefits in terms of improved privacy and data security.

There are technical ways around encryption, but they are complex and time consuming. The police have capability and software to decrypt pin codes and methods to tackle encryption. However, this is limited in response to sophisticated encryption used by some criminals.

Recommendations

There should be much greater collaboration between the NPCC/Home Office and device manufacturers.

There needs to be greater investment in research and development teams and in-house developers within forces to keep up with changing technology in collaboration with external software engineers and academia.

Cloud-based storage

> *"We don't always know if we're doing it in a lawful manner"*
>
> (Senior police manager)

Cloud computing has become the norm, with both business and personal users being attracted to its flexibility, scalability and accessibility. However, the cloud has been identified as one of the biggest challenges for digital forensics (Al Fahdi et al., 2013; Zawoad and Hasan, 2013; Biggs and Vidalis, 2009).

Garfinkel (2010) argues that the cloud threatens forensic visibility by denying access to evidence. This is because third party providers often host cloud-based services, and the servers are generally located in other countries (Vincze 2016). Getting access to evidence therefore involves all of the time-consuming legal processes necessary when operating across jurisdictions.

There is also a problem with the chain of custody in relation to the evidence. Grispos et al., (2012) point out that unless an investigator can disable a service, evidence cannot be protected from being destroyed.

Recommendation

The College of Policing should issue clearer guidance regarding the use of powers to extract cloud data.

4.5 LAW AND ETHICS

Perhaps some of the most significant challenges in the arena of digital forensics lie in law and ethics. In both arenas there is evidence that the pace of technological change and the realities of digital forensic work have outpaced the knowledge, understanding and beliefs of parliamentarians, legal practitioners and citizens.

Privacy

> *"Any sort of future legislation should be friendly enough so we can still do our jobs properly, but robust enough so people can be sure we're going to look after their private data"*
>
> (Digital strategy adviser)

> *"If you were searching a house, you wouldn't search everything"*
>
> (Frontline technical lead)

"'In the past, you would need a warrant to search someone's house, you'd swear in front of magistrates and you'd have to indicate what you thought you might find… you wouldn't go through every piece of correspondence"

(Senior police manager)

"We probably put people in a position where they feel forced to hand over their devices"

(Digital media investigator)

There has always been tension between a person's right to a private life and their right to safety and security. In order to protect us, the state may also intrude into our private lives under certain circumstances. The digital revolution has shifted the parameters of this debate by enabling a degree of surveillance and intrusion into the private sphere that before the internet would have been unthinkable. Not just governments, but powerful organisations of all kinds, are now able to know an extraordinary amount about our movements, behaviour and thoughts in so far as they can be traced digitally.

In relation to policing it is important that we understand where the boundary lies between what is appropriate in terms of intrusion into the private sphere and what is not. In her 2019 John Harris Memorial Lecture, the Commissioner of the Metropolitan Police Cressida Dick argued that the key issue for the police is proportionality: what degree of surveillance or intrusion is proportionate to a particular threat or the needs of a particular investigation? (Dick, 2019).

Unless the police are able to reassure victims on proportionality there is a signficant danger that the fear of handing over a phone and a computer and all the personal data held within them may deter victims from reporting crime. In light of the R vs Allen case (BBC News, 2019), the Crown Prosecution Service reportedly asked examiners to go through all of the victim's data. There is a serious tension here between the defendant having the right to a fair trial and respecting a victim's right to privacy.

In emerging areas, such as live facial recognition technology, the police are having to develop their own ethical protocols because legal frameworks are unclear. This puts the police in the uncomfortable position of being at the forefront of a privacy versus security debate that arguably would be better led by parliament.

Recommendations

There is a need for much clearer national guidance for police officers regarding the examination of digital evidence. We suggest that there should be minimal intrusion relative to the needs of the investigation.

This guidance should be backed up by improved training for frontline officers and support from Digital Media Advisers who can support their colleagues to determine what is required for the purposes of the inquiry and what is proportionate in relation to privacy.

Technical understanding in courts

"Courts are unrealistic when asking for evidence"

(Senior police manager)

We were told that a lack of understanding of digital forensics results in legal practitioners making unrealistic demands of examiners. This can include asking for further investigation within unrealistic timescales. Courts also often ask for evidence in complicated formats such as PDFs, on a disk or as paper copies. The Crown Prosecution Service then has to decrypt reports sent to them using instructions sent by examiners, which we were told are often not properly understood. Practitioners also told us that the audio visual systems in courtrooms are of a low quality and, for example, often fail to accurately present moving CCTV footage which may provide vital evidence for the jury.

An improved relationship between the Crown Prosecution Service and digital forensic investigators may help reduce instances of misinterpretation. We were told repeatedly by practitioners that legal professionals such as judges, prosecutors and defence barristers would all benefit from basic digital forensic training.

Recommendation

Training in digital forensics should be provided for all practitioners in the criminal law, including judges, prosecutors and defence barristers.

Data retention

Concerns were raised about the length of time data needs to be retained by law. The requirement to retain data for seven years after its latest review has resulted in vast archives that are expensive to maintain and which have slowed down police servers.

Recommendation

National data retention policies should be reviewed, and clear guidance issued clarifying when deletion is appropriate.

5. CONCLUSION

The vast digital traces that almost everyone now creates in the course of everyday life have created a serious problem for the criminal justice system. While the volumes of evidence now available can help to solve more cases, convict more criminals and exonerate more innocent suspects, gathering, processing, analysing and interpreting that data is mammoth task.

It is not an exaggeration to say that, as currently configured, the criminal justice system, from the police service to the courts, does not have the capability to meet this challenge. This has been the finding not just of this report, but of numerous reports and reviews in recent years.

This report adds value to this debate by seeking to understand the views and experiences of those at the frontline of delivery in digital forensics: digital forensic examiners and operational police mangers, as well as stakeholders such as prosecutors and academic experts.

The report has done two things. First, it is has sought to identify the “value added” of digital forensics. It is difficult if not impossible to do this in a comprehensive way, simply because the data is not available to do so. So instead, we have highlighted value by way of a number of case studies, in which practitioners have highlighted the difference that a technique has made to cases they have worked on.

Second, the report has scoped out the range of challenges that need to be overcome if we are to develop a strong digital forensic capability within policing. It should be noted that it is the intention of the National Police Chiefs’ Council (NPCC) that many of these challenges are addressed by the new Forensic Capability Network (FCN). This attempt to achieve much greater coordination of effort and strategic grip in forensics is very welcome and we hope that the recommendations we have made might be taken up by the NPCC and the FCN as this work advances.

APPENDIX

LIST OF INTERVIEWEES

Systems Developer, Metropolitan Police

Digital Strategy Adviser, Metropolitan Police

Frontline Technical Lead, Metropolitan Police

Digital Forensics Coordinator, Staffordshire Police

Digital Forensics Investigator, City of London Police

Digital Forensics Manager, City of London Police

Digital Forensics Hub Manager, Metropolitan Police

Inspector & Digital Forensics Unit Head, Metropolitan Police

Senior District Crown Prosecutor, Crown Prosecution Service

Academic, University of Exeter

Digital Media Investigator Team Supervisor, Lancashire Constabulary

Digital Forensics Team, KBR (formerly West Midlands and Thames Valley)

Digital Media Advisor, National Crime Agency

Head of National Police Capabilities Unit, Home Office

Cybercrime Detective, Dorset Police

Digital Forensics Manager, Greater Manchester Police

Digital Forensics Hub Supervisor, Leicestershire Police

Detective Constable for Online Child Sexual Exploitation, West Mercia Police

REFERENCES[2]

Al Fahdi, M., Clarke, N. L. and Furnell, S.M. (2013). Challenges to digital forensics: a survey of researchers & practitioners attitudes and opinions. *Information Security for South Africa*, pp.1-8.

BBC News (2019) Rape victims among those to be asked to hand phones to police. *BBC News,* [online] 29 April. Available at: <https://www.bbc.co.uk/news/uk-48086244>

BBC News (2020) Anglesey crossbow murder: Man guilty of Gerald Corrigan murder. *BBC News,* [online] 24 September. Available at: <https://www.bbc.co.uk/news/uk-wales-51618959>

Biggs, S. and Vidalis, S. (2009) Cloud computing: The impact on digital forensic investigations. In *2009 International Conference for Internet Technology and Secured Transactions (ICITST)* (pp. 1-6). IEEE.

Dick, C. (2019). John Harris Memorial Lecture 2019: Cressida Dick CBE QPM, Commissioner of the Metropolitan Police. Available at: <http://www.police-foundation.org.uk/past-event/2019-cressida-dick-cbe-qpm-commissioner-of-the-metropolitan-police/>

Forensic Capability Network (2020) <https://www.fcn.police.uk/>

Garfinkel, S.L. (2010) Digital forensics research: The next 10 years. *Digital Investigation*, *7*, Supplement, pp.S64-S73.

Grispos, G., Storer, T. and Glisson, W.B., (2012) Calm before the storm: The challenges of cloud computing in digital forensics. *International Journal of Digital Crime and Forensics (IJDCF)*, *4*(2), pp.28-48.

House of Lords (2019), *Forensic Science and the criminal justice system: a blueprint for change,* HL Paper 333.

INTERPOL (2019), *Global Guidelines for Digital Forensics Laboratories*, INTERPOL Global Complex for Innovation. Available at: <https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf>

Lillis, D., Becker, B., O'Sullivan, T. and Scanlon, M., (2016) Current challenges and future research areas for digital forensic investigation. In: *The 11th ADFSL Conference on Digital Forensics, Security and Law (CDFSL 2016)*, Daytona Beach, Florida, USA, May 2016.

Lopez, E. M., Moon, S. Y. and Park, J. H. (2016). Scenario-based digital forensics challenges in cloud computing. *Symmetry*, 8(10), pp.107.

NAO (2018) *Financial sustainability of police forces in England and Wales 2018* [pdf] Available at: <https://www.nao.org.uk/wp-content/uploads/2018/09/Financial-sustainability-of-police-forces-in-England-and-Wales-2018.pdf>

Page, H., Horsman, G., Sarna, A. and Foster, J. (2018). A review of quality procedures in the UK forensic sciences: what can the field of digital forensics learn? *Science & Justice*, 59(1), pp.83-92

Sommer, P. (2018) Accrediting digital forensics: what are the choices? *Digital Investigation* 25 (June 2018), pp. 116-120

The Law Commission (2011) *Expert evidence in criminal proceedings in England and Wales. No. 325.* [pdf]. Available at: <https://www.lawcom.gov.uk/project/expert-evidence-in-criminal-proceedings/>

Tully, G. (2017) *Forensic Science Regulator: Annual Report – November 2015-2016.* [pdf] <https://www.gov.uk/government/publications/forensic-science-regulator-annual-report-2016>

Tully, G. (2018) F*orensic Science Regulator: Annual Report – November 2016-2017.* [pdf]. Available at: <https://www.gov.uk/government/publications/forensic-science-regulator-annual-report-2017>

Tully, G. (2019) *Forensic Science Regulator: Annual Report – November 2017-2018.* [pdf]. Available at: <https://www.gov.uk/government/publications/forensic-science-regulator-annual-report-2018>

US CERT (2008) *Computer Forensics* [pdf] Available at: <https://www.us-cert.gov/sites/default/files/publications/forensics.pdf>

Zawoad, S. and Hasan, R., (2013) *Cloud forensics: a meta-study of challenges, approaches, and open problems*. [pdf]. Available at: <https://arxiv.org/pdf/1302.6312.pdf>

[2] Accessed 18 December 2020.

Email: info@police-foundation.org.uk

www.police-foundation.org.uk

ISBN: 0 947692 78 9

Charity Registration Number: 278257

THE POLICE FOUNDATION

The UK's policing think tank