



TRANSFORMING
FORENSICS



Forensic
Capability
Network



NPCC
National Police Chiefs' Council



Association of
Police and Crime
Commissioners

Digital Forensic Science Strategy

July 2020

Contents

Foreword.....4

Executive summary.....5

The challenges 6

 Core challenge 1: Volume

 Core challenge 2: Complexity

 Core challenge 3: Legitimacy

 Issue 1: Lack of support services

 Issue 2: Fragile commercial marketplace

 Issue 3: Limited strategic engagement with partners (academia and industry) to work on long term solutions

 Issue 4: Recruitment and retention

 Issue 5: Lack of DF Science awareness within policing

 Issue 6: Embedding quality

 Issue 7: Handling legacy data

The solution 8

 Improved operations

 Improved commercial practices

 Centralising science and Research and Development (R&D)

 Meeting the data challenge

 Developing the workforce

 Building trust

In conclusion 11

Introduction 12

Our starting point 12

New possibilities in a changing landscape 12

Here and now 13

Meeting the challenges 13

 Core challenge 1: Volume

 Core challenge 2: Complexity

 Core challenge 3: Legitimacy

 Issue 1: Lack of support services

 Issue 2: Fragile commercial marketplace

 Issue 3: Limited strategic engagement with partners (academia and industry) to work on long term solutions

 Issue 4: Recruitment and retention

 Issue 5: Lack of DF Science awareness within policing

 Issue 6: Embedding quality

 Issue 7: Handling of legacy data

Strategic objectives.....16

1. Improving operations.....19

The role the Forensic Capability Network plays 20

Core principles of future operations 21

Benefits 24

 Strategic benefits:

 Tactical benefits:

2. Improving commercial practices and R&D.....27

Industry 27

 Coordinating requirements

 Strategic engagement to develop capabilities

Research and development 30

Benefits 31

 Strategic benefits

 Tactical benefits

3. Meeting the data challenge 35

Infrastructure requirements.....36

Processing, analysing and sharing digital forensic data 37

Benefits 40

 Strategic benefits

 Tactical benefits

4. Developing the Workforce 43

 Developing a joint approach

 Collaborative governance

 Building a skills pipeline

 Standard approaches for training and competency

 Effective workforce planning

 Continuing professional development and learning

 Knowledge management

 Building multidisciplinary collaboration

 Addressing the needs of the wider workforce – CSIs, first responders, frontline data recovery users and investigators

Benefits 48

 Strategic benefits

 Tactical benefits

5. Building Trust 51

Public attitudes towards digital forensics 51

Ethical governance and oversight.....52

Improving governance and data security 53

 Operational guidance

 Data

 Quality standards

 Communicating public benefit

Benefits 57

 Strategic benefits

 Tactical benefits

Putting it all together.....59

Supporting research.....60

 Policing data capture

 Original research

 Rapid evidence reviews

 Proof of concepts

 Simulation modelling

Glossary of Terms.....61

Foreword

Digital Forensic Science sits at the heart of delivering justice in the 21st century, spanning the entire criminal justice system, from crime scene to courtroom. It shapes policy, offers a range of capabilities that better enable us to counter new and emerging threats, and is central to achieving our shared outcomes around reducing crime and increasing public safety.



To date however, we haven't been quick enough or co-ordinated enough in making use of the potential that digital forensics offer, to find a way to take advantage of the huge advances in mobile, cloud, artificial intelligence, sensors and analytics that are commonplace in almost every other walk of life. While crime and criminals have become ever more digitally sophisticated, our response, at every level of law enforcement, has been slow, fractured and piecemeal. To create a justice system that truly meets the needs of the public in the digital age, while also meeting demands for greater efficiency, we must think differently about our approach to every element of digital – and digital forensics in particular.

If we are to deliver against our ultimate priorities – to protect children from sexual exploitation, to break the scourge of County Lines, to disrupt terrorism and reduce serious violence – and do so in a way that is proportionate and ethical, we need a coherent, cohesive, and **collective** response to the use of digital forensics. This strategy lays out a way for us to meet these challenges head on.

In the course of developing this strategy, we have carried out research and analysis to understand, at a granular level, the

problems we face. While the problems themselves are familiar – growth in demand, rapid pace of technological change and policing's struggle to adapt – our research has served to highlight the scale and urgency of the issues and underline the pressure our service is under.

A number of these challenges are addressed in the recent NPCC and APCC National Policing Digital Strategy¹, which elegantly articulates how digital transformation, improvements in the use of data and technology, and a huge skills uplift are central to meet 2030 ambitions. But there is a difference between the data that the National Policing Digital Strategy looks at, and digital forensics data, which is our focus here. The data from victims, witnesses and suspects – the data for digital forensics – is from non-police sources and is about 20 times the volume of all other police data combined, and demands additional consideration around how it is captured, used and stored. But it is vital that our plans for digital forensics are no longer siloed away from the wider policing digital/ICT landscape as has too often been the case in the past. As such, the two strategies should be viewed as companion pieces: two sides of the same coin, and key drivers in delivering a high functioning, fully integrated, whole-system approach to digital policing. The ICO's recent report on the mobile phone examinations forces carry out in the course of criminal investigations in England and Wales, highlights that we need to rebuild and maintain public trust through better compliance with data protection legislation – we need to manage personal data consistently and proportionately to provide the best possible service to the criminal justice system. This strategy sets out a road map for us to do that.

The work already delivered by the Transforming Forensics Programme, in particular helping to establish the Forensic Capability Network as means

of delivering new forensics capabilities into policing, have been crucial steps in taking these problems on. This strategy builds on these successes, providing a blueprint for bringing about the step-change in the use of digital forensics that we all recognise is necessary in order to provide the world-leading level of service that our public deserves.

Key to the strategy is the industrialised, consistent and standardised approach to the use of technology. For example, in harnessing automation to make sure that we not only deliver better results quicker, but do so in a way that reduces the emotional distress for our teams caused by investigating disturbing images.

But the strategy is about far more than technology. It sets out a new approach to recruiting and retaining a workforce that will enable us to catch up, and keep up, with the constantly evolving digital landscape in which we operate. And it highlights how we can use flexible and novel commercial approaches to get the best from our partners to create a forensics marketplace that is able to respond to fast-changing Digital Forensic Science requirements. Crucially, the strategy also provides a path to restoring and maintaining public confidence in the way policing uses digital evidence, reassuring victims and witnesses that they will not be subject to unnecessary intrusion in the course of an investigation.

To deliver on these ambitions, new approaches to national and regional collaboration, and pooling our sovereignty in ways that support improved local operations, are necessary. Revised governance arrangements will support this, but, above all, it will require all those working in digital forensics – all of **us** – to lean into the issues, and work together in ways we never have before.

This strategy establishes a roadmap for how we will achieve our aims by 2025, and lays the foundations for a system

that will enable us to respond quickly, effectively and collectively to threats in the future, whatever those threats may be. The lion's share of work to develop this strategy was complete before the COVID 19 pandemic hit this country. Since then the circumstances in which we find ourselves have changed

dramatically. But we have responded quickly, creatively and with real resolve. We need to harness that same creativity, speed and resolve to meet the challenges we will face in the future head on.

We are pleased to share the strategy with you – and to invite you to join us on the journey.

Chief Constable James Vaughan
NPCC LEAD FOR FORENSICS
SRO, TRANSFORMING FORENSICS

Temporary Chief Constable Nick Baker
NPCC LEAD FOR DIGITAL FORENSICS

Martyn Underhill
POLICE AND CRIME COMMISSIONER, DORSET

Executive summary

Digital forensic (DF) science – examining digital evidence to support investigations and prosecutions – was once niche but is now very much mainstream. Over 90% of all crime is recognised as having a digital element, and society's accelerating use of technology means the critical role DF science plays will only grow. We have developed this strategy to address the huge opportunities and corresponding challenges this presents for policing.

The NPCC commissioned and owns this Digital Forensic Science strategy. It builds on and supports the National Policing Digital Strategy (NPDS). We draw on parallels with that strategy, how they relate to DF science, identify challenges unique to providing DF capabilities and lay out how we will address them. This strategy supports the aims and objectives of the Policing Vision 2025.

Traditionally, Digital Forensic Units (DFUs) delivered DF services. But DF science is expanding outside DFUs and forensic labs and frontline staff now do some digital forensic work too. So this strategy considers the needs of DF science across the criminal justice system, from crime scene to courtroom. We look at DF science as the 'golden thread' running through the investigative process, including specialist analysis by practitioners in DFUs as well as more straightforward extraction of data by trained users outside DFUs.

This strategy recognises the exciting potential of emerging technologies for policing. Investigative capability can be transformed with the rapid and unique insights from DF analysis of any of our myriad devices, which can replace months of physical surveillance, giving unprecedented



access to our thoughts through conversations or search histories; though if policing is to use this ability, it must do so responsibly, sensitive to the ethical issues that arise.

At the same time, DF services can take advantage of rapidly growing cloud services, allowing us to simplify and rationalise DF data storage, harness the power of automation, and explore new technologies such as machine learning. To allow policing to unlock the enormous potential of technology, forces need to coordinate effectively and work together to overcome the challenges this will entail.

The challenges

Transforming Forensics Programme (TF) research identified three 'core challenges' that DF science faces:

Core challenge 1: Volume

Growth in use of digital technology has led to exponential growth in demand for DF examinations. Driven by the number of devices, better communications and increased cloud storage, demand has been rising by 11-16% over the last few years, and we expect this to continue. The result? Backlogs and delays to investigations. These delays and backlogs impact victims, witnesses and suspects waiting for the outcome of investigations and often for the return of their devices. They increase the risk of harm too by delaying bringing offenders to justice. Most DFU work is fraught with risk - much of it involving child sexual exploitation (CSE) or other serious crime. Managing demand is complex, and policing's focus on these crimes to reduce the harm they cause generates more demand on DFUs.

Core challenge 2: Complexity

Digital examinations themselves present a complex challenge. There are more types of device, more end-to-end encryption, more varieties of data format, and more data stored in the cloud. The 'Internet of Things' is growing rapidly - so we need to develop new techniques simply to maintain DF capability to extract and analyse information, to avoid cutting off the criminal justice system from critical sources of evidence. But

force DFUs have limited capacity to research and develop innovative techniques and very few have access to external research support.

Core challenge 3: Legitimacy

Public awareness of personal data privacy is rising. Although broadly supportive of police using digital forensic analysis, recent issues around disclosure and consent for digital device examinations mean the public are more aware and alive to the issues involved. Meeting the challenge of rising data volumes, encryption and cloud storage means policing needs to work in new ways and it is crucial to maintain public trust and confidence in doing so. Policing needs to work proactively with Government to ensure the legislative and ethical frameworks on which these activities are founded are right for the digital age.

In this strategy we also seek to address several other pressing issues:

Issue 1: Lack of support services

DF services have grown organically over the last twenty years, often operating in relative isolation, without support from force ICT departments or procurement teams. Developing DF from 'cottage industry' to key investigative support function has happened outside many forces' corporate IT arrangements and it is unclear who is responsible for funding, managing and providing these IT services. As a result DFUs often lack core tools to help them manage their activity.

Issue 2: Fragile commercial marketplace

The Forensic Science Regulator (FSR) highlighted that forensic science funding reductions have led to a substantial decrease in the size of the supplier market and 'the potential for further major exits from the market and/or loss of a range of disciplines hangs in the balance'¹. DF services in policing rely on external suppliers for additional capacity and expertise. Action to put this market on a sustainable footing is essential because policing has insufficient internal capacity to cover the gap and this risks growing backlogs and failure to harvest critical intelligence, data and evidence.

Issue 3: Limited strategic engagement with partners (academia and industry) to work on long term solutions

A lack of coordination between forces limits policing's ability to build strategic relationships with academia and industry to develop and access new capabilities. Some larger forces/regional collaborations have attempted this individually, but absent a national approach, it is inconsistent and inefficient. R&D is uncoordinated and not shared. Policing is slow to take up existing new capabilities and this will erode their ability to exploit digital data sources to support investigations and prosecutions.

Issue 4: Recruitment and retention

Recruiting experienced digital forensics examiners is an issue for all forces. With a finite pool of experienced professionals to draw from, forces must compete with the private sector, and the growing



number of cyber security roles where there is substantial crossover with DF skills. Most forces have open positions for staff they find very difficult to fill and the difficulty of keeping existing staff is exacerbated by a lack of formal career paths and variable access to training and professional development.

Issue 5: Lack of DF Science awareness within policing

Frontline officers can now access tools for straightforward data extractions; and investigators will review results of digital forensic examinations. They often deal with different sources of digital evidence, where the value of each may not be clear. They need a basic level of understanding to ensure they do not miss opportunities to assess and understand properly the value of digital evidence. But there is no national DF training for these roles.

Issue 6: Embedding quality

The FSR mandated that all forces achieve accreditation to the ISO17025 quality standard for their forensic science activities. Despite a deadline of October 2017 compliance is still low. Less than 20% of processes requiring accreditation have achieved it, not because of lack of commitment from DFUs but because the pace at which digital forensics is changing and the lack of capacity makes it very challenging for forces to achieve quality accreditation. This challenge is greater when it comes to digital forensics than any other discipline because of the added complexity resulting from the range of digital forensics data types and methods. Regular releases of new consumer devices mean policing needs to be able to examine new devices immediately.

Unlike other forensic areas, there is no time for doing a controlled

validation study before introducing a new forensic technique. Using capabilities outside DFUs introduces yet more challenge, as does the requirement for ISO17020 accreditation for on-scene work by October 2020.

Issue 7: Handling legacy data

Handling and retaining data is difficult for forces because differing legislation, policy and guidance in this area does not provide a clear indication on what DF data needs to be retained and for how long. Legacy data, generated or seized for, or as a result of, past digital forensic examinations, is stored in various formats. For most forces, lack of access to case management systems and limited integration with force ICT means managing and weeding this data is largely manual. This puts a significant burden on forces and exposes them to compliance risks.

¹ FSR evidence to the HoL Science and Technology Committee, 2019 (<http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee-lords/forensic-science/written/96445.html>)

The solution

This strategy puts forward our vision for transformational change to DF science across several areas:

Improved operations

Standardising, industrialising and providing services centrally - 'doing it once for the benefit of many' are the foundations to transform DF science service. Standardising processes will allow forces to collaborate on casework, technology, R&D and quality assuring processes. This will underpin everything we do in the future, including automation. To develop the operating model, TF and FCN, in tandem with forces and partners, will build on the three-tier approach Digital Forensics Portfolio Board (DFPB) outline which many forces have already adopted. This tiered model will be delivered nationally and provide national, regional and local elements. By harnessing forces' effort across the country, we will ensure everyone pulls in the same direction, getting the most from joint work and helping establish the FCN as a national knowledge and expertise network for DF, all underpinned by a nationally networked technology solution.

Once this tiered operating model is embedded consistently, DF services will be more agile and responsive to fast-changing needs. Technology will enable agile working - using a flexible platform and toolset to scale up capability quickly when we need to and taking advantage of cloud technologies. There will be common ways of working and a shared information architecture, removing barriers to collaboration and enabling flexible resource deployment to meet demand. The service will be designed with

continual improvement at its heart, a system which can evolve, and with reach outside policing.

TF and FCN will work to ensure maximum value for investment in delivering the operational model and transforming DF science service for the whole criminal justice system, from crime to court, improving quality, consistency and timeliness.

Improved commercial practices

Bringing how policing engages with the commercial sector onto a sure and strategic footing is key to transforming DF science service. Coordinating this engagement nationally and agreeing joint requirements, will enable policing to leverage its collective buying power and act as an 'intelligent customer'. This will allow us greater influence to ensure the market develops the capabilities we will need and ensure the supplier market is sustainable and resilient.

Forensic service providers, carrying out digital forensic analysis on behalf of policing, are integral to DF science services. As part of the Forensic Marketplace Strategic Plan, FCN Commercial and Digital Forensic Market Operations Group (DFMOG) will seek consensus across policing on likely national demand in the future to allow FSPs to plan the services they deliver and give them confidence to grow and innovate to deliver those services. When forces agree common requirements allowing simpler deployment into standard workflows, **forensic tool vendors** will benefit. More strategic engagement with policing will also allow vendors to anticipate policing's future needs better when it comes to developing longer term capabilities.

Improving access for small, innovative suppliers in emerging areas to provide their services will ensure policing has access to the full range of technological innovation. There will be more engagement with consumer device providers, technology and online services, to inform and develop digital forensic analysis capabilities for these devices, technologies and services in future.

FCN Commercial will streamline how we engage with suppliers across the marketplace, developing model contract clauses for key areas such as data retention or security vetting. They will provide guidance for forces on routes to market and ensure references to interoperability and open standards are included in all future contracts.

Centralising science and Research and Development (R&D)

R&D is critical to driving continuous improvement in DF science. FCN Science will facilitate improving and scaling up how we coordinate and collaborate nationally, so we can implement innovative techniques more quickly. They will coordinate and influence an R&D programme drawing in R&D effort nationally, combining casework-driven capabilities that practitioners develop with industry research by tool vendors, and multi-disciplinary academic research. This will address short and long term research needs, dealing with everything from technology to wider issues such as ethical implications of cutting-edge techniques and the value DF science gives to the CJS. We will establish one or more innovation hubs, physically or virtually, to provide a

central point for R&D and specialist capabilities, and a way to draw in support from partners in academia and industry including UK Research and Innovation (UKRI) and DSTL. We will also establish a DF science advisory group in the FCN with representatives from academia, operational policing and research organisations to provide independent advice and guidance. We will set the expectation that all DF activity be grounded in sound scientific principles, with a robust evidence base for all new techniques, and that all processes involving DF science take a 'quality first' approach. In addition to traditional DF services which practitioners in DFUs with specialist knowledge and expertise deliver, this will include frontline capabilities that trained operators deliver, using locked-down methods where DF science knowledge is embedded in an automated workflow.

Meeting the data challenge

We will ensure that DF science delivers maximum possible benefit to the criminal justice system, extracting best value from the data policing holds. We will do this by improving and streamlining the way we manage digital forensic source data. TF and FCN will support forces to agree a consistent national approach to handling legacy DF data, producing operational guidance to interpret existing policy and legislation. Building on discovery work with forces, TF will support Government to develop national policy to manage DF data and prepare for future demand.

To enable us to tackle the growing challenges of data volume and complexity, TF should design and implement a DF science information



architecture built on the FCN Xchange platform including a national DF data model aligned to recommendations in the NPDS. As part of this, we must take decisions about the degree to which we centralise DF data management and technology. There are advantages but also ethical and security considerations the more integration there is between forces and partners. With this in mind TF will collaborate with forces to develop the optimal architecture for using cloud technologies.

A standard DF data model and information architecture will deliver huge benefits across the criminal justice system. Adopting this approach, structured data storage will facilitate managing data automatically and retaining it in compliance with legislation. This will allow intelligent search and review to tackle the huge

disclosure challenge around DF data. Such a model will support sharing information securely with partners, improve the service we provide to victims and witnesses and help to improve criminal justice outcomes.

Developing the workforce

To transform DF Science we must invest in our people. We need to recruit and retain a skilled workforce who are motivated, fully trained, well managed and equipped with access to the right tools and processes to deliver a world class DF service to the criminal justice system.

FCN Science, in partnership with the College of Policing (CoP), seeks to professionalise DF Science roles improving career opportunities and ensuring a culture of continuous learning supported by a national competency framework, training



and a workforce recruitment and retention plan. As part of this retention plan, in partnership with industry and academia we will build a 'skills pipeline' so we can reinforce the workforce continually. The community should coordinate continuing professional development to help practitioners collaborate and share knowledge. A knowledge base, continually updated, will provide quick and easy access to emerging learning and novel techniques.

The traditional understanding of a 'DF workforce' is changing. We need to widen this definition to include all staff whose activities include an element of DF science, including those using automated tools and workflows. FCN Science will work with the CoP to identify these roles and put the right level and depth of

training in place. General awareness training for all officers should include information about DF capabilities to support investigators to understand what comes out of DF examinations, and to allow officers to engage with DF services in a more informed way. This will ensure they can extract maximum benefit and understanding from any DF evidence to be used at court. FCN Science will lead a similar initiative to address the needs of the wider CJS.

Building trust

Legislation and ethics

The right legislation and ethical frameworks are critical to building and maintaining public trust and confidence in DF science in policing. We will support Government to

ensure that legislation is fit for purpose in a digital age and addresses future technological advances. The FCN aims to help policing maintain appropriate operational processes and governance, ensuring we address public ethical and trust concerns, and deliver better support to the CJS. The Government will work to ensure all DF Science activity is underpinned by clear powers and nationally agreed policies and guidance with close support from the FCN and input from the wider CJS, FSR and Information Commissioner's Office (ICO). This work will inform the national data ethics governance model, as outlined in the NPDS.

Quality and assurance

Transforming governance, the workforce, commercial engagement,

operations and how we manage data as we have laid out will ensure quality is 'built in' at every level. From crime to court there will be improvements to quality standards, effectiveness and efficiency by:

- Providing tools and methods that are robust and assessed for accuracy for quality assurance;
- Following the 'validate once verify many' methodology for a more efficient and achievable approach to validation;
- Enabling a national network to share learning, knowledge and experience;
- Delivering a single online quality management system, accessible at point of need;
- Building a standard approach to accreditation.

These steps will provide the public, the courts, practitioners and investigators with the trust, confidence and assurance that independent assessment to external quality standards brings.

In conclusion

In this strategy we propose a national 'whole system approach' to build a sustainable, future-proofed DF Science service to deliver the capabilities we need where we need them. DF science capabilities must help policing to outstrip and deal with the criminal threats wherever they come from, keeping pace with rapid technological advances and denying criminals the chance to exploit them. We propose a collaborative approach to establish a nationally-networked service cutting across all the themes in this strategy and which provides



a comprehensive response to the issues and challenges we identified at the outset.

Although an essential part of DF science, technology alone cannot deal with the challenges or solve the problems we face. We need a consistent, collaborative approach to our big challenges – volumes, complexity and legitimacy. It will take more than technology alone to deliver a rapid, quality assured digital forensic service nationally. Policing must come together on common ways of working. We need a cultural shift in practice, supported by strong governance, if we are to build this national response to support DF science to deliver effective and efficient service.

The scale of change we need across DF science means transformation will take time. So we propose to take a 'twin track' approach, combining TF activities which support longer-term change with 'quick wins' delivering rapid operational benefit to DFUs and policing. Everyone involved will collaborate closely with partners to ensure we deliver measurable improvements in service and benefits to the CJS, as well as ensuring all activity supports and

contributes to long-term DF science transformation.

Through more rapid and responsive DF services, this transformed capability will deliver better investigative outcomes, prevent and detect more crime, reduce harm, safeguard victims, and increase legitimacy and public confidence. It will embed a quality-first approach with a strong ethical foundation to maintain public confidence and trust, and bring innovation and cutting edge technology to DF science, building a continually improving service to tackle whatever challenges the future may bring.

This is an exciting vision for DF science and we can make it a reality in the next five years. We envision a world where evidence is secured quickly and efficiently for investigations and intelligence, and shared securely with prosecutors and disclosed fairly to the defence; where more sensitive and trusted ways of working improve the experience for victims and witnesses; where quality, accuracy and rigour mean that we deliver the best possible service to the Criminal Justice System and to the public we serve.

Introduction

Digital forensic science – the examination of digital evidence to support investigations and prosecutions, formally defined as ‘the systematic and coherent study of digital traces to address questions of authentication, identification, classification, reconstruction, and evaluation for a legal context’^{1,2} – is a once niche capability which is now mainstream. Over 90% of crime is already recognised as having a digital element³, and with the acceleration in use of technology in society we conduct more and more of our daily lives online, so the critical role digital forensic science plays will only continue to grow. This shift creates huge opportunities and presents corresponding challenges for policing. This strategy has been developed to address these challenges.

¹ Based on the definition in OSAC Technical Series 0002R1, ‘A Framework for Harmonizing Forensic Science Practices and Digital/Multimedia Evidence’, published by the US National Institute of Science and Technology (updated 2019): https://www.nist.gov/system/files/documents/2018/01/10/osac_ts_0002.pdf.

² A detailed definition of digital forensics is given by the UK Forensic Science Regulator in her Codes of Practice and Conduct (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/680708/Codes_of_Practice_and_Conduct_-_Issue_5.pdf).

That definition is intentionally wide, with explicit exclusions listed, as it aims to capture all activities which are in scope for regulation. The NIST/OSAC definition used here is complementary to the FSR’s definition, which in full is: ‘Digital forensics is the process by which information is extracted from any digital system or data storage media, rendered into a useable form, processed and interpreted for the purpose of obtaining intelligence for use in investigations, or evidence for use in criminal proceedings. The scope below includes aspects such as remote storage and systems associated with computing, imaging, image comparison, video processing and enhancement (including CCTV), audio analysis, satellite navigation, communications. The definition is intentionally wide, and any exclusions will be explicit. The following should be conducted by competent staff using methods approved by the organisation, but are excluded from the ISO 17025 digital forensics accreditation requirement: automatic number plate recognition, manual classification of indecent images of children, eFit, recovery from a working CCTV system, CCTV replay for viewing with no further analysis (acknowledging that there may be quality limitations to the material viewed). Extraction of data from cameras used at incident scenes is not included in this scope; when performed, it is part of incident scene recording.’

³ As stated by Mark Stokes, quoted in the House of Lords report ‘Forensic science and the criminal justice system: a blueprint for change’, <https://publications.parliament.uk/pa/ud201719/ldselect/ldscitech/333/333.pdf>

Our starting point

The NPCC commissioned and owns this Digital Forensic Science strategy. It builds on the National Policing Digital Strategy (NPDS), which vividly brings to life the opportunities and challenges for policing in the digital age, and supports the Digital ambitions and priorities for policing identified in that strategy. In doing so, we draw on parallels with the strategy and show how those priorities relate to digital forensic science. We will identify the unique challenges to providing digital forensic science capabilities and lay out how we will address them. In doing so the strategy supports the aims and objectives of the Policing Vision 2025.

Traditionally, Digital Forensic Units (DFUs) have delivered DF science services. But the role of DF science is expanding outside the forensic laboratory or DFU and with devolving DF capability to support wider investigative requirements, much digital forensic work is now conducted by investigators and front-line operational staff. Recognising this, this strategy considers the needs of DF science across the criminal justice system, from crime scene to courtroom. It also acknowledges the broad scope of DF science capabilities, from more usual computer and phone analysis to media forensics, cell site analysis and additional specialist capabilities. We acknowledge the increased scope of DF science, but we are clear that not all those involved in these activities are scientists or practitioners. Rather, digital forensic science is a ‘golden thread’ running through the investigative process. This can be delivered through the specialist skills and capabilities

of DFU staff, or by a trained user outside a DFU following a method and tool which has had DF science expertise embedded into the process. We will outline this further in the strategy.

New possibilities in a changing landscape

The insights DF science can bring to an investigation are unique in forensic science disciplines; society’s pervasive use of technology gives new power to DF science, allowing phones, computers and even smart speakers, watches or doorbells to act as ‘digital witnesses’ to what happens in daily life. We can get rapid insights from DF analysis which in the past could have taken months of physical surveillance. It also gives unprecedented access to someone’s innermost thoughts from the content of conversations, or search histories. If policing is to use this ability, it is vital it does so responsibly and sensitive to the ethical issues that arise.

As well as new investigative opportunities, advances in technology offer opportunities to expand DF services. Rapid growth in cloud services will allow us to simplify and rationalise DF data storage. These same cloud services allow investigations access to more processing power, to harness the power of automation and explore the potential of new and evolving technologies such as machine learning. But policing in the UK is neither organised nor funded to seize these opportunities. To allow policing to unlock the enormous potential of technology, forces need to coordinate effectively, something we explore in this strategy.

Here and now

To illustrate the scale of services digital forensics provide, police forces in England and Wales spent c.£120m on digital forensics in 2019/20⁴, with the equivalent of 1500 full-time staff (FTE) working in frontline roles in DFUs⁵. £17m of this was on hardware and software, with £10m on the costs of achieving accreditation to quality standards.

As a guide, the average DFU⁶ processes 930 computer items and 5000 phone items annually, with an average turnaround time of 10 weeks for phones and 17 weeks for computers. It will have a queue of 120 computers and 160 phones, with the oldest item being in the queue for eight months; for urgent cases, items can be turned around in about a week. Every year it processes and stores 250-350 TB of data.

In November 2019 all 40 DFUs responded to a digital assessment survey from which we have extracted these headline findings. Those responses helped to define the state of digital forensics in England and Wales for the first time.

⁴ The estimate of £120m is mainly based on the Digital State Assessment (DSA). This was a survey carried out in November 2019 of every DFU in the 43 territorial forces. This has been validated against other data, like the Police Objective Analysis, and other sample-based research, and is the best available up to date assessment of police spending on digital forensic science.

⁵ This covers ‘mainstream’ digital forensic activity, and does not include Regional Organised Crime Units (ROCs), the National Crime Agency (NCA), British Transport Police (BTP) or specialist provision such as counter-terrorism units (CT), nor does the FTE estimate include all DF activity performed outside DFUs, such as frontline operation of self-service kiosks, or the roles of digital media investigators (DMIs).

⁶ This summary is a description of a ‘typical’ force DFU. For this description the five largest force DFUs across England and Wales have been excluded. The remaining 35 force DFUs represent 60% of recorded crime, ranging in size from 0.6% to 3.7% of the total.

⁷ For example, Gartner Research predict a twenty-fold growth in mobile network data transmissions over the next five years (Gartner, ‘Digital Forensics – Future Challenges’, 2019).

⁸ <https://www.justicespectorates.gov.uk/hmicfrs/wp-content/uploads/peel-spotlight-report-diverging-under-pressure-2018-19-overview.pdf>

⁹ Ibid

¹⁰ Gartner, ‘Digital Forensics – Future Challenges’, 2019.

¹¹ Based on force responses to the Digital State Assessment

Meeting the challenges

Research carried out by the Transforming Forensics Programme (TF) to inform this strategy identified three ‘core challenges’ which are intrinsic to the growing demand for DF examinations. Tackling these requires an approach which delivers continual improvement, with the capacity to grow to meet these challenges in future.

Core challenge 1: Volume

The increase in use of digital technology has led to exponential growth in demand for DF examinations. The underlying demand, driven by the growth in numbers of devices, better communications and increased use of cloud storage, has been rising by 11-16% over the last few years, and this is projected to continue⁷. This has led to backlogs and delays to investigations ranging from a few months to a year and a half⁸. Her Majesty’s Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) PEEL (police effectiveness, efficiency and legitimacy) reviews identify these backlogs and delays as a consistent theme across all forces⁹. They directly impact victims, witnesses and suspects, who must wait not only for the outcome of investigations but in many cases for their devices - retained for digital examination - to be returned and increases the risk of harm to the public by delaying bringing offenders to justice. The majority DFU work is complex because of the level of risk involved - most of it involves child sexual exploitation (CSE) investigations and other serious crime - so managing the demand is complex. Police focus proactively, and rightly, on these



crimes to reduce the harm they cause, but this also generates more demand on DFUs.

Core challenge 2: Complexity

As well as the growing volume of submissions, digital examinations themselves present an increasingly complex challenge. There are more types of device to examine, more end-to-end encryption and more varieties of data formats, with an increasing proportion of data stored in the cloud. The ‘Internet of Things’ is growing rapidly - by 2025, machine to machine interactions may exceed traffic from human interactions¹⁰. This means we need to develop new techniques simply to maintain DF capabilities to extract and analyse information, to avoid the criminal justice system being cut off from critical sources of evidence in future. Yet there is limited capacity in force DFUs to carry out research and development (R&D) to develop innovative techniques¹¹, and very few forces have access to external research support.

Core challenge 3: Legitimacy

Public awareness of personal data privacy is rising. Although the



public are broadly supportive of police using digital forensic analysis, recent issues around disclosure and consent for digital device examinations have brought digital data handling into the public eye.¹²

Meeting the challenge of rising data volumes, encryption and cloud storage means policing needs to adopt new ways of working and it is crucial to maintain public trust and confidence in the process. Policing needs to work proactively with Government to ensure the legislative and ethical frameworks on which these activities are founded are right for the digital age.

¹² Public attitudes on digital forensics', research carried out by Revealing Reality on behalf of Transforming Forensics, March 2020

¹³ FSR evidence to the HoL Science and Technology Committee, 2019 (<http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee-lords/forensic-science/written/96445.html>)

In addition, there are several other pressing issues this strategy seeks to address:

Issue 1: Lack of support services

DF services have grown up organically within forces over the last twenty years, and often operated in relative isolation, without the support of force ICT departments to manage networks or procurement teams to assist in purchasing and managing contracts. The approach to procuring devices, IT and services is often inefficient, and does not support interoperability and seamless connectivity. The fragmented development of digital forensics from a 'cottage industry' to a key investigative support function has happened outside many forces' corporate IT arrangements

and as such the organisational responsibility for the funding, management and provision of these IT services is unclear, resulting in essential and basic services not being provided to DFUs. As a consequence, DFUs often lack core tools such as case management systems to help them manage their activities.

Issue 2: Fragile commercial marketplace

The Forensic Science Regulator (FSR) has highlighted that reductions in funding for forensic science as a whole have led to a substantial reduction in the size of the supplier market, and that 'the potential for further major exits from the market and/or loss of a range of disciplines hangs in the balance'¹³. DF services within policing rely upon external suppliers providing additional capacity and expertise; without action to put this market on a sustainable footing, and maintain access to external DF services, policing will be left with insufficient internal capacity to cover the gap¹⁴. This risks growing backlogs and failing to harvest critical intelligence, data and evidence.

Issue 3: Limited strategic engagement with partners (academia and industry) to work on long term solutions

The lack of coordination between forces limits policing's ability to build strategic relationships with academia and industry to develop and access new capabilities. Some larger forces or regional collaborations have attempted this on an individual basis, but in the absence of a national approach, this is inconsistent and risks

being repetitive and inefficient. Research and development (R&D) is uncoordinated and unshared, meaning policing is slow to take up new capabilities which already exist¹⁵, and over time will erode policing's ability to exploit digital data sources to support investigations and successful prosecutions.

Issue 4: Recruitment and retention

Recruitment of experienced digital forensics examiners is an ongoing issue for all forces. There is a finite pool of experienced professionals from which to draw, and forces must compete both with DF recruitment in the private sector, and with the growing market for cyber security roles where there is substantial crossover with DF skills. But these roles come without the potential exposure to distressing child exploitation material and the pressures of working in a very demanding environment, dealing with backlogs which can extend over months and which impact staff morale. As demand for digital examiners has grown, most forces have open positions for staff that they are finding very difficult to fill.¹⁶ Retaining existing staff is also a challenge exacerbated by a lack of formal career pathways and variable access to training and professional development opportunities.

Issue 5: Lack of DF Science awareness within policing

Capability for straightforward data extractions from mobile devices, and remote review tools allowing investigators to review the output of digital forensic examinations, are now available to the frontline. Frontline officers, first responders

and investigators often deal with many different sources of digital evidence, where the evidential value of each may not be clear; they need a base level of understanding to ensure they do not miss evidential opportunities and that the value of digital evidence is properly assessed and understood when communicated into the criminal justice system. But there is no national DF training package available for these roles.

Issue 6: Embedding quality

The Forensic Science Regulator (FSR) has mandated that all forces must achieve accreditation to the ISO17025 quality standard for their forensic science activities, with an original deadline of October 2017 for accreditation of digital forensic methods. Despite this deadline, compliance is still low, with less than 20% of processes requiring accreditation having achieved it. This is not because of lack of commitment from DFUs, which are spending a significant amount of time and funding working towards implementation of quality standards. Rather, the pace at which digital forensics is changing and the lack of capacity within DFUs makes it very challenging for forces to achieve quality accreditation.

This challenge is greater when it comes to DF than any other discipline because the range of different DF data types and methods multiply the complexity of validation activity. New consumer devices are released regularly, meaning that policing needs to develop the capability to examine these new devices immediately. Unlike other areas of forensics, there is no time to do a controlled validation study before introducing a new forensic technique. The devolvement of

capabilities outside DFUs is a further challenge, as is the requirement to gain ISO17020 accreditation for on-scene work by October 2020. Forces identified validation of methods as their top priority at a TF digital forensics engagement event, as failing to gain accreditation means forces are vulnerable to challenges at court.

Issue 7: Handling of legacy data

Data handling and retention is a complex area for forces, as differing legislation, policy and guidance in this area does not provide a clear indication to forces on what DF data needs to be retained and for what period. Legacy data, generated or seized in preparation for, or as a result of, past digital forensic examinations, is stored in various offline formats and for most forces, lack of access to comprehensive case management systems and limited integration with force ICT means management and weeding of the retained data is a largely manual process. This places a significant burden on forces and exposes them to risks relating to compliance. This is an area of concern for all forces nationally, as identified from the responses to the digital state assessment carried out by TF; it is also a concern for commercial FSPs providing digital forensic services to policing, who must put their own data retention arrangements in place.

¹⁴ Gartner, 'Digital Forensics – Future Challenges', 2019.

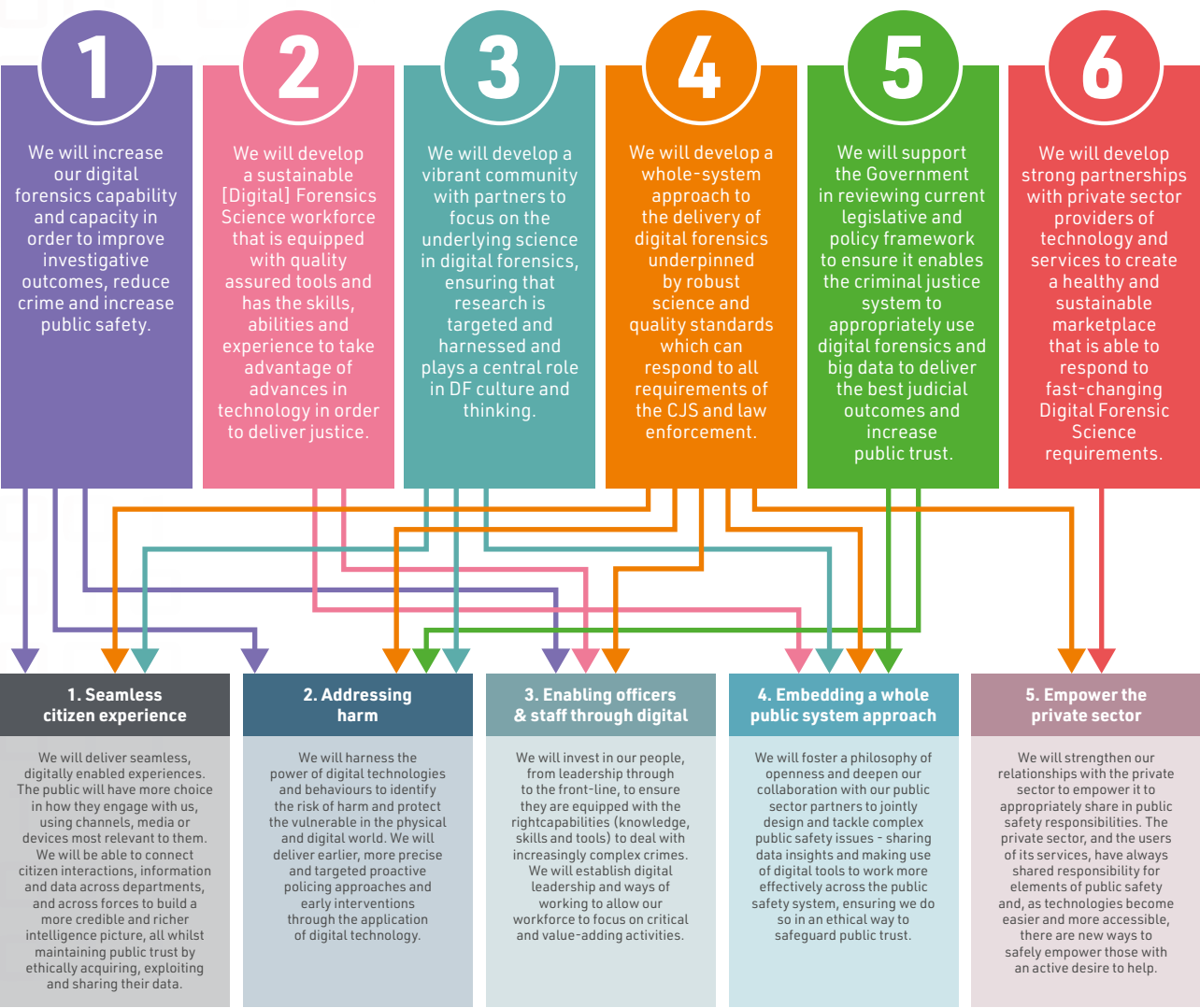
¹⁵ 'Unleashing the value of digital forensics', Police Foundation research carried out on behalf of TF, March 2020

¹⁶ Gartner, 'Digital Forensics – Future Challenges', 2019.

Strategic objectives

With these opportunities, challenges and issues in mind, we have identified the key strategic objectives for the transformation of digital forensic science in policing, empowering policing to catch up and keep up with the rapid pace of technological change.

These strategic objectives fully support and have been mapped to the ambitions and priorities of the **National Policing Digital Strategy**:



This strategy acknowledges that incremental improvements will not achieve the vision, which calls for a much more radical transformational attitude and the delivery of a nationally networked, integrated approach if we are to keep pace with a rapidly changing technological landscape. Our approach is described through five interconnected themes – characterised by the sections in this document – all of which play a key part in delivering the strategic objectives.



1

1. Improving operations

This section contributes to deliver Strategic Objectives 1 and 4:



Digital forensic services across UK policing are fragmented and disjointed. At present there are 40 DFUs serving the 43 territorial forces. Collaboration between forces, either formal or informal, is limited, and a 'typical force' DFU does not do work for others, nor does it have the capacity to do so². Individual units develop their own methods, procure and deploy their own hardware and software and manage their individual quality accreditations in line with the FSR's requirements. All of this involves substantial duplication of effort and inevitable waste of resources³. Despite this, the core functions of force DFUs have striking commonalities, and there is clear scope to standardise methods and share support services between units. To improve operational efficiency, we need to 'industrialise' and streamline this fragmented landscape, redesigning DF from the ground up.

radical shift in approach can address the operational difficulties, and that an uplift in funding or efficiency improvements through aggregation alone will not be sufficient to meet growing demand.

"How we used to do digital forensics" is no longer fit for purpose in a world where data volume and complexity have ballooned, and a substantial subset of the data required is in the cloud. Throwing massive volumes of extracted data to investigators, who generally lack the tools and methods to interrogate the data effectively, just shifts a problem; a more integrated approach could be transformative."

Gill Tully,
Forensic Science Regulator
2019 ANNUAL REPORT, 25 FEBRUARY 2020

The original 'cottage industry' operating model, which has developed over time, must be replaced with 'DF science by design', delivering a national model which is robust enough to meet existing operational challenges, and agile and responsive enough to solve the problems of the future. The TF programme's early research and analysis⁴ makes clear that only a

¹ E.g. through section 22 agreements, where forces have pooled their DF resource, with varying degrees of integration between formerly separate units.

² The 'typical DFU' analysis is based on the digital state assessment, a survey of all forces carried out by TF to capture a baseline of their current state in relation to key DF measures such as volume of submissions, staffing, technical infrastructure and specialist capabilities, in December 2019.

³ Forensic Science Regulator (FSR), Gill Tully, in her 2019 Annual Report, 25 February 2020.

⁴ From the baseline data capture conducted by TF in early 2019, capturing a representative sample of data from 8 forces.

The role the Forensic Capability Network plays

The newly established Forensic Capability Network (FCN), formally launched in April 2020, is key to improving operations, providing central support services on a national basis.

Although capabilities vary across England and Wales, there are typically three levels of digital forensic services, namely:

Level 1 - Undertaken by frontline staff or non DF Practitioners:

Frequently involving the use of self service Digital Forensics Kiosks.

Level 2 - Undertaken by DF practitioners:

Predominantly in Digital Forensics Hubs or Laboratories or by Forensic Service Providers.

Level 3 - Undertaken by DF specialists:

Predominantly in Central Digital Forensics Laboratories or by Forensic Service Providers

Improving DF operations is at the core of this strategy. Digital forensic science's fundamental role is to support policing's ongoing mission to make our communities safer, delivering responsive forensic science

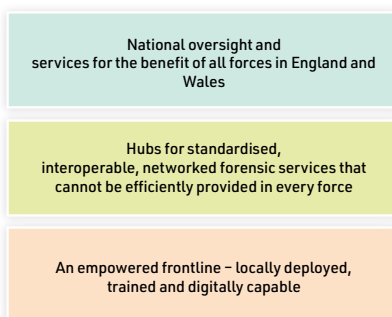
capabilities to meet the needs of the criminal justice system and empowering policing to change the way it investigates crime in the digital age. Without DF science as a core support service, policing

cannot deliver on its pressing priorities, including tackling county lines gangs, protecting children from sexual exploitation, combating terrorism and reducing serious violence.

The Forensic Capability Network

The FCN is a community of its members forensic science capabilities and expertise, comprised of a network of forensic science professionals across UK policing, a core team to co-ordinate and orchestrate forensic service delivery, and a technology platform and toolset to connect and enhance forces' existing forensic capabilities.

It will oversee and deliver transformational change as part of a proposed three-tier model:



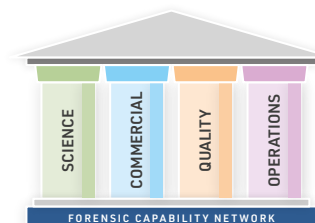
It has been designed to enable policing to work collectively to deliver high quality forensic science capabilities, to share knowledge and learning, and to improve resilience, efficiency, quality and effectiveness.

It is structured around 4 pillars, **Science** (incorporating Workforce), **Commercial**, **Quality** and **Operations**, to deliver:

a way to give effective support to NPCC portfolio leads; harmonise our collective efforts; maximise investment; transform our forensic science landscape and achieve a paradigm shift in both our individual and collective performance;

a club that we can all own and develop in the way that makes most sense to us, as those responsible for delivering policing and law enforcement outcomes to our communities;

a truly networked policing model that leaves Chief Constables and PCCs in control of what forensic science activity is undertaken and where, but creates the environment that enables FCN members and the FCN community as a whole to maximise resources, resilience and effectiveness.



Its role will be to:

Manage the market for forensic services, whether delivered by police forces or commercially

Ensure that services, from crime scene to court room, are **standardised and accredited**

Provide, directly or through commissioning, **specialist forensic services**

Enable forces to harness technological change by **co-ordinating R&D**

Increase **resilience** of forensic services and help cope with major incidents.

Core principles of future operations

This strategy proposes that in the near term TF work with forces to identify and analyse their needs and to develop the future operating model to provide DF services. This work will follow certain core principles:

Standardisation – this is the most critical principle which will enable all subsequent improvements. We cannot standardise all DF processes, so working with forces TF will identify the most common high volume processes where standardisation is possible. TF will support forces to converge on a single version of that method. This will then allow validation, process design and training development to be done once for the benefit of many, avoiding duplication of effort nationally. Once processes are standardised, it will be simpler to adopt standard technology. To that end TF are developing a reference architecture for hardware and software which in turn will cut down on procurement, deployment and integration costs. TF are also working to agree standard interfaces and data formats, where possible adopting existing initiatives such as Cyber-investigation Analysis Standard Expression (CASE)⁵ to enable forces to move away from vendor monopolies and give them the flexibility to switch out existing software components for new solutions. A key element of this will be a taxonomy of techniques, enabling structured DF service delivery. This taxonomy will enable TF to classify DF techniques to identify where they overlap and ensure forces have consistent approaches, mapping

capability nationally and identifying capability gaps.

Automation/industrialisation – once we have standardised it, we can then automate a process, and where this process is high-volume with low variability, there is the potential to make significant efficiency gains. The TF programme ran a number of proof-of-concepts which demonstrated that industrialising manual processes can deliver capacity increases of up to 30%, reducing turnaround and hands-on time by eliminating repetitive manual process steps. There are other benefits too, from inbuilt auditing, improved consistency and the reduced risk of human error, to improving staff wellbeing by avoiding exposure to distressing material in investigations involving child sexual exploitation (CSE). There is wide support in the DF Community for industrialising volume methods. 97% of respondents at a TF engagement event supported doing so⁶.

Providing and coordinating services centrally – the FCN will be able to deliver a number of supporting and/or specialist services in future, following the principle of 'doing things once for the benefit of many'. This includes validating centrally (conducting or coordinating validation testing, as determined through consultation with forces) and providing support procuring DF services, tools and equipment. Developing the DF operating model will demonstrate which services are suitable to provide nationally and which policing should continue to deliver locally, but at Table 1 below we detail some design considerations. A forensic information ecosystem will be at the core of this coordination, enabling forces to task and manage resources

Improving our response to county lines crime

Improving the operating model for digital forensic services will support coordinating investigations across forces and areas. This is particularly useful for county lines investigations spanning different regions.

The FCN's forensic information ecosystem will help identify which forces or areas hold relevant information so that an investigator will be able to see that there have been previous linked cases and make enquiries to the relevant force(s). Once common ways of working are agreed, investigators will receive the relevant data in a standard format with which they are familiar. This will allow the officer to review it easily as part of the investigation, using methods and tools standard across forces.

When an officer identifies a new, time critical line of enquiry linked to, for example, other victims from a new geographical area they can use the tasking and coordinating capabilities the FCN will provide to request rapid DF support in that region.

They will also be able to link in cell site information from call data records to add to the evidential package, because a standardised information architecture simplifies sharing digital evidence, including with the CPS. This will help make sure evidence presented at court is clear and compelling. Rapid forensic support will transform the speed of the investigative response, how comprehensive it is and consequently help protect further victims from harm.

- this is fundamental to managing centrally provided services successfully. It will also generate useful management information to assist policing and monitor progress towards improving service delivery.

⁵ Cyber-investigation Analysis Standard Expression (CASE) is a community-developed evolving standard that provides a structured (ontology-based) specification for representing information commonly analysed and exchanged by people and systems during investigations involving digital evidence.

⁶ From live online feedback gathered from attendees during the event (December 2019).



Providing DF services at the point of need, a tiered model – most forces have already moved towards providing DF capability at the front line through self-service kiosks which enable trained officers to extract data from mobile devices by following a locked-down workflow.

Some forces or regions have also implemented a 'hub model' to centralise some of their more specialist capabilities in a single location, while continuing to provide standard DF capability at multiple sites. With a tiered model, the more highly skilled and trained DF specialists are located centrally and focus on developing processes and new techniques, as well as dealing with complex casework, while less specialist technicians or analysts carry out the day-to-day work. This ensures that the appropriate person does the appropriate tasks, it provides value for money and, importantly, it forms the basis

for developing a career structure and providing opportunities for development and progression. For this model to work effectively learning and information must flow between the tiers in both directions, i.e. the lower tiers escalate more complex requirements for support where they need it, and those in the specialist tiers disseminate knowledge of novel techniques and leading practice from the central labs to hubs and the front line.

Through this structure, policing will be able to control how front-line methods are configured and doing so will ensure that all methods adhere to quality assured processes. For example, to support devolved capability for triage, the FCN will 'package' this accompanied by guidance, training material and standard operating procedures (SOPs) for easy to use deployment at level 1. To support this model a knowledge base will be essential,

as well as an infrastructure which enables everyone to collaborate and give or receive remote support.

Cloud first - this principle applies to all public sector IT, and providing DF services through the cloud could be truly transformational. The FCN Xchange will be the first nationally accredited cloud platform to store and analyse operational police data. The FCN Xchange is scalable by design and it could extend to DF. Once tools have been tested and validated nationally, the Xchange can make them accessible for local use. As the National Enabling Programmes' standards roll out, it will become easier for police forces to join the FCN Xchange and to use the standard support tools and toolsets they will provide. In future, those handling urgent, high profile cases should be able to access additional processing resource through the cloud to speed up analysis and access case data remotely, regardless of where that data is acquired, facilitating national collaboration. But digital forensic data presents unique challenges because of its sensitive nature. This means that before we can decide conclusively what potential there is to use cloud storage for digital forensic data it will be important that ethical and legislative requirements are considered in detail and met fully. This is discussed in more detail later in the strategy.

Evidence based – to develop a robust operating model, sound science and evidence must underpin all design decisions. This principle has been fundamental to the activity to inform this strategy to date, which we have based on research commissioned from industry, academia and policing. TF have used the initial

information they collected from forces to develop a simulation model to explore how various interventions impact DFU performance. TF will further refine this simulation model to support decision-making as the new operating model develops. In future, testing new technologies and approaches in the field before deploying them more widely will be key to learning useful lessons to increase the success of wider rollouts. To support this, TF have developed a toolkit for forces to use to maximise the usefulness of information they capture from

future field test deployments. The toolkit and simulation model will be resources which the FCN can draw on to provide evidence-based business change support to forces, alongside management information to track success. This will enable the whole community to learn from good practice, so innovation at a case and DFU level is promulgated and shared to continually improve the overall operating model.

The most essential element of this is establishing clear and collaborative governance structures for future DF

activity. Pooling sovereignty will be essential to maximise the benefits of joint working through the FCN, and forces must prioritise agreeing DF science governance arrangements as part of the new operating model. The FCN will work in partnership with policing and with government to support the development of proposals for the governance structures, and will work with existing governance to embed them successfully.

LOCAL	REGIONAL/INTERMEDIATE	NATIONAL
Local provision lends itself to operational DF services where: • Volumes are enough to justify maintaining expertise locally • Speed of response to local incidents is important (e.g. DFU staff attending crime scene) • There is a need to provide convenience to customers (e.g. facilities for officers and legal teams to access evidence) • There are high transport costs or slow transport times (e.g. to access ingestion facilities for physical evidence) • There is a need to meet local priorities (PCC choices)	Regional collaboration is appropriate where regional scale is the natural unit of organisation, this can be where: • There is a strong connection with other regionalised functions (e.g. ROCU, CT) • Crimes or incidents commonly cross force borders • There are specialist tools and techniques where demand is insufficient to maintain in every force, or the competency is held by a small community of highly specialist technicians (e.g. complex analytical techniques such as specialist on-site acquisition or RF analysis, or emerging technologies) • Achieving the change to a national provision is impractical in a single step Regional collaboration can form the basis for hub-and-spoke organisational models and may form a logical stepping-stone on the road to wider national collaboration.	However, there is a strong case for managing some services nationally: • Where economies of scale continue to increase with size (e.g. data storage) • Where development can take place once and be shared across all forces (e.g. standard operating procedures; method validation; forensic information ecosystem; quality management system; research & development; training curriculum; competency frameworks) • To achieve strength in numbers e.g. advocacy to FSR and UKAS, negotiations with suppliers • To provide standard functions where there is little policy variation (e.g. contract management) • Least frequently used specialist functions e.g. X-ray analysis of damaged chips • Where there are low or zero transport costs (e.g. digital evidence from internet/cloud-based investigations) • Crime or incidents are borderless or national in scale • Integration with other national function or service e.g. College of Policing; national contingency planning.

TABLE 1 DESIGN CONSIDERATIONS FOR LOCAL/REGIONAL/NATIONAL ELEMENTS OF AN OPERATING MODEL

Benefits

Strategic benefits:

- Swifter access to justice for victims, improving victim satisfaction
- Increased willingness to report crime, by avoiding the need for victims and witnesses to give their devices to police for a lengthy investigation
- More rapid and responsive DF service enabling early disruption of offending, safeguarding victims and witnesses
- Effective collaboration on methods, technology and infrastructure, avoiding duplication of effort nationally and achieving best value for the public
- National capability accessible to all – including rarely used and specialist niche methods – increasing access to specialist capability for forces and improving ability to bring offenders to justice
- Centralised provision and coordination of services (e.g. procurement and validation), improving efficiency
- Proportionate and consistent ways of working that can achieve compliance with FSR requirements, the General Data Protection Regulation (GDPR) 2016 and the Data Protection Act (DPA) 2018, reducing risk to forces and improving trust and confidence
- Industrialisation of manual processes to deliver capacity increases, improving accessibility of DF services to policing

Tactical benefits:

- Elimination of manual rekeying and transfer of data between tools and systems, reducing risk of error
- Reduction in backlogs through industrialisation, offering improved capacity for examinations and quicker turnaround times
- A more proportionate investigative response through use of triage and a tiered model
- Closer and more integrated working with investigators – to deliver quality assured evidence at the point of need
- Avoiding exposure to distressing material through automation of processes
- Access to a knowledge base available nationally enabling collaboration and remote support

Colour code for timescale for delivery:

Short term activity	0-18 months
Medium term activity	18-36 months
Long term activity	36-60 months

Code for assigning responsibility:

- R – Responsible
Does the work to complete the activity
- A – Accountable
Accountable for completion of activity
- C – Consult
Provide information for the activity
- I – Inform
Kept informed of activity progress

⁷ Work already underway by DSTL in conjunction with FSR as part of development of ground truth datasets.

⁸ Shared responsibility between College of Policing and FCN

⁹ Will require cross-government engagement, including Home Office and Ministry of Justice

¹⁰ This work is currently underway through the Cyber-investigation Analysis Standard Expression (CASE) project.

Key steps towards delivery

ACTIVITIES	TIMESCALE	TF	CORE FCN	NPCC / APCC	FORCES (FCN MEMBERS)	OTHER
Analyse forces’ DF Science needs	S	R	A	I	C	I
Design the future operating model	S	R	A	C	C	I
Standardise priority methods and processes	S	R	A	I	C	C
Develop a taxonomy of techniques	S	A	C	I	C	R ⁷
Map national capability and identify capability gaps	S	R	A	C	C	C
Consult with forces to develop an approach to central validation	S	C	RA	I	C	C
Develop a knowledge base	S	C	RA	C	C	R ⁸
Issue a toolkit for forces to maximise benefits from future field test deployments	S	R	A	I	C	I
Refine the DFU simulation model to support decision-making	S	R	A	I	C	I
Design the ‘whole-system’ strategic level governance model	M	I	C	R	C	RA ⁹
Develop a reference architecture for hardware and software	M	R	A	I	C	C
Development of standardised data formats	M	C	C	I	C	RA ¹⁰
Deliver central support services for validation and procurement	M	C	R	C	A	C
Implement a future operating model	M/L	R	A	C	R	C
Develop a Forensic Information Ecosystem (FIE) platform to facilitate coordination between forces	M/L	R	A	C	C	C
Develop management information reports from the FIS	M/L	R	A	C	C	C
Design and implement the infrastructure to enable collaboration	M/L	R	A	C	R	C

2

2. Improving commercial practices and R&D

This section contributes to deliver Strategic Objectives 3, 4 and 6:



To transform how we deliver digital forensic service, policing needs to draw on all the resources available to it, taking full advantage of the potential offered by engaging with industry and academia if we are to innovate to keep pace with criminality and technology in the way we need to. The recent House of Lords Science and Technology Committee inquiry into forensic science in the UK¹ highlighted that policing could not solve the problems or deal with the structural challenges that affect DF service delivery in isolation, but needed to act in partnership. Private sector providers are essential to delivering DF service and key to a nationally networked approach. So too are other organisations – including higher education institutions, specialist research organisations, start-ups and existing DF tool vendors - which can support innovation in the future.

Industry

Commercial suppliers can work with policing on digital forensic science in two main ways:

- **Forensic service providers** can support forces to manage their casework demand by carrying out digital forensic analysis for them;
- **Forensic tool vendors** can provide the specialist hardware and

software policing uses for forensic examinations, both to policing and to private providers. This is key to developing new capabilities.

There are other commercial relationships with suppliers such as training providers or those who provide quality accreditation support services. Developing a strategic approach to engaging with all these organisations will be part of the work the FCN Commercial pillar undertakes – and will be central to the Forensic Marketplace Strategic Plan the FCN is developing in conjunction with the NPCC Digital Forensics Market Operations Group.

Coordinating requirements

The fragmented way in which DF service is delivered is most obvious when we look at commercial engagement. The 40 DFUs all act separately and the end result is that policing presents a complex market for providers to serve, especially in face of more than 40 sets of requirements and different business contexts and priorities into which providers and vendors deploy or sell their products. Providers have to take a different approach to integrating their products into the processes and infrastructure that exist in each force. Even small differences can increase the complexity and cost to both policing and suppliers. Agreeing on a standard approach to coordinate their requirements will make the process significantly more efficient and cost effective for both.

By coordinating and agreeing its requirements jointly, policing will be a single 'intelligent customer' and able to harness its buying power effectively. So too commercial providers will benefit, from the reduced cost of engaging when

¹ Forensic science and the criminal justice system: a blueprint for change, <https://publications.parliament.uk/pa/ld201719/ldselect/ldsctech/333/333.pdf>

they respond to tenders, but also because it will be significantly less complex and costly to install and configure their products/services into a standard environment than into multiple slightly different operating environments. This strategy proposes that the Digital Forensics Market Operations Group (DFMOG), supported by the FCN Commercial pillar, play a key role to capture and manage forces' requirements. It also proposes that the FCN Commercial pillar take the lead in developing model clauses for future contracts and standardising the approach to take in specific areas such as standards and accreditation, business continuity, data protection, vetting, cyber security and data storage and retention. With this in place, the FCN Commercial pillar will also be able to develop efficient routes to market for policing, using the most appropriate procurement approach for best value. FCN Commercial will also award contracts and frameworks where FCN members ask them to do so. The FCN will be responsible for the overarching performance of such frameworks. They will also manage suppliers when forces award contracts under FCN frameworks and support forces to deal with any issues that arise with those suppliers.

For forces to meet existing and future DF challenges they need a flexible and responsive way to engage with commercial providers. When we develop a new commercial approach there are many important considerations. Any commercial approach must ensure vendors cannot 'lock' forces in so we will need

to be explicit in all future contracts about the need for interoperability and open standards. Small, innovative organisations should be encouraged to provide policing with their services, especially specialists in key emerging areas such as artificial intelligence and machine learning. Existing procurement processes favour large, long established companies, but in the future policing should have access to the full range of technological innovation across the market. This should be an area of focus for FCN Commercial, and considered within the forthcoming Forensic Marketplace Strategic Plan.

By coordinating their DF requirements internally policing will be able to engage with the commercial sector more strategically and effectively in the longer-term. They will be able to provide a clearer understanding of their collective need and free up resource for long-term planning, where two key areas of focus will be vital: firstly a focus on forecasting the demands policing is likely to make of FSPs in the future and secondly horizon-scanning to identify what challenges DFUs are likely to face, so that policing can help inform the work that vendors and FSPs do to develop new tools and techniques. The FCN will also support this coordination between tool vendors by encouraging them to set-up a vendor group for DF science collaboration.

There is an important point on budgets we need to highlight here: to take advantage of these new technology opportunities including cloud storage and everything we recommend in this section, policing will need to find a more flexible funding model when it comes to capital versus revenue spending.

Strategic engagement with forensic service providers

The commercial FSP market has changed dramatically over the past fifteen years. Originally developing rapidly and in tandem with the growth in demand for DF analysis, the market shrank in reaction to reductions in forensic budgets across the country because of wider police budget constraints.

The FCN Commercial team and DFMOG aim to stabilise this market and put it on a sustainable footing. But to achieve this, policing will need to agree on what it will require from FSPs in the future and the balance of demand between in-house and outsourcing services nationally. At present, this balance of demand varies from force to force, with some aiming to carry out all their work in-house, and others using external providers more. The nature of demand varies too, with some forces using FSPs for routine analysis, and others using them for specialist services which they cannot provide in-house. Because the work is specialist and because of the need to maintain quality accreditation and security vetting it is impractical to recruit and deploy staff quickly to grow capacity rapidly. The unpredictable shifts in demand create serious challenges for external FSPs. The Forensic Marketplace Strategic Plan should ensure that in future the demands to be made of FSPs be coordinated across policing to make it easier for FSPs to plan the services they will provide, and the role of FSPs will be a key consideration in developing the future operating model. Forces and PCCs will need to agree a broad national approach. This presents a challenge within the existing governance framework, so



it is key to focus early on developing proposals for a governance approach which could enable this commercial coordination.

Strategic engagement to develop capabilities

In-house and external digital forensic services depend on digital forensic tools extracting and analysing data from the diverse range of sources available to DF. New devices such as

in-car entertainment systems, smart watches or other 'Internet of Things' devices present new challenges. We also have to continually improve capability to deal with changing demands, for example meeting GDPR requirements and the need to be proportionate when extracting data from victims' and witnesses' devices. If we coordinate horizon scanning through FCN Science and FCN Commercial it will focus vendors' efforts to address the challenges

policing anticipates it will face. It also creates the opportunity for strategic engagement and collaboration to develop new capability in the longer term, including with law enforcement partners such as the National Crime Agency (NCA), counter terrorism or immigration enforcement, Her Majesty's Revenue and Customs (HMRC) and the Serious Fraud Office (SFO). This will include, where appropriate, strategic engagement with device manufacturers to better

inform and develop digital forensic analysis capabilities for those devices in future, which will enable policing to anticipate and prepare for future technology demands.

Research and development

R&D is critical to driving continuous improvement when it comes to delivering DF services, especially since both the forensic technology and the technology under investigation evolve so quickly. If we are to seize available opportunities, we must improve and scale up how we coordinate and collaborate so we can implement innovative techniques more quickly.

This strategy proposes that the FCN Science Pillar coordinate dedicated support to influence national R&D. This includes both casework-driven DF R&D within policing and outreach, engaging with academia at a strategic level via UK Research and Innovation (UKRI). FCN Science will lead on planning, managing and coordinating a sufficiently well-funded R&D and innovation programme that supports short and longer term needs as well as national and force level requirements. This work needs to map the research landscape, define areas of research need and work with UKRI to identify future funding streams and opportunities to address them. Continuing engagement with casework-based, practitioner-led R&D within forces, will allow FCN Science to link wider research activity back to operational policing requirements, ensuring it maintains an emphasis on delivering benefit for digital forensic science. It will be an important principle that all R&D informs our collective knowledge.

This work will also focus on identifying cross-disciplinary research which we may be able to apply to digital forensic science, and support 'rapid operationalising' research or technology into the digital forensic science environment. Should we identify a technique of operational benefit, FCN Science and Quality pillars will work together to coordinate testing, validation and development to quality assure the technique for policing to use and ensuring it adheres to quality standards.

To facilitate coordination, this strategy proposes creating one or more innovation hubs, either physical or virtual. As we outline in table 1, these will serve as regional hubs or the basis for groups of forces to work together, providing services that are uneconomic to provide in individual forces. They will centralise capabilities and be the route to draw in support from partners in academia and industry, to collaborate on challenges, opening up spaces for small suppliers to engage with policing to test new technologies and capabilities. In this, they will function as a business incubator or 'catapult centre', where businesses, scientists and engineers can work collaboratively on late-stage R&D to transform high-potential ideas into new products and services. They will also act as a central point to link with R&D ongoing as part of other national programmes and initiatives, including coordinating with the Capability Improvement Hub that the Digital Intelligence and Investigation (DII) programme within the College of Policing is developing.

To help identify capability gaps and opportunities and to help paint a full strategic picture of national R&D we

propose establishing an academic advisory group inside the FCN Science pillar to provide independent advice and guidance. This group should have representatives from operational policing, academia and other research organisations, including the Defence Science and Technology Laboratory (DSTL), other specialist areas of law enforcement such as the Accelerated Capabilities Environment (ACE) and Data Communications Group (DCG) and organisations such as the Forensic Science Regulator (FSR) and Information Commissioner's Office (ICO).

To achieve all this, there will need to be sufficient funding to support R&D. At present, funding for DF R&D nationally outside policing is limited². DSTL receives limited funding for both in-house and externally commissioned R&D from the Home Office. The Home Office (Office for Security and Counter-Terrorism) also funds some DF research and development through its Science and Technology Unit, and the EU Horizon2020 programme has funded some DF projects, with some UK participation.

FCN Science will build on this in future. It will support and influence funding bids through a range of routes, including the UKRI Board and through Home Office Science, and develop reciprocal agreements with universities, as well as continuing to work to identify and secure additional R&D funding. Engagement at a national level will continue to raise the profile of DF research, and FCN Science will shape a national R&D and innovation programme to coordinate available funding and drive research activity in this area.

Benefits

Strategic benefits

- Reduction in lead time for new techniques resulting from a joined-up approach, enabling policing to keep pace with technological advances and improve investigative and CJS outcomes
- Engagement with service providers and tool vendors to effectively coordinate development of new tools and techniques, increasing capability available to policing and delivering best value for the public by reducing duplication of effort
- Standardised approach to requirements delivers procurement cost efficiencies, doing once for the benefit of many
- Standardised ways of working simplify implementation of new technologies
- Engaging strategically with FSPs to shape future service requirements will deliver a more sustainable FSP marketplace, providing a more resilient and efficient DF service
- Single intelligent policing customer to harness collective buying power
- Central support with overarching performance and management of suppliers under FCN frameworks, reducing overhead for individual forces and ensuring more effective supplier management to improve delivery
- Dedicated support to influence national R&D, increasing DF R&D nationally to build capability
- Academic advisory group providing independent advice and guidance, to ensure policing can access full potential of ongoing R&D

Tactical benefits

- Innovation hubs to centralise expensive or least frequently used techniques, widening access to innovative capability for all forces
- Reduced outsourcing costs and improved turn around times on casework.
- Engaging with DF tool vendors to stimulate technology developments against nationally agreed requirements

² In comparison with similar areas, such as cybersecurity, where national funding is available for Centres of Excellence (<https://www.ncsc.gov.uk/information/academic-centres-excellence-cyber-security-research>)

Improving our response to serious crime

We need to use a range of specialist capabilities to identify and extract digital evidence in serious crime and terrorism investigations. To develop state of the art capabilities effectively, policing must engage with partners to understand what the state of the art is and what innovation is going on. Hackathons or similar challenges provide a collaborative environment to work on joint challenges, bring policing, industry and academia together and can spark new ideas which can grow into innovative new capabilities, such as video analytics of crowd behaviour to support real-time incident response.

<https://www.gov.uk/government/publications/dasa-real-world-incident-response-hackathon-information-sheet>

Benefits in practice

In a proof of concept, TF worked with the East Midlands Special Operations Unit (EMSOU) and two tool vendors to streamline how two of the unit's core tools integrated. In collaboration, the vendors developed new capability to automate data transfer, replacing a process which had 27 separate manual steps. The new process

allows data extracted from mobile devices to be automatically ingested into the system which processes it for officers to review. The integration the vendors developed through this collaboration is widely applicable and is now available commercially to all forces. Working closely with forces allowed the vendors to focus on what the forces needed and on successfully developing that product.

Key steps towards delivery

ACTIVITIES	TIMESCALE	TF	CORE FCN	NPCC / APCC	FORCES (FCN MEMBERS)	OTHER
Coordinate Policing to standardise DF requirements	S	C	R	C	A	C
Develop model clauses for future contracts	S	C	R	C	A	C
Where required develop new routes to market, using the most efficient procurement approach	S	C	R	C	A	C
Establish an academic advisory group to provide independent advice and guidance	S	I	R	I	A	C
Strategic engagement with tool vendors to meet anticipated requirements	S	C	R	C	A	C
Establish dedicated support to coordinate national R&D	S	I	R	C	A	C
Map the R&D landscape and define areas of research need	S	I	R	C	A	C
Shape a national R&D and innovation programme to coordinate available funding and drive research activity	S/M	I	R	C	A	C
Develop the Police/Marketplace relationship to understand scale/scope of future demand.	S/M	C	R	C	A	C
Create an innovation hub(s) to centralise strategic work on specialist capabilities	M	I	R	C	A	C

Colour code for timescale for delivery:

Short term activity	0-18 months
Medium term activity	18-36 months
Long term activity	36-60 months

Code for assigning responsibility:

- R – Responsible
Does the work to complete the activity
- A – Accountable
Accountable for completion of activity
- C – Consult
Provide information for the activity
- I – Inform
Kept informed of activity progress



3

3. Meeting the data challenge

This section contributes to deliver Strategic Objectives 1, 4 and 5:



The power of digital forensic science lies in the ultimate evidential value of its source data. We will ensure that digital forensic science delivers maximum possible benefit to the criminal justice system. We will do this by improving and streamlining the way this data is managed, by making it more accessible and understandable so we extract the best value from the data policing holds. By exploring everything the data can tell us and taking advantage of

innovative new capabilities to analyse and review we will increase the likelihood of successful investigations and prosecutions. In the next section we outline how we will also ensure that the processes we apply to data are robust and reliable so we can have confidence in the results we obtain. Managing DF data as a strategic asset will ensure that the data with which policing is entrusted is being used as UK citizens would expect – to keep them safe from harm¹.

'[In a] simple street robbery 20 years ago... the complainant, the defendant, an eyewitness and a handful of others might have been able to contribute some small scientific evidence. Now, the potential is for that evidence to be: that of those witnesses, coupled with their mobile phone evidence identifying where they were at particular times; the messages from the complainant's and defendant's mobile phones; the dashcam footage from public and private vehicles going by; the CCTV evidence; the armband/FitBit-wearing defendant who can demonstrate that his heart rate was not escalated at the time of the robbery, and so on. The risk is that the investigators and subsequently the trial then drown in the data...'

David Ormerod,
Chair of Criminal Law at UCL

¹'Public attitudes on digital forensics', research carried out by Revealing Reality on behalf of TF, March 2020.

IN EVIDENCE TO THE HOUSE OF LORDS SCIENCE AND TECHNOLOGY
COMMITTEE INQUIRY INTO FORENSIC SCIENCE, 6TH NOVEMBER 2018

To understand how we can best optimise how we use this data, we need to distinguish digital forensic source data – the data directly extracted from devices – from data resulting from a digital forensic analysis. Both are digital forensic data and require a quality assured process to be followed during extraction and review, but it is important to make the distinction and be clear about the extent to which investigators can rely upon data if it received no critical technical scrutiny. In some cases, the evidential value of the data comes from its content: for example, an investigation of threatening text messages sent to an ex-partner may only require the extracted data to prove the case. In this case, a level 1 examination may be appropriate (and this will be subject to quality standards, with a trained operator following a validated process). However, if a defendant alleges that the messages in question are fake, it is the provenance which is relevant – how the messages came to be there – rather than the content. This requires further digital forensic analysis, with a DF practitioner using their skills to reconstruct the chain of events.

The practitioner might check corroborating details, such as metadata on when messages were received and viewed, against their own knowledge of tool capabilities and device characteristics. They might consider alternative scenarios, such as an online service being used to send the message with a faked sender number, based on their knowledge of additional possibilities to explain what they observe. They might analyse the raw source data to verify how the tool has interpreted dates and contact identity. They could conduct tests to verify the feasibility of these scenarios and establish which alternative

explanation is most likely. The output of this, expressed in a digital forensic report, will be of greater evidential value than the digital forensic source data to address that specific point, because it has received scrutiny from a DF practitioner with relevant knowledge and expertise. Understanding the requirements in each case determines the level of service which is needed, and understanding the evidential value of the data in context is vital to managing DF data in future. This also links to education for investigators and the wider criminal justice system to improve understanding. We consider this in the next two sections.

Infrastructure requirements

There has been, and continues to be, huge growth in the sources from which we can extract data, and in the amount and variety of data we capture from them. As well as transforming the possibilities for how we use digital forensic science this growth and variety create considerable challenges. At present, digital forensic submissions make up the largest individual source of data in police forces across the nation². How we manage and store DF data is therefore a critical priority for policing to tackle, to ensure it complies with existing policy and legislation and maintains public confidence as infrastructure requirements and costs continue to grow in line with demand.

As a first step, TF will support forces to agree a consistent national approach to handling their legacy DF data from previous cases forces have already completed within units. TF received responses to the

digital state assessment that show forces would benefit from guidance on interpreting the relevant legislation and policy in this area to support compliance. TF will provide operational guidance, informed by early discovery work which will help determine a future national approach to storing and managing this data. In tandem with this, TF will support Government in developing national policy to manage DF data and to prepare for future demand, working closely throughout to ensure consistency between TF's shorter-term operational guidance and the longer-term policy direction. When there are policy changes in future the FCN will lead on producing updated digital forensic science operational guidance feeding into the Authorised Professional Practice the College of Policing owns and updates.

The National Policing Digital Strategy gives a clear steer to adopt a 'cloud first' approach to infrastructure, where it is economical. Using the cloud could transform managing DF data, enabling central data management and simplifying how results are shared with investigating officers and onwards to the CJS. It will also enable controlled and audited online access to digital evidence, providing greater assurance and transparency.

However, there are major architectural decisions to be made before we can determine what optimal use of cloud technologies for digital forensic services will be. Bandwidth requirements are significant, because of the volume of data policing needs to upload and store, as are the potential costs. When developing the detailed operating model, we must take decisions about the degree to which we centralise DF data and technology – there are advantages but also ethical and security concerns to consider

the more the integration there is between forces and partners. TF will work with forces, other national programmes, the National Police Technology Council (NPTC) and other organisations, and with Government to ensure we consider fully and resolve the issues linked to increased connectivity and collaboration on data sharing in policing. At the same time, TF's early discovery work with forces will capture the necessary requirements to help determine the optimal architecture for DF services in the cloud.

Processing, analysing and sharing digital forensic data

Recent high profile cases have highlighted the challenge when disclosing digital evidence³. The House of Lords' report on forensic science⁴ demonstrated that we need to improve both the ability to review the output from DF examinations and how we coordinate disclosure with the CJS, which underlies the current review of guidelines by the Attorney General⁵. Taking a whole system view clearly shows that there is limited benefit to improving the ability for digital forensic practitioners to extract large volumes of data if it will overwhelm the ability of investigators to review it at a later stage. Therefore, we must prioritise implementing improved technology for search and review, including, where appropriate, use of artificial intelligence (AI) and machine learning (ML) techniques, which will track the steps investigators take during search and review, simplifying the production of disclosure material and supporting documentation in

Improving our response to knife crime

Knife crime investigations often involve multiple individuals and a huge amount of source data across different platforms, from messaging data on mobile devices, to YouTube videos or other social media. Investigators will be able to bring this data together using the simplified review platform, based on a standard data model, meaning they will be able to search across the data 'as one' whether it is a YouTube video comment or a WhatsApp message. AI and ML capabilities can help to link material connected to an individual of interest, even if they are referred to using different nicknames, and translation tools will simplify searches in other languages. Applying new capabilities like sentiment analysis to messages will help to sift the huge volume of data, identifying potentially threatening messages and highlighting them for officers to review rapidly.

line with the National Disclosure Improvement Plan.

One example of AI in practice is assisting child sexual exploitation investigations to index and categorise images, not just to improve throughput and capacity, but to support staff wellbeing by reducing their exposure to distressing material⁶. Freeing up investigator time will also allow them to concentrate on other investigative tasks such as identifying victims, reducing harm

to children by tackling hands-on child abuse. Future applications could include sentiment analysis of messages to identify threatening communications, or visual analytics to classify photographs of firearms and other weapons. This could bring significant benefit to investigations, but it will be vital to ensure that any future AI or ML technology we implement is based on robust validation of its results, and following comprehensive evaluation of the ethical issues that may arise.

A recent proof-of-concept run by the Metropolitan Police focused on introducing new technology to simplify the review task for officers – without the use of AI or other automation – which showed a number of benefits, including an average time saving of 68% when reviewing data, clearer reporting of results into the CJS, and an audit trail of search activity which other users could follow.

²Based on feedback to TF from individual forces, up to 95% of all data held within force, by volume, originates from DF submissions.

³For example, the R v Allan case which collapsed due to late disclosure of text messages to the defendant.

⁴'Forensic science and the criminal justice system: a blueprint for change', May 2019, <https://publications.parliament.uk/pa/ld201719/ldselect/ldscitech/333/333.pdf>

⁵'Consultation on revisions to the Attorney General's Guidelines on Disclosure and the CPIA Code of Practice', February 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/879676/Consultation_document_-_FINAL.pdf

⁶Matt Burgess, 'AI is helping UK police tackle child abuse way quicker than before', 17th July 2019, <https://www.wired.co.uk/article/uk-police-child-abuse-images-ai>

Essential to improving how we handle DF data is to standardise the way we store this data, by developing a national DF data model. This model will define standard metadata for different types of digital forensic information – such as text messages, photos, documents or system log files – which will allow storage in a structured vendor-independent form. There are two key benefits to doing this:

- the retention or weeding of data can be automated if the relevant metadata is stored, as a case management system can test whether conditions for retention or deletion are met;
- it makes intelligent searching possible, as queries can be based on any attribute of the data – for example, any photographs taken with a specific camera model – and opens possibilities for more sophisticated analytics.

Once DF data is stored in a standard, structured way, it opens up possibilities for analysis which also include early identification of common trends in criminal behaviour – such as whether they are using a particular chat app to groom vulnerable children. This would enable policing to disrupt this activity and prevent future harm. TF will work to develop a DF data model, aligned with the recommendation in the National Policing Digital Strategy to develop an overarching national data model for policing. In doing so they will draw on existing work in this area by the international Cyber-Investigation Analysis Standard Expression (CASE) project, which the major DF vendors support, learning and building on it and collaborating where possible to develop future specifications.

This data model will support moving towards full interoperability between tools and infrastructure throughout the DF workflow, based on standard data formats and interfaces between tools to enable forces to share data between them. Once in place, this interoperability will allow data exchange between tools and networks – for example, between a force's dedicated digital forensics network and their main corporate infrastructure – enabling them to review material remotely, making it accessible to investigators more quickly and providing a more effective service to policing. Governance and quality assurance will be built in by design, ensuring all actions taken in respect of the data will be logged to provide an audit trail of search strategies and decisions, and to ensure that access to the data is secure and available only to those who need it.

Looking further ahead, there are future opportunities to build on this to integrate other forms of investigative digital data, such as call data records from communication service providers, and open source data from internet research, bringing together all digital-related evidence into a single unified portal. This will transform the way investigators combine information into an evidential package. This framework would also allow us to generate streamlined reports in a standardised way, regardless of the tool used to extract the data, to help investigators, prosecutors, juries and other members of the wider CJS to understand digital forensic results better.

This approach will also simplify sharing data in a secure and auditable way between CJS partners, private sector suppliers, and other

police forces. It will make working collaboratively possible, it will reduce risks relating to sharing data offline and enable wider digital services to be more rapid and responsive. Once this is in place, we will have achieved the aim of Policing Vision 2025 to 'improve our use of digital intelligence and evidence and ensure we can transfer all material in a digital format to the criminal justice system.'⁷

"We must continue to exploit the opportunities presented by technology and data. Advances in technology are being used right now by criminals and the pace of change will only get faster. We need to catch up, and keep up, to protect the public"

Chief Constable Martin Hewitt
SPEECH – APCC AND NPCC SUMMIT 2020,
26 FEBRUARY 2020

⁷Policing Vision 2025, <https://www.npcc.police.uk/documents/Policing%20Vision.pdf>

Intelligent search and review of digital evidence

A structured data model for storage of digital forensic data will provide a foundation to develop more advanced tools, enabling investigators to extract meaning from the raw data ingested, searching for entities and attributes rather than being limited by keywords or previously-known identifiers. This will enable a single overview of ingested data, regardless of its source, allowing an investigator to search in real-time across indexed data from all evidence items in a case. Integration of analytic capability will provide meaningful information insights and build up a rapid intelligence picture to speed up investigations.



DFS-002

Improving our response to child sexual exploitation investigation

Transforming the way we work will bring a number of benefits for investigations into CSE. At the outset, investigating officers will have access to triage capabilities meaning they can identify priority devices quickly and screen out devices where there is a low likelihood of relevant material. Early access to reliable triage findings means they can progress immediate safeguarding enquiries, reducing risk and harm to victims. This triage can be at scene or prior to submission, whichever is most appropriate for case circumstances. Quality assured and fully accredited triage methods will be deployed in line with the associated threat, risk and harm.

When devices are submitted for forensic examination, the initial stages of processing will be automated so material is available for review as quickly as possible. This automation will include a link to CAID so CSE material is identified. Automation will also use the latest AI/ML tools to support automatic image categorisation, to increase the likelihood of detecting new images of abuse rapidly. When the initial processing is complete, there will be fewer images that need manual review, reducing the demand and emotional impact on staff tasked with reviewing

the CSE material. Simplified review tools will make reviewing more straightforward and ensure that material of interest is tagged for later forensic analysis by a specialist. The extracted data will be available to officers securely over the police network allowing them to review the findings from any network computer and avoid any investigative delays. When the investigation is complete, the system will generate an evidential package in a standard format, helping investigators and the CJS understand the significance of the findings more easily, and identify the real issues.

Adapting and integrating with existing systems during early implementation will enable secure data sharing with the CPS, defence and court through the FCN Xchange including all necessary material for disclosure. The forensic information ecosystem will facilitate the entire process, handling intelligent automation of tools, auditing, and secure data sharing and management. The process will be quicker and more efficient. It will be robust and standardised, transforming the policing response to CSE investigations and ensuring swifter justice to reduce harm.

Benefits

Strategic benefits

- More rapid progression of investigations to maximise access to all investigative opportunities, including in critical 'golden hour'
- Improved evidential data and case management, enabling victims to be kept informed of case progression, and providing increased confidence that their data is handled proportionately, fairly and securely
- Enables whole-system approach to linking different types of digital evidence, including communications data and open-source material, meaning best evidence can be provided into the CJS to improve case outcomes
- Standardised data models allow interoperability between tools and infrastructure, supporting collaboration and making processes more streamlined and efficient
- Improves data governance and reduces risk at a national level, ensuring forces are following

- a consistent approach to data management
- Centralised management of the system reduces overheads and improves security and governance of activity, helping to embed a quality-first approach
- Identify common trends in criminal behavior, enabling policing to be proactive in disrupting criminality and reducing harm
- Agreed national approach for proportionate and secure data sharing between forces and partners

Tactical benefits

- Investigators able to review material remotely increasing availability and accessibility, speeding up the investigative processes
- Faster and more relevant insights through the use of machine learning and AI, improving investigative outcomes and reducing the demand on human reviewers, improving wellbeing
- Interoperability and data sharing between forces and other CJS users, reducing data management overheads, simplifying integration of other forms of evidence into an evidential package and reducing workload relating to disclosure

Key steps towards delivery

ACTIVITIES	TIMESCALE	TF	CORE FCN	NPCC / APCC	FORCES (FCN MEMBERS)	HO	OTHER
Develop operational guidance for the storing and handling of live and legacy data	S	R	A	C	C	C	I
Identify requirements for optimal cloud architecture for DF	S	R	A	I	C	C	C
Develop a national policy to manage DF data	M	C	C	C	C	RA	C
Review & reissue operational guidance for the storing and handling of live and legacy data in response to any national policy changes	M	R	A	C	C	C	I
Implement new and innovative technology for search and review	M	R	A	I	C	C	C
Implementing automated workflows to support DF activities	M	R	A	I	C	I	C
Develop standard interfaces between tools to facilitate full interoperability (API)	M	R	A	I	C	I	RC ⁸
Develop an overarching national data model for policing	M	R	A	I	C	C	I

Colour code for timescale for delivery:

Short term activity	0-18 months
Medium term activity	18-36 months
Long term activity	36-60 months

Code for assigning responsibility:

- R – Responsible
Does the work to complete the activity
- A – Accountable
Accountable for completion of activity
- C – Consult
Provide information for the activity
- I – Inform
Kept informed of activity progress

4

4. Developing the Workforce

This section contributes to deliver Strategic Objectives 2 and 4:



Digital forensic science has grown organically over the past twenty years, and this is evident to see in the disparate workforce of today. This workforce brings a range of skills, experience and perspectives to the work they do. Those working in DF can range from police officers with investigative experience who are now applying that expertise in a new area, to technical experts or engineers who bring computer science or hardware knowledge and apply that to reconstructing a digital evidential trail for example. The mix of skills digital forensic science needs from its workforce means that this variety is a strength. But it also presents challenges to developing a consistent approach to quality standards, competency assessment and workforce planning.

DFU staff demonstrate a strong public service ethos. They take pride in the important work they do¹. But because demand is heavy and resourcing lean, there is excessive pressure across DFUs which mean recruiting and retaining staff is a serious challenge². This is especially so because the skills we need for digital forensic analysis are the same skills the fast-growing cyber-security sector values, and values highly. The traditional understanding of a 'DF workforce' is also changing. Expanding DF capabilities outside DFUs, from first responders seizing devices to investigators reviewing digital data to be used in court, mean

we need to widen this definition to include all staff whose activities involve an element of DF science. If we are to achieve our ambition to transform digital forensics it is critical that we develop a strategic approach to growing a sustainable DF workforce with the right skills, a clear career pathway and continuing professional development to keep pace with technology. Understanding the current workforce

Improving our response to low-level crime

Devolving capabilities to the front line means that officers investigating lower level crime will be able to use these capabilities for investigations which would otherwise be limited by scarce specialist resources. For example, mobile phone data is key to investigating drug supply offences. Greater awareness training and access to the knowledge base will help officers take better decisions about which devices to seize and what level of analysis is needed. Trained kiosk operators can now use self-service technology, via a method which has been fully quality assured, to extract this data from phones they seize. This means quicker access to digital evidence for investigators and freeing up DFU staff to focus on more technical DF analysis work.

¹ From engagement with DFUs by the TF team, and e.g. 'DIGITAL FORENSIC INVESTIGATIONS IN POLICING - INITIAL FINDINGS REPORT FROM THE SWFC', unpublished report by Dr D. Wilson-Kovacs, University of Exeter 2018

² The digital state assessment identified an average turnover of 15% for DFU staff, with a vacancy factor of approx. 10%. This follows earlier findings from Gartner highlighting the difficulties forces faced in recruitment and retention (Digital Forensics Future Challenges, a report from Gartner for TF, 2019).



TF carried out the 'digital state assessment', including mapping the staffing make-up of DFUs nationally, and exploring how we provide DF services outside DFUs³ Responses highlight the staffing challenges DFUs face and corroborate earlier industry research⁴ which identified the difficulties forces face building DF capabilities. In line with this strategy's core aim of coordination and 'doing once for the benefit of many', we need a consistent approach to managing DF skills and competencies so that forces can take full advantage of standardising methods and approaches. Equally, a clear career structure is vital to building and retaining a professionalised workforce, giving talented staff a route to develop and progress further.

Developing a joint approach

The strategy proposes that first FCN Science develop a workforce **recruitment and retention plan** mapping the challenges the existing workforce faces and identifying strategies to resolve those challenges. This work must acknowledge the differing needs different DFUs have - they vary widely in size, staff makeup, funding, training provision and specialist capability. A core element will be building a

career structure for DF science roles. This work will take into account that many staff may not want to progress into management roles, but into more specialist areas or that other staff may wish to broaden their specialist knowledge or add to their specialisms, rather than advancing in grade. This means career paths must not only be linear. The structure must also take into account the mix of police officer and staff roles in units, particularly where more senior roles have traditionally been available only to warranted officers rather than to police staff. This plan must take all these issues into account to make a DF science career in policing more, or at least as, attractive than other industries where the same skills are in demand.

Collaborative governance

Improving job satisfaction across different forces with differing employment conditions, pay and reward structures is a key challenge to resolve. Existing policing delivery structures limit forces' ability to standardise these things, so unless there is more radical change, the plan we develop should make recommendations for individual forces/PCCs to ratify. The FCN governance structure should develop

a decision making process so that members can agree on role profiles, staffing split and so on.

Building a skills pipeline

In the recruitment and retention plan FCN Science will examine how to open up new routes into DF science careers, including developing proposals for a national apprenticeship scheme, and engagement with higher education institutions to develop schemes for vocational learning, such as sandwich year placements and joint project supervision. This will ensure that degree courses have a closer link to the skills and experience we need in the workforce. Through these measures we will build a 'skills pipeline' to reinforce the workforce on a continuing basis. In conjunction with the College of Policing's (CoP) DII project, which is developing modules under their Digital Learning workstream to cover digital skills, we will also develop a **basic training programme** to ensure recruits have a standard set of skills regardless of their entry route. DFU staff also need early career mentoring, providing staff the time and support to focus on their professional development and future career routes. Lack of diversity is a particular challenge in STEM roles⁵, and recognised as such, and it will be important to increase diversity among the DF science workforce.

³Through the digital state assessment, conducted in autumn 2019. This was limited by the quality of the data returned, but highlighted a lack of overall coordination of DF activities within forces, which could be carried out by multiple groups or teams, e.g. those monitoring registered sex offenders (RSOs) or those conducting collision investigation as well as the more obvious DFUs.

⁴Digital Forensics Future Challenges, a report from Gartner for TF, 2019.

⁵See, for example, <https://www.diversityintech.co.uk/>, <https://nii.oip.gov/topics/articles/importance-diversity-and-inclusion-forensic-sciences> and <https://digitalforensicsmagazine.com/blogs/exploring-cybersecuritys-diversity-problem/>

Standard approaches for training and competency

As well as a basic training programme, the FCN and CoP should collaborate to develop a **training framework** to support forces in assessing the variety of vendor-specific and other privately provided DF specialist training courses which are available. These courses vary in their depth and how comprehensive they are. They are also relatively costly because of their specialist technical content in comparison to other training courses policing provides⁶. If we are to ensure forces get value for money from limited training budgets, we need to review the training landscape to support them to select the most appropriate training. The FCN/CoP should assess the feasibility of accrediting relevant training courses to help forces take these decisions. Building on this, FCN Commercial and FCN Science should lead work with vendors to address training requirements the review will identify.

To provide an effective way to assess, maintain and monitor the knowledge, skills and behaviours of individual forensic practitioners, the FCN, working jointly with the CoP's Digital Skills and Standards Framework workstream, must make developing a standard **national competency framework** for DF skills a priority. There is no such approach at present, with some forces using the Skills for Justice National Occupational Standards and other forces developing their own. A coordinated national framework would simplify workforce planning and support career progression,

⁶Typical DFU analysis compiled from the DSA shows that the average DFU spends £75k on training annually.

ensuring roles are consistent across forces, and inter-force collaboration. This will also contribute to building a clearer career structure for DF science roles, and enable forces, FSPs, the CoP and the FCN to collaborate to develop professional profiles for each role. FCN Quality will help to facilitate using this competency framework with a nationally-provided eQMS (electronic quality management system).

Effective workforce planning

Once we have this standard competency framework in place, the FCN will carry out a comprehensive **skills audit** to assess the workforce needs and identify the skills gaps. There are then a range of measures to deploy to address the needs and gaps we identify, including training, targeted recruitment and sourcing specific capabilities externally. The CoP and the FCN can explore this fully in a national **workforce planning strategy**. Because there are so many interdependencies FCN Science should lead the FCN contribution, supported by FCN Quality and in close collaboration with FCN Commercial because of the clear crossover with the scope of the forthcoming Forensic Marketplace Strategic Plan. Any workforce planning strategy must consider workforce requirements holistically, i.e. not only within DFUs, but taking the wider skills ecosystem for DF science into consideration.

Continuing professional development and learning

In digital forensic science, more than any other forensic science discipline, continual learning is essential if we are to maintain capability to handle emerging technologies. We need a multifaceted approach, encouraging

practitioners to take responsibility for their own development and to make continuous learning part of their day to day work. The 70:20:10 model of learning where the individual balances learning on the job (70%) with learning from others (20%), supported by formal learning opportunities (10%), provides an effective basis from which to develop our approach.

The FCN, with its nationally networked approach, is an ideal mechanism for this. It can facilitate collaboration between practitioners in different forces by providing a platform for sharing knowledge and data, as well as co-ordinate R&D and dissemination of good practice from the work in the innovation hub(s) to make sure staff can keep their knowledge up to date. Forces should offer staff the opportunity to rotate between their 'home' force DFUs and the FCN innovation hub(s) on short secondments, to give them personal development opportunities and to ensure that there is a strong connection between R&D capability development and operational needs. This will also help to counterbalance demands on staff when the bulk of their workload is CSE investigations, helping to improve wellbeing and morale.

Knowledge management

An essential component of continuous learning is using a knowledge management system, or a knowledge base, to provide a central location to share good practice, information about novel techniques, or capability requirements. This knowledge management system could be built on the Knowledge Base workstream in the CoP, or developed separately, but however we take it forward both specialist DF

staff and others involved in the wider investigation should have easy access to it for information and support. For example, for first responders or CSIs on scene it should include details of potential digital evidence sources and instructions for handling each of them.

We propose a crowd-sourced practitioner-populated knowledge base to ensure rapid knowledge refresh and to keep it up to date. It should have rules to show the reliability of the information based on the number of corroborating votes or reports⁷. So too it must be flexible enough to extend to different future capabilities, allowing for example, use of augmented reality (AR) technology to scan scenes and highlight devices to recover⁸.

Building multidisciplinary collaboration

Peer review and sharing skills is vital to continual learning and to enrich the DF workforce. Opening up to wider collaboration through the FCN's innovation hub(s) gives staff the opportunity to be part of exciting joint work between forces, other public sector organisations, industry and academia, making use of the wider DF skills ecosystem to stimulate learning and development. There are a number of methods to facilitate this – schemes such as the cyber-Specials scheme to draw in technical expertise

⁷In a similar way, the categories assigned to images within the CAID database depend on a 'voting' approach (https://www.cps.gov.uk/legal-guidance/indecen-and-prohibited-images-children#_Toc533073890).

⁸This was also suggested in a report produced by Policy Lab on behalf of the Home Office (2018), focusing on how to increase frontline staff and courts' literacy in digital forensics.

⁹<https://www.college.police.uk/What-we-do/Learning/Police-Education-Qualifications-Framework/Pages/Police-Education-Qualifications-Framework.aspx>

to assist in tackling cybercrime, or internships for post-doctoral students to collaborate on research activity could help facilitate building this multidisciplinary collaboration and we propose that FCN Science explore these, with the goal of allowing multidisciplinary teams to build and work remotely.

Addressing the needs of the wider workforce – CSIs, first responders, frontline data recovery users and investigators

There are many roles along the crime scene to court route which, although not DFU roles, are involved in some DF activity. Some of these roles have clear crossover with DFU work and others simply need a more general understanding of DF science.

The police investigation landscape is changing and has seen some units build up DF skills and DFU type capability to get around the challenges of DFU backlogs. So, many services are doing DF activities outside the DFU structure which are not covered by any forensic governance. This lack of structure and governance presents risks for quality and resilience of service, not to mention broader reputational risks for policing.

With the aim of developing a standard training framework which is flexible and adaptable enough to fit the needs of policing for all digital forensic science activities, the FCN will work with the CoP to identify all roles across policing that use DF science outside traditional DFUs. This will include roles such as Digital Media Investigators, cybercrime investigators, or staff in ROCUs and cover the full range of roles where

a DF science process is employed, including those processes which are embedded into tool workflows (such as self-service kiosks) and not just those where specialist judgment or interpretation of evidence is taking place. The FCN and CoP will identify the common elements of their activities and do a capability and skills review for these roles.

The FCN and CoP will also identify roles which need a more general DF awareness, such as officers who are first responders on scene, investigators planning forensic strategies, or reviewing the output from digital forensic tools

‘Every detective needs to know the basics of digital evidence - where it is likely to be located, how it can be safely collected and preserved without being contaminated in the process, and the core techniques that are used in analysis’

Professor Peter Sommer
WRITTEN EVIDENCE SUBMITTED TO THE HOME AFFAIRS SELECT COMMITTEE, 2013
[HTTPS://PUBLICATIONS.PARLIAMENT.UK/PA/CM201314/CMSELECT/CMHAFF/7070WE14.HTM](https://publications.parliament.uk/pa/cm201314/cmselect/cmha/7070we14.htm)

Officers need to know these basics to understand, at the very least, the weight of forensic evidence and to avoid misunderstandings when they are communicating it in court. They also need to be aware of the difference between the digital forensic source data which may be extracted using a

self-service kiosk, and the digital forensic analysis provided by a digital forensic specialist, and which they need in the circumstances. Although officers who carry out self service examinations receive training and should complete competency assessments, there is no corresponding assessment to gauge what their understanding is of DF evidence. Without knowing the potential of digital evidence, officers will be unable to complete forensic submission requests effectively, and risk missing evidence because they do not submit it for examination or because they do not provide relevant information, such as known user names, to the DFU.

The College of Policing's work on the Policing Education Quality Framework (PEQF)⁹ includes learning standards which cover this area. The FCN should assess this from a DF science perspective, and collaborate with the CoP on any required updates. Once complete the FCN should make all investigators aware of the material and how to access it to support their continuing

professional development. The knowledge base will provide further support in understanding the output from DF examinations, and information about DF capabilities. The frequently updated content will complement a basic training package for all newly recruited police officers, available online to all officers wishing to refresh their knowledge and skills.

The Home Office also commissioned work by Policy Lab to look at how we could best increase frontline staff and courts' DF literacy. This work proposed a number of interventions, such as putting a DF evidence case study on the wall in an investigative office, providing an app to support first responders on scene, a voice assistant to give guidance and suggestions, or a 'DF coffee run' to increase informal cross-pollination of knowledge between investigators and practitioners. The FCN are ideally placed to review these and work with forces to pilot these ideas to assess their benefit.

Quality assurance and governance of activity will help to assess the wider success of these measures;

this should focus as a priority on officers carrying out DF activity (such as the use of self-service kiosks) and could include a regular dip-sample of these cases, to reinforce competency assessments officers must take before carrying out self-service examinations. Introducing a national digital forensic configuration authority (NDFCA) through the FCN will support forces to manage this. Wider quality assurance should also include a review of cases involving digital evidence to recognise themes related to a lack of understanding or where evidential opportunities are not being pursued.

The very last stage in the digital evidence process is presentation at court. A lack of understanding in court can thwart the efforts of everyone who has contributed earlier in the chain. Greater understanding on the part of investigating officers will help to support this, but there is a wider need for prosecutors, defending barristers, judges and juries to have a base level of understanding to assess the value of DF evidence properly. We cover this in the next section.

Forensic Workforce Strategy

	Recruitment & Retention	Education & Training	Learning Culture	Workforce Competence	Workforce Planning	
Short term	Fit for purpose professional profiles Guidance for selection for aptitude & potential	National forum Training needs analysis Current status of training provision	Learning for emerging capabilities Identification of CPD priorities Delivery of online CPD events	Existing capability map Competence framework Framework embedded in eQMS	Existing workforce profile & skills gaps Understand demand	Short term
Medium term	Common induction Promotion of the profession Coaching & mentoring Career planning/CPD	Training QA strategy Agreed standards of education training & assessment Work placements / approved providers	Curation of learning resources Embed reflective practice Embed 70:20:10 model of learning	Analysis of future capabilities 21st century skills gap analysis National capability map	Expectation and motivation of the next generation workforce	Medium term
Long term	Flexible working Talent management Feedback culture Public value focus	Flexible & approved learning pathways Apprenticeships Workplace ready vocational qualifications	Shift from push learning to pull Learning experience platform Learning any time anywhere	Academic planning linked to capability demand Data analytics Sustainable workforce skills	Demand drives academic planning Workforce redesign where needed	Long term

Supported by National Forensic Workforce Development forum

DFS-011



Benefits

Strategic benefits

- Improved staff morale, welfare and wellbeing
- Skills pipeline to grow the DF science workforce, maximising access to talent
- Improved retention of existing staff, maintaining the benefits of experience and established effective team working
- Better quality of DF outputs through upskilling the workforce, ensuring the appropriate expertise is available to meet requirements
- Facilitation of collaboration between practitioners in different forces, using national platform for sharing knowledge, helping to drive innovation and advance collective knowledge
- More effective coordination of DF expertise through innovation

hubs, improving policing's access to DF specialisms

- A solid foundation of training for frontline users and investigators, helping to improve investigative outcomes and effective communication of DF evidence in court
- Clear framework for competency to support adherence to quality standards, improving compliance and confidence in DF evidence

Tactical benefits

- Competence at all levels from self-service to expert builds confidence and trust within the workforce
- Continuous professional development supporting practitioners to develop competence for new and emerging techniques
- Better value for money for forces procuring specialist training courses
- Knowledge base to provide central location to share good practice, new techniques or capability requirements, ensuring practitioners and frontline users follow consistent methods to support a quality-first approach

Key steps towards delivery

ACTIVITIES	TIMESCALE	TF	CORE FCN	NPCC / APCC	FORCES (FCN MEMBERS)	HO	OTHER
Develop a workforce recruitment training and retention plan	S	C	RA	C	I	I	C
Develop a training framework to map existing available training courses	S	C	RA	C	I	I	R*
Undertake feasibility study for accrediting training courses	S	C	RA	C	I	I	R*
Develop a training framework of requirements for all roles where DF science processes are employed	S	C	C	C	I	I	RA*
Prepare a workforce planning strategy	S	C	RA	C	I	I	R*
Develop national role profiles for core DF roles using national competency framework	S	C	R	C	I	I	A
Undertake a national DF skills audit	S/M	C	R	A	I	I	I
Develop new routes into DF science careers	S/M	C	R	A	I	I	R*
Establish continuous professional development requirements for core DF roles	M	C	R	A	I	I	R*

Colour code for timescale for delivery:

Short term activity	0-18 months
Medium term activity	18-36 months
Long term activity	36-60 months

* It is assumed that the College of Policing will play a pivotal role in conjunction with others in delivering each of these activities

Code for assigning responsibility:

- R – Responsible
Does the work to complete the activity
- A – Accountable
Accountable for completion of activity
- C – Consult
Provide information for the activity
- I – Inform
Kept informed of activity progress

5

5. Building Trust

This section contributes to deliver Strategic Objectives 1, 3, 4 and 5:



Building public trust is an increasingly significant issue for digital forensic science. Against a backdrop of rising awareness of data security, the EU General Data Protection Regulations (GDPR) giving individuals more control over their personal data, and with publicity surrounding police use of new technologies such as facial recognition and AI it is easy to see why. Public interest and advocacy groups raising privacy concerns, especially for rape victims asked to give access to their devices and data¹, has highlighted concerns around digital forensics which we must address if we are to maintain and build a broad consensus around policing's use of DF science.

In developing this strategy, we sought to understand the broad spectrum of public attitudes to digital forensics, not just to know the public's view on how digital forensic science should be used, but also to gauge the levels of awareness and understanding. We commissioned research², including a survey, focus groups and in-depth interviews to investigate and to inform how we design the future operating model taking public views into account. We want to ensure we can introduce new capabilities in a consensual way and build public requirements into the

design. The scope of this extends to all digital forensic activity, within and outside DFUs, and all digital forensic data, both source data and that which results from digital forensic analysis, as we discussed previously in this strategy.

This strategy also aims to improve awareness and understanding of digital forensic techniques across the CJS, highlighting the strong emphasis on quality all the way through the digital forensic examination process. We want the courts to be confident in the quality of DF output and the effectiveness of DF techniques, to improve trust and enhance the service to victims and witnesses. To realise these benefits we need trust in digital forensic science. We can only do this by maintaining trust in DF science in the courtroom, the final stage of the digital investigation process.

Public attitudes towards digital forensics

Considering the issues we raise previously, our research found that, at present, there is a relatively high level of trust in how policing uses digital forensics. 86% of respondents agreed that policing should be able to use digital forensics when appropriate to help solve crime. Respondents were generally well informed about digital forensic capabilities, understanding the type of information which might be relevant to police investigations.

¹ See, for example, 'Digital Strip Searches: The police's data investigations of victims', Big Brother Watch, July 2019 (<https://bigbrotherwatch.org.uk/wp-content/uploads/2019/07/Digital-Strip-Searches-Final.pdf>)

² This research was carried out by Revealing Reality on behalf of TF, in spring 2020, and involved an online survey of 2000 respondents, representative of the UK population as a whole, supplemented by two focus groups split by age (18-40, and 41-70) plus two in-depth interviews with respondents who had first-hand experience of sharing their digital data with the police.

'It's gold dust really, isn't it, to have all that information...'

Focus group respondent

Respondents felt that witnesses (31%) and victims (28%) in particular should need to give consent before sharing their data with the police, compared to 19% of respondents who thought suspects needed to give their consent. Most respondents thought that knowing what data police wanted to access (74%), and how they would use it (72%), should be essential before consent could be given; they were happy to give consent as long as they would be kept appropriately informed.

However, respondents, especially in focus groups, expressed more concerns the more they thought and learned about the digital forensics process. This suggests that considering the details more deeply might affect their overall view. Discussions about the intrusive nature of digital searches also reflected this view. On initial questioning, focus group respondents all felt strongly that searching someone's house physically was more intrusive than searching their phone, even though the digital data could include their most personal and private photos and messages. But one of the interviewees saw phone searches as much more invasive, based on her own personal experience: 'it's an invasion of your thoughts'. This disparity is potentially because of a lack of understanding of how revealing a digital forensic investigation can be, a point we could

explore in future research.

Focus group respondents expressed a desire to know more about how the police accessed their data. For example, they were concerned that police could access their data remotely without them being aware. One suggestion was for an independent body to oversee the police's access to data, to enforce restrictions on access and ensure that investigators only received necessary information following a specific request. This links with a suggestion from practitioners at a TF engagement event to implement a 'digital escrow' solution to address concerns about intrusive access to victims' or witnesses' data. This type of solution would hold data securely and only provide subsets of data in response to an investigative request with clear justification, following a specific line of inquiry.

Ethical governance and oversight

The increasing scope of digital forensic capabilities raises new ethical dilemmas for policing to consider. Some of these overlap with other digital investigation issues, such as using AI to analyse datasets and concerns about aggregating investigative data. Other concerns are particular to DF science. For example, managing sensitive personal data coming from mobile phone analysis, which involves 'collateral intrusion' into others' privacy when reviewing messages, or friends and family photographs. These are complex issues and there are no easy answers.

Recognising the challenge, a number of sectors have established panels, groups and committees

to consider and advise policing on ethical issues. The landscape is varied, encompassing force-specific independent ethical panels (such as the Metropolitan Police³ and West Midlands Police⁴ panels), independent advisory bodies (the Centre for Data Ethics and Innovation⁵, or the Ada Lovelace Institute⁶), reviews into specific technologies (the Law Enforcement Facial Images and New Biometrics Oversight and Advisory Board⁷) and the NPCC ethics portfolio, that DCC David Lewis oversees, covering policing more widely. However, none of these had focused on the ethical issues specific to digital forensics, centring on privacy, consent, proportionality and data governance. To date, when these issues have come to the fore in policing, the typical approach to handle them has involved setting up a Gold Group which focuses on a specific issue rather than having an ongoing remit to address the root cause. In addition, with all the different factors involved in decision-making this varied landscape presents the risk of inconsistency between ethical judgments.

We need a clear process for policing to follow for ethical approval to deploy a new technique, or to obtain a view on whether an existing method is acceptable, in the same way that university ethics committees consider and approve applications for research where ethical issues may arise.

³ <http://www.policingethicspanel.london/>

⁴ <https://www.westmidlands-pcc.gov.uk/ethics-committee/>

⁵ <https://www.gov.uk/government/organisations/centre-for-data-ethics-and-innovation>

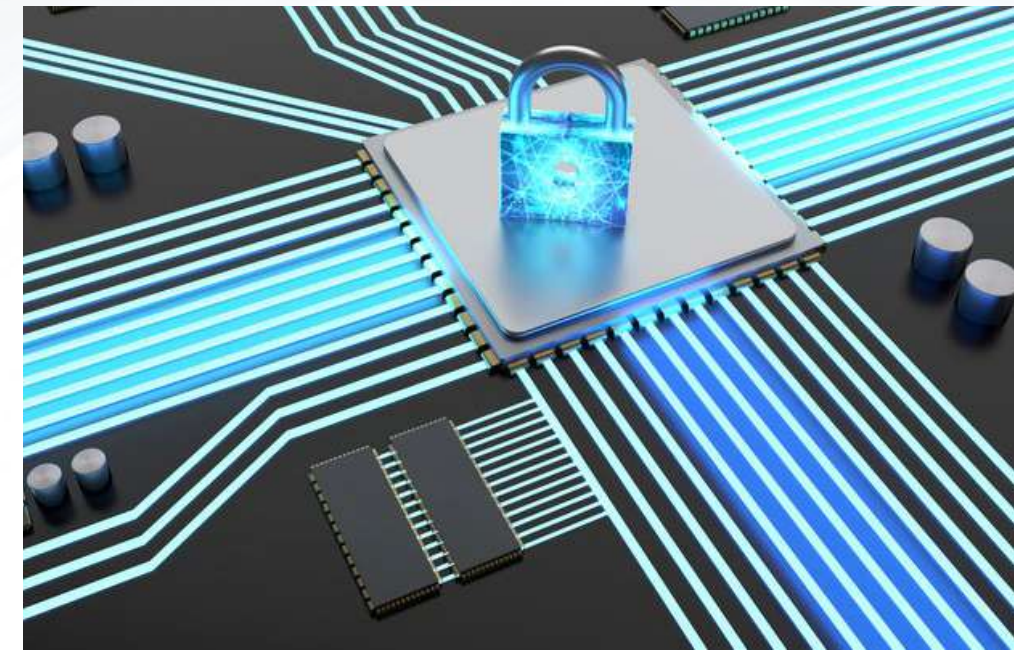
⁶ <https://www.adalovelaceinstitute.org/>

This strategy proposes that we develop an **ethical governance model for digital forensic science** which provides guidance and governance for new capabilities. Consolidating biometrics governance across the NPCC under the Biometrics Committee is the first step to addressing this, with subcommittees covering Data, Forensics, Technology and Ethics to address the key issues requiring a national approach. As part of this framework, FCN Science will work closely with the relevant subcommittee(s) to develop an agreed process which ensures decisions are independent and transparent, so that policing is not only taking the right approach, but can be seen to be doing so. To underpin this, the Home Office will work with the Biometrics and Forensics Ethics Group⁸ to consider the major ethical issues affecting digital forensics, such as the collection, use, retention and deletion of digital forensic source data, and the aggregation of large datasets. This will inform future policy, which in turn will steer technological development and tactical decision-making, and shape public debate.

Improving governance and data security

Operational guidance

Rapidly developing technology has raised questions for forces in some areas of DF activity, such as acquisition of data stored in the cloud as part of a digital forensic investigation. TF public attitudes research suggested that the majority of people saw no distinction between



acquiring data held on a device and data stored in the cloud (68% of respondents thought consent should cover all data accessible from a device, not just that stored on it), but the approach to this will be different, especially since material is likely to be stored in a different legal jurisdiction. This strategy proposes that TF develop operational guidance on behalf of FCN Science to interpret existing legislation and policy that applies to DF to give forces a clear national approach. As part of this work TF and FCN will engage with the CoP as the lead on Authorised Professional Practice (APP) in policing.

Furthermore, TF and FCN will support Government, with input from the wider CJS, the FSR and the ICO, to review the existing policy and legislative framework for the entire scope of DF activities, to ensure clear powers and national policy underpin them all. Close collaboration between TF, FCN and other agencies will help to ensure that operational

guidance produced in the near term is consistent with future longer-term policy direction. As we mentioned earlier in this strategy, when there are policy changes in future the FCN will lead on producing digital forensic science operational guidance feeding into the Authorised Professional Practice the CoP owns and updates.

This work will consider the issues of proportionality and necessity to develop a governance framework which will support forces to meet regulatory requirements, for example in capturing, processing, and storing personal data. It will also consider the needs of the whole criminal justice system, taking parity of opportunity for defendants into account. It is well known that disclosure must include anything which could assist the defence case or undermine the prosecution,

⁷ <https://www.gov.uk/government/groups/law-enforcement-facial-images-and-new-biometrics-oversight-and-advisory-board>

⁸ <https://www.gov.uk/government/organisations/biometrics-and-forensics-ethics-group>

but this principle can apply at an earlier stage. When acquiring volatile data, for example, it would be good practice to have in mind other reasonable lines of enquiry to ensure that information which could corroborate an alternative explanation of events is not missed or ignored. Digital escrow could be a helpful solution here, but it is important to consider overall the right balance of the rights of defendants against the privacy of victims or witnesses.

Data

Managing personal data effectively is key to building confidence and trust. The existing systems and processes in policing do not help build either confidence or trust. The standardised approach to storing data which we propose earlier in this strategy will help here by giving the public more transparency around how policing holds and processes their data. A comprehensive forensic information ecosystem will allow policing to give the public information on how their data will be used, and how it will be shared. We will be able to assure victims and witnesses that their data is secure, that there are appropriate audits and that only those with an investigative need will be able to access their data. A common approach across forces to forensic case management is key to providing this assurance and TF should develop a suggested high-level design and roadmap for implementation, working with the National Police Technology Council and other partners such as Police ICT Company (PICT Co).

Investment in structured data storage and forensic case management will also support

compliance with disclosure requirements. Operational guidance that TF, on behalf of FCN Science, will develop will improve data control and oversight throughout the digital forensic workflow. With support from the FCN to embed clear guidance, detailed data models and enabling technology in place, data can be shared securely for joint working between forces and partners (such as specialist external providers where niche expertise is required).

Where appropriate, and only where they can secure ethical approval and preserve privacy fully, policing could share data with partners in an anonymised form to help capability research and development. R&D and developing novel technologies successfully is constrained by a lack of availability of operationally representative data to test and steer development, but it is essential that privacy concerns be addressed before any data sharing can take place.

TF will work with partners to explore the future potential for developing and using privacy-preserving technologies and consider digital escrow as we outlined previously. They will also explore the feasibility of selective extraction (taking only the relevant data from a device) and the potential application of other relevant technologies which could help build trust, such as blockchain. This will inform the longer term operating model.

Quality standards

Embedding a quality culture throughout all areas of DF science is a fundamental shift and something that is still ongoing. The FSR set a deadline of October 2017 for all

providers to achieve accreditation to ISO17025. Despite this, compliance is still low, with less than 20% of the processes which need to be accredited achieving it so far. Future legislative change is expected to give the FSR statutory powers of enforcement⁹, and compliance is therefore vital to ensuring continued public confidence in law enforcement. Staffordshire University carried out research for TF¹⁰ and found that constraints on resources limited forces' ability to get accreditation despite their eagerness to do so.

The research identified collaboration as a particular issue because forces wanted to share the workload but did not have the support for coordination which would maximise the benefits. For example, some forces had come together in formal collaborations and some had shared SOPs with other forces, but there was no wider coordination to divide the workload nationally and avoid duplicating effort. This strategy proposes that FCN Quality play a key support role in future by coordinating and communicating activity, tasking digital accreditation support teams to share learning between forces, and agreeing the prioritisation of central validation activity to reduce the burden on individual forces. This should help forces to meet the challenge of achieving accreditation to ISO17020 for on-scene activity, by learning from the previous experience in relation to ISO17025.

Digital forensic science is the only forensic discipline where both the

techniques staff are using and the data sources they are analysing are evolving constantly. This creates unique challenges, among them enabling innovation and at the same time making sure processes are quality assured and robust. If we are to meet the future challenge in this area, we need a more strategic approach. This is the focus of recent work DSTL have done with the FSR and the NPCC Digital Forensics Portfolio Board (DFPB) to scope the work involved in creating ground truth datasets for validation. DSTL are ideally positioned to support policing in this work and this joint approach should continue, supported by FCN Quality and with engagement with the United Kingdom Accreditation Service (UKAS).

Practical measures to embed a quality-first approach also include providing **central validation support**. FCN Quality will deliver this by coordinating work between forces or in collaboration with DSTL or other partners, sharing results with forces so they can verify the method locally.¹¹

To do validation testing we also need **comprehensive ground truth datasets**. DSTL should continue their work in this area, with support from FCN Quality and engagement with the FSR and UKAS, collaborating on a national and even international scale where possible. Preparing these datasets is largely manual and time-consuming work and there is clear benefit to a central approach.

FCN Quality can support policing to ensure all DF science processes,

¹¹This approach was partially tested through the development of a standard validation package for the self-service kiosk method, done by DFPB in partnership with DSTL and forces. This standard validation package was tested by Staffordshire Police on behalf of TF to assess the feasibility of a national central validation approach; useful learning has been identified from this approach, requiring some modification to the method, and further insights from the process will be incorporated into the future approach.



technology solutions and guidance are the best they can be, with quality built in by design to foster trust in DF science processes. By taking a national view, the FCN will be able to leverage expertise throughout UK policing, taking the best elements from each force's practice.

FCN Science and Quality must also collaborate to identify the places outside DFUs where DF science is going on, and meet the challenge of embedding this quality approach in those places. To do this they will need forces' agreement where units and staff fall outside forensic science governance, and the FCN must develop an approach to address this. This will help determine the feasibility of a **national digital forensic configuration authority** for DF science, to ensure standard tools and methods are used consistently at different geographical locations. FCN Quality must take the disparate nature of DF service into account when designing the most appropriate deployment model for this, and provide a package of support that will fit the diversity of operating contexts in forces. This centralised support will make full use of the scope within the FSR's Codes of

Practice and Conduct to maximise efficiency by accrediting a method once and deploying many times.

“There are many digital forensics activities taking place outside DFUs, in what has essentially grown up as a cottage industry. In particular, DMIs are undertaking virtually the same processes as DFUs and additional processes at scenes, but none of the DMI units is compliant with the standards required for digital forensics and few are yet working towards compliance”

Dr Gillian Tully

FORENSIC SCIENCE REGULATOR INCREASING KNOWLEDGE AND UNDERSTANDING IN THE WIDER CJS

Quality standards are a key element of building trust in DF evidence at court. So too is increasing understanding of DF evidence. If prosecutors do not fully understand the import of digital evidence, and miss its significance, they will not present it effectively. This is especially likely in cases where the evidence comes from diverse sources or involves large volumes of data. If the judge and jury do not have a base level of understanding, they will be unable properly to assess the value of the DF evidence in the context of the case. Finally, but just as importantly, if the defence do not understand DF sufficiently they will be unable to challenge adequately evidence the prosecution presents, something which is fundamental to providing an effective defence.

To make sure everyone who needs to be is appropriately trained and aware, we need training and awareness-raising programmes targeted at barristers and the judiciary, with content reviewed regularly.

This will share good practice for cases involving DF evidence; for example, the review of digital forensic analysis reports by both prosecution and defence to agree findings or identify issues or disputes remaining to be resolved before a trial. As well as this, we need a more general programme to communicate positively to the public about DF capabilities and potential¹². Within government, this is a focus of the forensics sub-group of the Criminal Justice Board, which has wide representation from various stakeholders including the Home Office, Ministry of Justice, TF and the FCN. This group will consider and progress further initiatives, such as developing primers covering digital forensic science following the successful introduction of similar primers by the Royal Society on DNA and gait analysis¹³.

FCN Science will play an integral part in this future activity.

Improving our response to rape and sexual offences

A transparent, open attitude towards digital forensic data storage will help to build victims' and witnesses' confidence in all investigations, but especially so and especially important in sexual offences. A more timely and rapid digital forensic service will mean victims and witnesses will get their devices back more quickly, which again should maintain victim and witness confidence in investigations. The forensic information ecosystem will enable investigators to keep individuals informed and assure them of how their data is being handled, stored or shared. Likewise, strong ethical safeguards will ensure that whether victims or suspects, their data will be treated impartially. We will explore how feasible selective extraction or digital escrow are for a proportional approach balancing the needs of investigations with individual privacy, to ensure fairness for all involved in the criminal justice process.

¹² See 'How digital forensics is transforming the Metropolitan Police', Financial Times, 2019, for an example. <https://www.ft.com/content/2d0ef116-ca18-11e9-af46-b079e8bfe40c0>

¹³ <https://royalsociety.org/news/2017/11/royal-society-launches-courtroom-science-primers/>

Communicating public benefit

If we are to achieve what we aim to through this strategy then it is essential that we maintain public support. To do that, we need to demonstrate how valuable DF is to the CJS and the wider public and that we only use DF legitimately. TF commissioned rapid evidence reviews on this topic from Staffordshire University¹⁴. These reviews highlighted a lack of existing evidence to demonstrate the value of DF to criminal justice outcomes. Anecdotally, practitioners and investigators reported that DF examinations added value, but there are no systems in place to measure how many investigations DF science has supported or how prosecutions have depended on it. Likewise, although there is ample research documenting how individual techniques have been developed and applied, the review identified that there are no evaluations of the benefits these techniques bring in an operational context.

To measure and monitor the contribution DF science makes to investigations we need to implement a forensic information ecosystem, available to all DFUs. As outlined previously, this strategy proposes that TF develop the high-level design and roadmap for this system, in agreement with forces, the FCN and CJS partners. It will include appropriate performance measures, based on available data, which TF will work up in close collaboration with the Home Office as part of a wider initiative to develop suitable metrics for measuring DF science performance across the whole CJS¹⁵.

To build the public trust and trust across the wider CJS, the FCN will work in partnership with the Home Office and other Government departments, as well as key stakeholders such as the Victims' Commissioner, to inform future policy and communications strategy in this area. Consulting with and engaging the public as we develop and introduce new techniques will be essential. So too will be testing public opinion to inform how we develop new capabilities. TF and the FCN must adopt an open and traceable approach, developing in partnership with academia and industry to provide constructive challenge and diversity of thought.

Benefits

Strategic benefits

- Improved public trust and enhanced service to victims and witnesses
- Improved awareness and understanding of DF techniques across the CJS, with an emphasis on quality throughout the DF examination process
- Development of an ethical governance model for digital forensic science will provide clear guidance and governance for new capabilities, reducing risks for forces and increasing public confidence
- Development of operational guidance to give forces a clear national approach, ensuring compliance and reducing risk
- Exploring the future potential for privacy preserving technologies will help build public trust and

improve engagement from victims and witnesses with the criminal justice process

- More effective case management to reduce the numbers of cracked trials and risk of miscarriages of justice
- Implementing metrics for DF performance will demonstrate the value DF science adds to the CJS and improve transparency

Tactical benefits

- Increased confidence in DF science leading to secure convictions or acquittals
- Improved traceability and auditing of DF processes through implementation of a forensic information ecosystem, supporting forces in effective information management
- Simplifying compliance with disclosure requirements through structured data storage and effective forensic case management
- Coordinated accreditation activity will reduce the overhead on individual forces, reducing the cost of compliance and enabling quicker progress towards accreditation

¹⁴ Patel, A, "Transforming Forensics Digital project: What works in digital forensics? (Effectiveness of digital forensics techniques)", and Fieldhouse, SJ, "Transforming Forensics Digital: What impact does digital forensic analysis have in improving criminal justice outcomes? (a Rapid Evidence Assessment)", 2019.

¹⁵ https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/796812/Forensics-implementation-plan-April-2019.pdf

Key steps towards delivery

ACTIVITIES	TIMESCALE	TF	CORE FCN	NPCC / APCC	FORCES (FCN MEMBERS)	HO	OTHER
Review the existing policy and legislative framework for the entire scope of DF activities	S	C	C	C	RA	C	I
Provide support to forces to achieve quality standard accreditation.	S	I	RA	I	I	C	C ¹⁶
Explore the future potential for developing and using privacy preserving technologies	S	R	A	I	C	C	C
Develop digital evidence training and awareness-raising material accessible to barristers and the judiciary	S	I	RC	C	C	C	RA ¹⁷
Agree a plan for communication to the public and press about DF capabilities and potential	S	I	R	C	A	I	R ¹⁸
Develop an ethical governance model for digital forensic science.	M	C	R	C	A	C	C
Develop and maintain comprehensive ground truth datasets	M	C	A	I	C	I	R ¹⁹
Develop and improve data control and oversight for the forensic workflow	M	R	A	I	I	C	C

Colour code for timescale for delivery:

Short term activity	0-18 months
Medium term activity	18-36 months
Long term activity	36-60 months

¹⁶Specifically, UKAS and the Forensics Science Regulator
¹⁷Falls within scope of Ministry of Justice
¹⁸Proposed to be delivered by the Criminal Justice Board, Forensic sub-group
¹⁹Currently managed with Defence Science and Technology Laboratory (DSTL) on behalf of Forensic Science Regulator

Code for assigning responsibility:

- R – Responsible
Does the work to complete the activity
- A – Accountable
Accountable for completion of activity
- C – Consult
Provide information for the activity
- I – Inform
Kept informed of activity progress

In Conclusion

In this strategy we propose a national ‘whole system approach’ to build a sustainable, future-proofed DF Science service to deliver the capabilities we need where we need them. DF science capabilities must help policing to outstrip and deal with the criminal threats wherever they come from. The service must keep pace with rapid technological advances and deny criminals the chance to exploit them. We put forward a collaborative approach which will establish a nationally-networked service cutting across all the themes in this strategy and which provides a comprehensive response to the issues and challenges we identified at the outset.

Technology is an essential part of digital forensic science and will be an essential component in transforming DF science. But at its heart this is not simply a technology problem to solve. We need a consistent, collaborative approach to our big challenges – volumes, complexity and legitimacy – and it will take more than technology alone to deliver a rapid, quality assured digital forensic service nationally. To do this, policing must come together on common ways of working. We need a cultural shift in practice, supported by strong governance, if we are to build up this national response to support DF Science to deliver effective and efficient service. The scale of change we need across DF science means that full transformation will take time. So we propose to take a ‘twin track’ approach, combining TF activities which support the longer-term change with ‘quick wins’ delivering rapid operational benefit for DFUs and policing. Everyone involved will collaborate closely with partners to ensure we deliver measurable improvements in service and rapid benefits to the CJS, at the same time ensuring that all activity supports and contributes to the longer-term transformation of DF science.

Through more rapid and responsive DF services, this transformed capability will deliver improved investigative outcomes, preventing and detecting more crime, reducing harm, safeguarding victims and increasing legitimacy and public confidence. It will embed a quality-first approach with a strong ethical foundation to maintain public confidence and trust, and bring innovation and cutting edge technology to DF science, building a continually improving service to tackle whatever challenges the future may bring.

This is an exciting vision for DF science and we can make it a reality in the next five years. We envision a world where evidence is secured quickly and efficiently for investigations and intelligence, and shared securely with prosecutors and disclosed fairly to the defence, where more sensitive and trusted ways of working improve the experience for victims and witnesses, where quality, accuracy and rigour mean that we deliver the best possible value and service to the Criminal Justice System and to the public we serve.

Supporting research

Policing data capture

- **Baseline data capture:** a focused survey completed by a representative sample of 8 UK forces covering DFU demands and challenges, 2018
- **Digital state assessment:** a more detailed survey following on from the baseline data capture, completed by 42 UK forces covering DFU demands, challenges, current capabilities, infrastructure, R&D, staffing and organisation, 2019
- **Typical DFU analysis:** a representative summary of a typical force DFU compiled from analysis of the DSA data, 2019

Original research

- **Impact of ISO17025 accreditation work on UK digital forensic units, Laura Wilkinson and Claire Gwinnett, Staffordshire University, 2019:** literature review and mixed method analysis of survey of UK forces to understand impact of work to achieve ISO17025 accreditation on DFUs, covering challenges, resource requirements and current position
- **Digital Forensics – Future Challenges, a report for NPCC – Transforming Forensics, Gartner, 2019:** an assessment of the current state, challenges and opportunities for UK law enforcement in relation to DF, based on interviews with policing and FSP stakeholders, and research by the global Gartner analyst community
- **Public attitudes on digital forensics, Revealing Reality, 2020:** nationally representative survey,

focus groups and interviews to understand the public awareness of DF capabilities and attitudes towards policing's use of these, covering privacy and consent issues

- **Unleashing the value of digital forensics, Rick Muir and Stephen Walcott, Police Foundation, 2020:** literature review and interviews to understand the challenges and opportunities for digital forensic science to add value to the criminal justice system

Rapid evidence reviews

- **What works in digital forensics? Effectiveness of DF techniques, Dr Asma Patel, Staffordshire University, 2019:** assessing the evidence base for the value of specific DF techniques in an operational context and mapping the existing body of DF techniques
- **What impact does digital forensic analysis have in improving criminal justice outcomes?, Dr Sarah Fieldhouse, Ms Megan Needham, Mr Robin Parsons, Staffordshire University, 2019:** assessing the evidence base for the impact of DF services on criminal justice outcomes nationally and internationally, and suggesting possibilities for future research

Proof of concepts

- **Automation of the digital forensic workflow:** separate deployments in the Metropolitan Police, West Yorkshire Police and East Midlands Special Operations Unit using different tools to automate aspects of the digital forensic process, assessing the impact on capacity,

turnaround time, user satisfaction and other benefits, 2019

- **Central validation:** implementing a standard kiosk level 1 validation package in Staffordshire Police, and assessing the feasibility of establishing a central validation function nationally, 2019

Simulation modelling

A model of core DFU processes showing throughput and turnaround times, developed based on time-and-motion study data shared by the North East Transformation, Innovation and Collaboration (NETIC) initiative, used to model the effect of changes to resourcing, deployment and the automation of process steps, 2020

This research was commissioned to inform the digital forensic science strategy and has not been published separately. For further information, please contact:

contact@transformingforensics.pnn.police.uk

Glossary of Terms

TERM	DEFINITION	URL
Accelerated Capabilities Environment (ACE)	The Accelerated Capability Environment (ACE) solves fast-changing digital and technological challenges facing law enforcement and national security agencies. It brings together expertise from industry and academia to innovate collaboratively and deliver front-line mission impact at pace	https://www.gov.uk/government/groups/accelerated-capability-environment-ace
Accreditation	Formal recognition through external assessment that an organisation is competent to perform specific processes, activities or tasks (which are detailed in a scope of accreditation) in a reliable, credible and accurate manner. Accreditation underpins the quality of results by ensuring their traceability, comparability, validity and commutability	
AI	see Artificial Intelligence	
App	(Application) Alternative referred to as a mobile app, a program for smartphones, or tablets	
Artificial Intelligence	Refers to the simulation of human intelligence in machines that are programmed to think like humans and mimic their actions	
Attorney General	The Attorney General is chief legal adviser to the Crown and has a number of independent public interest functions, as well as overseeing the Law Officers' departments	https://www.gov.uk/government/ministers/attorney-general
Augmented reality (AR)	Blends interactive technology with the real world environment with computer generated visual overlays, sounds and other sensory projections	https://www.livescience.com/34843-augmented-reality.html
Automation	In a digital forensic science context, this refers to linking different examination processes together using software to start each process at the appropriate time, passing relevant data between separate processes to avoid manual intervention or input	
Bandwidth	The transmission capacity of a computer network or other telecommunication system	
Biometrics	Automated recognition of subjects based on their behavioural and biological characteristics for example fingerprints	
Blockchain	A blockchain is a data structure that contains records, called blocks, which are linked together in a cryptographically secure way	
CAID	Child Abuse Image Database, maintained by the Home Office to support rapid identification of images of Child Sexual Exploitation (CSE)	
Callout	An instance of being summoned to deal with an emergency or to provide a service on demand	
Case management system	An IT system which records and tracks progress of (forensic) cases, including the actions taken in respect of submitted evidence items	
CCTV	Closed Circuit Television	
Cell site analysis	Process through which the raw call data records for a phone are used to identify the potential location of the device.	

TERM	DEFINITION	URL
Chips	A small section of a single crystal of semiconductor, usually silicon, that forms the substrate upon which is fabricated a single semiconductor device or all the individual devices comprising an integrated circuit	
CJS	Criminal justice system	
Cloud	An approach to computing in which the end user connects to a remote network of computers (the cloud) in order to run programs, store data, etc. This enables users to access large amounts of data storage and computing power from anywhere in the world without having to own and maintain these resources themselves.	
Cloud First	By Cloud First, we mean the public cloud rather than a community, hybrid or private deployment model	https://www.gov.uk/guidance/government-cloud-first-policy
Cloud services	Remote delivery of computing services over a network (including storage, processing, software, infrastructure) as opposed to the use of locally installed hardware or software. 'The cloud' usually refers to provision of these over the Internet, but private clouds are also used, via dedicated private networks.	
Code of Practice	The Forensic Science Regulator's Code of Practice augments the international standards for forensic science to ensure the UK adopts the highest quality processes for forensic science.	https://www.gov.uk/government/publications/forensic-science-providers-codes-of-practice-and-conduct-2020
College of Policing	Professional body for the police training and development in England and Wales.	
CoP	College of Policing	https://www.college.police.uk/Pages/Home.aspx
Cottage Industry	Business activities in which there are many individuals or small companies are working in a decentralised way.	
CSE	Child sexual exploitation, including indecent images of children (IloC) or child abuse imagery (CAI) investigations.	
CSI	Crime Scene Investigator	
CT	Counter Terrorism	
Cyber-investigations Analysis Standard Expression (CASE)	Cyber-investigation Analysis Standard Expression (CASE) is a community-developed evolving standard that provides a structured (ontology-based) specification for representing information commonly analysed and exchanged by people and systems during investigations involving digital evidence.	https://caseontology.org/
Cyber Security	Protection against the criminal or unauthorised use of electronic data, or the measure taken to achieve this	
Dashcam	A digital camera that that is used in a motor vehicle in order to record what is happening. Some dashcams may also record speed & location	
Data	A defined structure of the pattern of information	
Datasets	A collection of separate sets of information that is treated as a single unit.	
DCG	Data Communications Group	

TERM	DEFINITION	URL
DF	Digital forensics, a colloquial way to refer to digital forensic science	
DFPB	NPCC Digital Forensics Portfolio Board	
DFU	Digital Forensic Unit, a department within a police force dedicated to digital forensic analysis of devices and/or data, staffed by practitioners or specialists. In some forces, may be known as a digital forensic laboratory	
Digital Escrow Solution	A proposed approach to hold digital forensic source data securely, only providing subsets of data in response to an investigative request with clear justification, following a specific line of inquiry	
Digital Forensic Science	The systematic and coherent study of digital traces to address questions of authentication, identification, classification, reconstruction, and evaluation for a legal context	https://www.nist.gov/system/files/documents/2018/01/10/osac_ts_0002.pdf
Digital Forensics Market Operations Group (DFMOG)	NPCC managed group to monitor the commercial issues relating to the outsourced digital forensic marketplace	https://www.npcc.police.uk/
Digital State Assessment	A survey of all forces carried out by TF in 2019 to capture a baseline of their current state in relation to key DF measures such as volume, staffing, technical infrastructure, etc	
DII	Digital Intelligence and Investigation, a project within the College of Policing	
Disclosure	The legal requirement for the prosecution to provide any material to the defence which may assist the defence case, or undermine the prosecution case	
DMI	Digital Media Investigator. The Digital Media Investigator supports major crime, incidents, operations or any investigation that requires specialist digital investigative assistance	
DNA	A self replicating material which is present in nearly all living organisms as the main constituent of chromosomes. It is the carrier of genetic information	
Encryption	Procedure used in cryptography to convert plain text into cipher to prevent anyone but the intended recipient from reading/accessing that data	
eQMS	Electronic Quality Management System	
EU Horizon 2020 programme	European Union research and innovation programme.	https://ec.europa.eu/programmes/horizon2020/en
Facial Recognition	A facial recognition system is a technology capable of identifying or verifying a person's identity from a digital image or a video frame from a video source.	
FCN Commercial pillar	Team within the Forensic Capability Network dedicated to supporting the forensics marketplace.	
FCN Operations pillar	Team within the Forensic Capability Network dedicated to maximising resilience and effectiveness through supporting new ICT delivery.	
FCN Quality pillar	Team within the Forensic Capability Network dedicated to achieving and maintaining a quality service with efficient, standardised processes.	

TERM	DEFINITION	URL
FCN Science pillar	Team within the Forensic Capability Network dedicated to identifying and exploiting opportunities so members can meet future challenges by having the people, knowledge, skills, and specialist tools and capabilities they need.	
FCN Xchange	Cloud platform to store and process forensic data, and provide access to forensic tools	
Fitbit	Brand of activity tracker.	
Forensic Science Regulator	A government appointee responsible for ensuring that the provision of forensic science services across the criminal justice system is subject to an appropriate regime of scientific quality standards.	
FSP	Forensic Service Provider, a commercial company providing forensic science services.	
FSR	See Forensic Science Regulator	
FTE	Full time equivalent - a way to express staffing equivalent to a single full time role. For example, two part time staff working 2.5 days each are equivalent to one FTE	
Gait Analysis	Anatomical and biomechanical analysis of the walking and body movement of individuals that are captured on CCTV	
GDPR	General Data Protection Regulation: a legal act of the European Union intended to protect people's personal data	https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/711097/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf
Hardware	The physical portion of a computer system, including the electrical/ electronic components (e.g. devices and circuits), electromechanical components (e.g. a disk drive), and mechanical (e.g. cabinet) components	
HMRC	Her Majesty's Revenue and Customs	https://www.gov.uk/government/organisations/hm-revenue-customs
House of Lords	Upper house of Parliament of the United Kingdom which debates legislation and has the power to amend or reject bills	https://www.parliament.uk/business/lords/
House of Lords Science and Technology committee	The science and technology committee is appointed to consider science and technology developments and reports back to the House of Lords	https://www.parliament.uk/business/committees/committees-a-z/lords-select/science-and-technology-committee/publications/
ICO	Information Commissioner's Office, the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.	http://www.ico.org.uk
ICT	Information and communications technology	
Internet of Things (IoT)	The interconnection via the internet of computing devices embedded into everyday objects, enabling them to send and receive data (i.e. speakers, wearable technology)	

TERM	DEFINITION	URL
ISO17020	Specifies requirements for the competence of bodies performing inspection and for the impartiality and consistency of their inspection activities. In a digital forensic context, ISO17020 is the standard applicable to on-scene forensic activities	
ISO17025	Specifies the general requirements for the competence to carry out tests and/or calibrations, including sampling. It covers testing and calibration performed using standard methods, non-standard methods, and laboratory-developed methods. In a digital forensic context, ISO17025 is the standard applicable to digital forensic activities including extraction, processing, analysis and reporting	
IT	Information Technology	
Kiosk	A generic term used to refer to a preconfigured 'off the shelf tool' used to extract or review digital data from devices, using a simplified locked-down workflow	
Legacy data	Digital forensic data generated or seized in preparation for, or as a result of, past digital forensic examinations	
Machine learning	A subset of artificial intelligence, involving algorithms that 'learn' and improve performance based on input data, without being explicitly programmed	
Machine to Machine Interaction	Also known as M2M, direct communication between devices using any communication channel	
Media forensics	The use of specialist digital forensic techniques to examine audio or video evidence, e.g. to authenticate audio recordings	
Ministry of Justice	Ministerial department of the British Government.	https://www.gov.uk/government/organisations/ministry-of-justice
National Digital Forensic Configuration Authority (NDFCA)	The configuration authority is an individual or body within the "entity" that ensures that digital forensic deployments, their method(s) and workflow(s) are preconfigured, deployed, maintained and quality assured, and operators are competent and authorised as set out in the Forensic Science Regulator's (FSR) Codes of Practice and Conduct.	
National Disclosure Improvement Plan	Joint National Disclosure Improvement Plan is to address issues that will result in improved disclosure processes and procedures.	https://www.cps.gov.uk/publication/national-disclosure-improvement-plan
National Police Chiefs' Council	National Police Chiefs' Council - The NPCC brings police forces in the UK together to help policing coordinate operations, reform, improve and provide value for money.	https://www.npcc.police.uk/
National Policing Digital Strategy	National Digital Policing Strategy 2020-2030: Digital, Data and Technology Strategy, co-authored by the National Police Technology Council and the Police ICT Company.	https://ict.police.uk/wp-content/uploads/2020/01/National-Policing-Digital-Strategy-2020-2030.pdf
National Policing Technology Council	Oversees and strategises technology within policing at a national level.	https://ict.police.uk/governance/
NCA	National Crime Agency	https://www.nationalcrimeagency.gov.uk/

TERM	DEFINITION	URL
Niche	A specialised segment of the market for a particular kind of product or service	
NPCC	See National Police Chiefs' Council	
Offline	Not controlled by or directly connected to a computer or the internet.	
PCC	Police and Crime Commissioner, an elected official who is responsible for holding the Chief Constable of a force to account	
Personal data	Personal data is information that relates to an identified or identifiable individual	
PICT Co	See Police ICT Company	
Police ICT Company	Policing Technology partner	https://ict.police.uk/about-us/
Policing Education Quality Framework (PRQF)	Professional framework for the training of police officers and staff	https://www.college.police.uk/What-we-do/Learning/Policing-Education-Qualifications-Framework/Pages/Policing-Education-Qualifications-Framework.aspx
Policing Vision 2025	NPCC's Policing Vision 2025 sets out a plan for policing over the next ten years. It will shape decisions around transformation and how we use our resources to help to keep people safe and provide an effective, accessible and value for money service that can be trusted	https://www.npcc.police.uk/documents/Policing%20Vision.pdf
Processing power	Speed in which a computer can perform tasks and interact with applications	
R&D	Research and development, innovation, introduction, and improvement of new and existing digital forensic processes or strategies to further DF value within policing	
Retention	<i>Data retention</i> defines the policies of persistent data and records management for meeting legal and business data archival requirements. <i>Staff retention</i> is the aim of maintaining existing staffing resource over time.	
ROCU	Regional Organised Crime Unit	https://www.ncsc.gov.uk/information/regional-organised-crime-units-rocus
Section 22 agreement	Agreement made by policing bodies to collaborate, in line with the requirements of section 22A of the Police Act 1996.	
SFO	Serious Fraud Office	
Software	A collection of instructions that enable the user to interact with a computer, its hardware or perform tasks	
SOP	Standard Operating Procedure, a documented, repeatable and consistent method of working	
STEM	Science, Technology, Engineering, and Mathematics	
TB (Terabyte)	"Terabyte" is a measurement of data, capacity or quantity of data (for example 1000 gigabytes)	

TERM	DEFINITION	URL
TF	Transforming Forensics, an NPCC programme to deliver transformational change in forensic service delivery within policing	
Tool	A program that is employed in the development, analysis, repair, or enhancement of other programs or of hardware. Traditionally a set of software tools.	
Triage	The process by which you collect, assemble, analyse, and prioritise digital evidence from a crime or investigation to support investigative decision-making	
Turnaround time	The time between the submission of an item for digital forensic analysis and the provision of findings/results to the submitting officer	
UCL	University College London	https://www.ucl.ac.uk/
UKAS	UK Accreditation Service	https://www.ukas.com/
UKRI	UK Research and Innovation	https://www.ukri.org/
Validation	Validation is the confirmation by examination and the provision of objective evidence that the particular requirements for a specific intended use are fulfilled	
Weeding	Systematic removal of resources from a collection of data or information based on selected criteria	
Skills for Justice National Occupational Standards	Statements of the standards of performance individuals must achieve when carrying out functions in the workplace, from Skills for Justice	https://www.sfjuk.com/resources
Defence Science & Technology Laboratory (DSTL)	Dstl is an executive agency, sponsored by the Ministry of Defence, which ensures that innovative science and technology contribute to the defence and security of the UK	https://www.gov.uk/government/organisations/defence-science-and-technology-laboratory/about



TRANSFORMING
FORENSICS



Forensic
Capability
Network



NPCC
National Police Chiefs' Council



Association of
Police and Crime
Commissioners

Digital Forensic Science Strategy

www.fcn.police.uk
contact@transformingforensics.co.uk

July 2020