HMICFRS

His Majesty's Inspectorate of Constabulary and Fire & Rescue Services

Digital forensics

An inspection into how well the police and other agencies use digital forensics in their investigations

Contents

Foreword

The use of digital media, digital devices and social media has exploded in the past decade. Twenty years ago, few could have imagined quite how pervasive digital technology would become in our lives.

Many of us take for granted mobile phones that are like pocket computers, electronic devices that can be activated from across the world, or homes with more, and better-quality, cameras than many business premises had in the early 2000s. These advances in technology inevitably influence the way the police respond to crimes and victims. And how they gather evidence of crimes from a range of devices, now commonly referred to as digital forensics.

Technology can be used to commit or help commit crimes. This can take the form of offenders using devices to access social media and harass, bully or stalk victims, or organised crime groups communicating internationally using digital encrypted devices. With fraud rapidly increasing online and the growing fear of cybercrime, the digital age presents real problems for those responsible for keeping the public safe. Unless improvements in digital forensics are made, policing will fall further behind in this digital revolution.

These technological advances shouldn't be seen just as threats; they bring opportunities too. For decades, policing has relied on forensic science to help catch and convict criminals. The use of fingerprint, DNA and other forensic evidence is now commonplace in court proceedings. Forensic science is generally well regulated, professional and trusted. The police and Crown Prosecution Service (CPS) understand how to gather, assess and use this evidence effectively in court to bring criminals to justice. These types of evidence remain important to policing. But the rapid emergence of a digital society, in which most people carry mobile devices, has created a huge opportunity for police to gather new types of evidence of crimes and identify criminals.

During this inspection, we examined how effective the police are at providing digital forensics to secure evidence of crime and protect victims. It has become increasingly clear that the police service hasn't kept pace with the scale of the challenges they face. In some cases, we found that the police simply didn't understand what digital forensics meant. We found a national backlog of over 25,000 devices waiting to be examined. This didn't include all the devices likely to be in the system.

We found delays in some areas so egregious that victims were being failed. In some areas, the system of digital forensic examination is slow, ineffective and less professionally managed than the other police forensic disciplines. We also had little confidence that the police service had a coherent plan for improving the current situation.

We found that the needs of victims were rarely taken into consideration when the police seized digital devices for examination to secure evidence of crime. In an age where so many live on and through these devices, there appears to be little recognition of the effect this can have on an already traumatised victim.

Some victims' phones and mobile devices, containing a range of personal information and contacts, were kept by the police for many months. This hasn't served the criminal justice system well. To compound the issue, there are no set standards or oversight of services. All too often, victims of serious offences are receiving a poorer service as a result.

Some forces are leading the way with their improved response to crimes with digital forensic evidence and the treatment of victims. But we found little evidence of this being more widely shared and adopted by others. Too often, victims are being let down by a postcode lottery: their experience depends too heavily on the force area they live in. The time period for forces to start examining devices varies widely. Better performing forces start within weeks, whereas others start within 18 months. This gulf in performance cannot continue.

In our inspection, we didn't see enough examples of policing making effective and efficient use of digital forensics. Many forces didn't have a sufficient level of understanding of the work involved to recover evidence from mobile phones, computers and other digital devices.

Policing has often developed solutions to national issues by using training or authorised professional practice, or co-ordinating best practice. This can be seen in many areas: one example is the examination and recovery of ballistic material, such as bullets and cartridges, from crime scenes. Regardless of where in the country the crime scene is, crime scene managers and investigators examine and recover any firearm or ballistic material in a set way. This process been designed by scientists to get as much forensic information as possible from each scene. This isn't the same in digital forensics. Until this consistency of approach is achieved, victims will continue to suffer.

There is a clear precedent for the professionalisation of digital forensics. But few forces are following this model. While other police forensic evidence techniques serve the public well, we can't yet say the same for digital forensic evidence.

There are obvious challenges. The scale of information that can be recovered from the examination of digital devices can be huge, with some mobile phones now able to store 130,000 digital images and other data. Extracting and storing this information is a problem the police service and the CPS haven't yet resolved. And the disclosure of this material, in accordance with legislation, continues to present difficulties too.

But digital devices have been with us for years and their development – bigger storage, more involvement in crime and more potential for evidence – will accelerate. And yet this inspection paints a sorry picture. The police service, working with the Home Office and the CPS, must do more to improve how digital forensics is developed now and in future. The alternative is a worsening failure to keep pace with the activities of criminals and the expectations of victims and witnesses.

Summary

In this inspection, we examined the provision of digital forensics in police forces and regional organised crime units. We considered whether they understood and could manage their demand, and whether victims of crime were receiving a quality service.

Digital forensics is a branch of forensic science, which includes the recovery and examination of digital devices. Today most, if not all, crimes have some form of digital footprint. We found that the demand for digital forensic examinations was increasing year on year, and in some cases outstripped the capacity of forces to respond effectively.

During this inspection we found that, nationally, there were over 25,000 devices waiting for a digital forensic examination. In 2013, a smartphone stored on average 16GB of data, equivalent to about 15 books. Today's smartphones can retain 128GB of data, equivalent to the books on about 90 metres of bookshelves. The sheer scale of the information held on mobile devices today presents one of the greatest challenges to law enforcement's ability to secure and preserve evidence.

The current increase in demand is unlikely to stop. This causes delays to investigations that affect victims, witnesses and suspects. Delays in examination of devices carry many risks. In some cases, devices held by police may contain sensitive information, such as child sexual abuse, drugs and firearm material. In some forces, this can go unnoticed until examined many months after the devices have been seized.

We make nine recommendations to improve the efficiency and effectiveness of digital forensic services.

Understanding current demand

During our inspection we found an inconsistent approach to how forces recovered and examined digital devices. In some forces senior leaders didn't fully understand current demand for digital forensics, and the subsequent effect on investigations and victims. This lack of understanding is part of the reason for an insufficient focus, in some forces, on the problems. The result is long delays in some investigations, and victims and witnesses losing access to their mobile phones for many months.

There is a national digital forensic strategy. We expected to find forces had adapted this into a plan to meet the demands of digital forensics locally. Only two of the forces

we visited had such a plan. We also found there was no effective governance or oversight, either nationally or locally, to help understand demand now, or increased demand in the future.

The lack of understanding of current demand had a knock-on effect in how forces prioritised examinations, and how they matched skills and resources to their response. Policing needs to work harder to fully understand current demand and put effective governance and performance structures in place. This would help establish good practice and improve the service to the public.

We found that investigators didn't always understand how to manage digital forensic opportunities at crime scenes. Many forces have digital media investigators (DMIs) who are trained and skilled in identifying and securing digital evidence. Their role is to support crime investigators. But there aren't enough of them. It is often their secondary role in their force, and they aren't as widely used as they should be. More effective use of DMIs will reduce demand by improving the initial decision-making at crime scenes about whether or not to seize devices.

Prioritisation

Once seized, digital devices require examination, and relevant information then needs to be extracted and assessed. We found that all forces had a triage process to prioritise the examination of devices by allocating a grading. This was done mainly on the facts of the case. The views of victims or witnesses, or wider safeguarding issues, weren't always considered. We also found that the decision on grading and examination of devices was rarely, if ever, reviewed unless requested by an investigator.

Even after triage there were vastly differing operating practices. In some forces we found limited waiting times, whereas in others we found that a similar case could wait months for examination to begin. This amounts to a postcode lottery for victims, who are often vulnerable.

Investigators reported incidents of prosecutors being overly cautious, requesting unnecessary examinations. We found that policies regarding disclosure and digital material were in place. Such issues should be managed via local criminal justice boards. For persistent issues there may be a requirement for the National Police Chiefs' Council and the Crown Prosecution Service to intervene.

We found encouraging evidence that forces had a plan to examine victims' devices within 24 hours in rape or serious sexual offence cases. It is too early to fully assess the success of these plans; we will revisit this area in future inspections. Forces should make sure that digital forensics services are effective for all victims and witnesses, not just those involved in rape or serious sexual offence cases. Their support and safeguarding must be the priority.

Capability and capacity

Policing needs to have the right number of staff, properly trained and equipped, supported by realistic finance plans, to effectively provide digital forensic services. Few forces have this in place to meet demand currently.

The main resources to obtain digital forensic evidence are digital forensic kiosks and digital forensic units. Both are used to extract information and evidence from digital devices. Most forces have invested in their digital forensic units, but often demand is still not being met. Most forces have also invested in staff and technologies in this area; however, the gap between the demand and these resources is still too great.

The use of digital kiosks to provide initial analysis and support volume crime investigations is widespread. However, we found that the staff using these kiosks were often unsupervised. Improving the process for kiosk use is likely to improve digital forensic performance.

We found little evidence of collaboration, regionally or nationally. This is disappointing, especially around procurement and shared access to specialist equipment. Technology to extract digital evidence is often expensive and may be beyond the reach of many forces. Collaboration between forces is likely to be more efficient and effective in building greater capacity and capability.

The technology and skilled staff required to provide digital forensics is often expensive. We found that financial leaders didn't always understand what was required, and digital forensics wasn't linked to force strategies or plans. This has led to business cases, submitted by unit heads, being considered in isolation and not as part of a co-ordinated plan.

This emphasises the need for local plans to implement the existing national strategy. Funding is available, but we found it was often unco-ordinated, with some forces missing opportunities due to a lack of awareness. This needs better co-ordination via the Home Office and National Police Chiefs' Council.

Accreditation and training

Any public or private body that provides digital forensic services must comply with the Forensic Science Regulator's codes of practice and conduct, including achieving accreditation to international standards. The United Kingdom Accreditation Service, as the UK Government-designated national accreditation body, undertakes assessment of organisations to international standards.

Everyone we asked about accreditation said it was essential, but most told us that the process was bureaucratic and costly. To achieve accreditation, there will undoubtedly be a cost to individual forces. Every force in England and Wales was seeking accreditation in one or more digital forensic services at the time of our inspection. In addition, other law enforcement agencies were similarly seeking accreditation.

To achieve and maintain accreditations for all these organisations isn't only expensive, but also leads to unnecessary duplication and will be nearly impossible long term.

Unless law enforcement moves away from so many varied approaches to achieving accreditation and towards a more co-ordinated response, the public will continue to receive a very different level of service across the country. Police and other agencies need to work with the Forensic Science Regulator to design a more efficient process that better serves the needs of the public.

The College of Policing has several digital forensic training programmes. However, too few officers and staff areas are being given access to this training. We didn't find any examples of forces trying to collaborate with private businesses to benefit from the sharing of skills and technologies. There are few career pathways for specialist staff in digital forensics. The police service with the College of Policing need to address this and improve educational opportunities for frontline responders and investigators.

Future plans

We found little evidence that forces had plans in place to respond to anticipated future demand. This isn't surprising given that many forces don't understand the current demand. For example, few forces could explain how they would meet upcoming challenges and developing technologies.

Secure storage of digital data is a significant problem. We found most forces were struggling to keep pace with the amount of storage required and to comply with management of police information guidance. We were told that the most likely long-term solution was cloud-based storage (the on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user). Despite this, we found only a few forces actively pursuing this option. Some were reluctant to consider cloud-based solutions because of security concerns and legal requirements. Some forces have sought legal advice to use the cloud for data storage. His Majesty's Revenue & Customs now uses the cloud for storage and examination of digital data. But there is still no national guidance to provide clarity and direction on this subject.

Policing can't meet the technological challenges alone. It will be expensive and often beyond the police's abilities. There needs to be a co-ordinated effort to work together with forensic providers and other private businesses to develop and share skills and technology. Yet we found little evidence of this happening through any form of collaboration.

Recommendations and areas for improvement

We have made nine recommendations in this report.

Understanding demand

Recommendation 1

By April 2023, the National Police Chiefs' Council should appoint a dedicated lead for digital forensics, who should, by July 2023, develop a governance and oversight framework to better understand the national demand for digital forensic services.

Recommendation 2

By December 2023, each force in England and Wales should develop a governance and oversight framework to better understand the local demand for digital forensic services.

Prioritisation

Recommendation 3

By April 2024, the National Police Chiefs' Council, supported by the College of Policing, should encourage an increase in the number of dedicated, competent and trained digital media investigators available to advise investigators and at crime scenes.

Recommendation 4

By September 2023, the National Police Chiefs' Council and all forces within England and Wales need to include the management of digital forensic kiosks in their governance and oversight frameworks.

Capacity and capability

Recommendation 5

By April 2023, the Home Office should review digital forensic budgets and funding. Future additional funding should support the national digital forensic strategy and be well communicated and easier to access.

Training and accreditation

Recommendation 6

By April 2023, the College of Policing should make sure all its digital courses have sufficient focus on investigations and victims' needs.

Future plans

Recommendation 7

By June 2023, the National Police Chiefs' Council lead for digital forensics, the Home Office and relevant support services should provide guidance to all forces on the use of cloud-based storage and computing power.

Recommendation 8

By November 2024, chief constables should integrate digital forensic services under their existing forensic science structure.

Recommendation 9

By November 2024, the Home Office should work with the National Police Chiefs' Council, the College of Policing and the private sector to design an alternative operating model that would provide effective and sustainable digital forensic services to support police investigations.

Introduction

Background and context

Digital forensics is a branch of forensic science. The main purpose is to examine, extract and process data from digital devices. This science must use sound forensic techniques to have credibility in the criminal justice process.

Almost every criminal investigation has opportunities to recover digital evidence, whether from computers, mobile phones, CCTV, GPS systems or other digital devices. But recovering this data as evidence comes at a cost and isn't always easy. Many law enforcement bodies are struggling to keep pace with advances in technology. The volume of data that is stored on devices often makes examinations complex and lengthy.

Traditionally, computer examinations were carried out by small specialist teams, operating independently, such as high-tech crime units. As technology has developed and demand increased, these teams have grown. This growth has often been unstructured, with little or no planning or expansion strategy to respond to the increased number of digital forensic examinations.

The police service is struggling to meet the demands placed on it by the digital age. It currently lacks a solid foundation on which to build a co-ordinated response to improve how it manages digital forensic services.

About us

His Majesty's Inspectorate of Constabulary and Fire & Rescue Services independently assesses the effectiveness and efficiency of police forces and fire and rescue services in England and Wales, in the public interest. In preparing our reports we ask the questions that citizens would ask.

Our terms of reference

Our 2021/22 inspection programme and framework included the thematic inspection of digital forensics.

In this inspection, we examined how effective the provision of digital forensics is in forces and regional organised crime units (ROCUs), and how well they understand and plan for future demand.

Our terms of reference for this inspection, which were agreed following consultation with the Home Office, were to consider whether:

- forces and ROCUs understand current demand from digital forensics, and the impact this has on investigations, victims and outcomes;
- forces and ROCUs prioritise and carry out examinations for the benefit of victims;
- forces and ROCUs have sufficient capacity and capability to meet demand, and whether they use external providers effectively;
- forces have sufficient accredited resources or consider whether commercial providers have established quality management regimes, validation and accreditation; and
- forces and ROCUs have sufficient plans to meet future demand.

Methodology

We structured the inspection into the following areas:

- understanding current demand;
- prioritisation;
- capability and capacity;
- training and accreditation; and
- future plans.

We reviewed documents provided by the National Police Chiefs' Council, United Kingdom Accreditation Service, Forensic Science Regulator and the College of Policing, as well as the 43 force management statements.

Fieldwork for the inspection took place between February and May 2022. We used a common set of questions and interviewed personnel in similar roles in each of the forces and ROCUs we visited.

During our inspection we visited eight police forces and four ROCUs in England and Wales. We also visited the National Crime Agency, British Transport Police, the City of London Police, Her Majesty's Revenue & Customs, and the Crown Prosecution Service. We spoke with the National Police Chiefs' Council lead for digital forensics and the Forensic Science Regulator, and visited an independent digital forensic laboratory.

During each visit we held interviews or focus groups with relevant personnel. We also interviewed chief officers and some police and crime commissioners as part of our inspection.

Understanding current demand

This chapter covers:

- national understanding of digital forensics;
- local understanding of digital forensics;
- scene management; and
- digital media investigators.

Advances in technology offer police and other law enforcement agencies the opportunity to provide better services to victims and communities in many ways. Within criminal investigations, this has fundamentally changed how police and other law enforcement agencies look for and gather evidence. The traditional approach to investigations, relying on witnesses, fingerprints and DNA, is being overtaken by the 'digital footprint' we all leave. It requires all of law enforcement to think and operate differently, and while some have started to adapt, many lag behind.

There is evidence that organised crime groups and other criminals are exploiting technology to commit crime and evade detection. The police must better understand the demand generated by digital forensics if it is to make sure there are enough staff with the skills to investigate crime in this digital age.

During our inspection we found an inconsistent approach to digital forensics. We found some senior leaders didn't understand current demand or how this affected investigations, and, more importantly, the impact it had on victims.

National understanding of digital forensic demand

The police service doesn't understand the demand for digital forensic examinations. And we have little confidence that it understands how much policing will rely on this type of evidence in the future.

Accurate information illustrating national demand isn't collected. Some national data was collected between May 2020 and August 2022. This data suggested that in June 2020 there were approximately 19,000 devices awaiting examination in digital forensic units (DFUs). By August 2022, this figure had risen to approximately 25,000 devices, an increase of 32 percent in two years.

The benefits of digital forensic evidence are now increasingly being understood by many investigators. Across England and Wales this has led to an exponential increase in the demand for examination of an array of digital devices. Yet we found little evidence that the service understood the volume of examinations, the scale of data to be extracted, or the time required to gather evidence effectively and efficiently.

This situation is different from how forces manage other forensics services such as DNA, fingerprints and image capture, where the level of demand is better understood and resources are provided to meet that demand.

Nationally, the development of digital forensics is managed by the National Police Chiefs' Council (NPCC, which brings UK police forces together to help them co-ordinate operations, reform, improve, and provide value for money) as part of its forensics portfolio board. A deputy chief constable chairs this board, and the current lead has three portfolios to manage, including digital forensics.

In 2020, the *Digital Forensic Science Strategy* was published on behalf of the NPCC and the Association of Police and Crime Commissioners. This contains six projects to support its overall aim of transformational change to digital forensic science:

- improving operations;
- developing the workforce;
- building trust;
- improving commercial practice;
- meeting the data challenge; and
- research and innovation.

There is a national strategy and some governance of digital forensic services being developed. But there is no governance or oversight associated with the provision of digital forensic services across England and Wales. As a result, there is no co-ordinated response from the service to address the existing backlogs, fluctuations in demand, and an absence of trained and accredited specialists. There is also a lack of any data being collected to measure demand across the system. This means that it is impossible to judge whether, now and in the future, the level of resources can cope with the growing reliance on digital evidence.

The absence of a clear picture of how much work digital forensic examinations create, in the collection, storage, analysis and then presentation at court, means the service is ill-prepared to respond to any further growth in digital devices. Victims are being let down as demand overwhelms some police forces.

We see that there is an urgent need for policing to focus on digital forensic improvements. This would be made easier with a dedicated NPCC lead to focus on the challenges raised in this report. Other key areas of policing, for example violence against women and girls, and serious and organised crime, already have a

dedicated NPCC lead. There is also a need for the NPCC to develop a national governance structure that includes a performance framework aimed at improving services to victims. These should be replicated locally, providing a clearer picture of demand to support planning and investment.

Recommendation 1

By April 2023, the National Police Chiefs' Council should appoint a dedicated lead for digital forensics, who should, by July 2023, develop a governance and oversight framework to better understand the national demand for digital forensic services.

Recommendation 2

By December 2023, each force in England and Wales should develop a governance and oversight framework to better understand the local demand for digital forensic services.

Local understanding of digital forensic demand

The volume of demand continues to grow, and we found that some forces had a backlog of over a year to examine devices. The potential for generating high-quality evidence from digital devices almost inevitably drives this increase in demand. As a result, there will always be devices waiting to be examined and some, by the nature of the work, will take considerable time to complete.

However, in many cases the time taken is too long. Investigators cited long delays to receive examination results, often exceeding service level agreements. This often extends investigations and has a negative impact on the victim. One example provided was the rape of a seven-year-old girl. Due to delays in digital forensic processes, the victim was nine years old by the time the evidence was returned to allow the suspect to be charged.

The pace of change in digital forensics has led to forces creating digital forensic capabilities that are, in some cases, not able to respond to their current demand. We found that this evolution of teams and units was often developed without a clear strategy or plans for how that demand is likely to change and grow. DFUs appeared to have grown organically in response to increased pressure. The service and individual forces have been slow to realise that the equipment, units, staff and skills they have aren't fit, in many cases, to respond effectively to the digital forensic age. This is despite digital imagery and data capture being in mainstream society for many years now.

Few forces could quantify the true scale of their digital forensic demand. For example, we found a lack of detailed information around the number of devices requiring

examination, which hadn't yet been submitted to the DFU. There was also no assessment of the time it would take to examine devices generally. Without this information it is impossible for forces to plan for now and invest for the future.

During our inspection, we found no single consistent organisational structure across the forces we visited. In some cases, DFUs were part of investigation departments, and in others they were part of a combined forensic structure. There is no definitive model and forces have adopted structures that suit local needs. However, units often appeared isolated within force structures, and struggled to secure support from finance, human resource, and IT departments.

In many forces we visited there were a small number of specialists managing digital forensic services. And senior leaders we interviewed made clear that they relied heavily on those specialists. However, we found little evidence of any succession planning or resilience in these key roles. We encourage forces to develop plans to build resilience in this highly specialised area.

We spoke to leaders within the DFUs we visited. Overwhelmingly they were knowledgeable, passionate and striving to provide the best service possible. Improvements in performance and capability were often the direct result of their endeavours.

We did find examples of forces developing their understanding of current demand. For example, Gwent Police prepared a workforce plan that aligned appropriate numbers of staff to digital forensic demand. But this was an exception, with other forces less well advanced in assessing demand.

We believe it is essential that digital forensic governance is incorporated into force performance frameworks. This will provide senior leaders with the information to assess risks and make better resourcing decisions.

Scene management

Some forces have increased staff and introduced new technologies to try and keep pace with growing demand. But this is unlikely to work on its own, and better management of crime scenes is needed. The initial approach to identifying, seizing and examining digital devices must become more sophisticated. Subjecting devices to an initial assessment at the scene is an effective way of reducing the number of devices submitted to DFUs for examination.

We saw examples of forces using fully equipped digital forensic examination vans to attend crime scenes. This approach allowed investigators and examiners to conduct initial assessments of digital devices in a secure and sterile environment, without the need to seize and retain large numbers. In many forces, these are known as 'digi-vans'. They carry specialist tools, which can be used to help differentiate between devices likely to contain evidential material, and those less likely to help in an investigation. This process also helps investigators decide which devices to submit to

DFUs for more detailed examination. As well as reducing demand on DFUs, this practice also prevents devices being kept from owners for months, simply to make sure there is no evidential material.

Staged and sequential examination of exhibits for traditional forensic techniques is well established. Examinations are selective and designed to secure the best evidence, without examining and testing every item or mark. We found that the approach to digital examinations wasn't as systematic as this. Making improvements in this approach will reduce demand on DFUs and the time taken to review material, and reduce delays to investigations.

Digital media investigators

Digital media investigators (DMIs) are a significant asset in better managing crime scenes and improving investigations that involve digital device evidence. But there aren't enough of them, they aren't being sufficiently trained and developed, and they aren't being used properly.

The use of crime scene managers (CSMs) and investigative strategies to support investigators is commonplace. Generally though, the knowledge and experience of CSMs relate to traditional crime scenes, where they advise on securing fingerprints, imagery and DNA, among other things. Many lack experience or training in how to preserve and secure digital evidence.

Investigators must be able to identify, prioritise and manage opportunities for digital evidence at crime scenes. This often requires specialist knowledge, such as how to manage volatile data (any data that is stored in memory, exists in transit, that will be lost when the device loses power or is turned off).

Many forces aren't able to provide this service at crime scenes. This inconsistent approach in accessing cloud information poses a real risk of investigators missing digital opportunities to solve more crime. We found many examples of investigators lacking the required skills or training to do this. The role of DMIs, who have some expertise in recovering digital evidence, can provide this support to investigators.

We found that most forces still didn't have enough DMIs, and they were mainly being used to support serious crime incidents. Consequently, volume crime investigators are unable to access specialist support, from either CSMs or DMIs. This is more likely to lead to wrong decisions being made at crime scenes, including too many exhibits being seized. And in some cases, unnecessary requests for examination of devices being made. This adds extra demand to an already overburdened system. Staff in focus groups told us that resulting delays were a significant issue and contributed to failed prosecutions.

This initial response to digital crime scene examination must improve. There is a clear need for wider use of DMIs. Policing has a blueprint for forensic management of crime

scenes involving CSMs and crime scene investigators. The use of DMIs should develop similarly.

Innovative practice: Managing digital crime scenes

We found examples of forces making significant improvements in this area.

Bedfordshire Police reviewed the effectiveness of its digital forensic service. It appointed a senior leader, who reported directly to the chief officer team. This resulted in the force reorganising its services and investing in technology. It introduced digital media investigators who work closely with crime scene investigators to help fill gaps in knowledge. The digital media investigators:

- provide advice and attend crime scenes (sometimes using digi-vans);
- help crime scene investigators develop investigative strategies; and
- liaise with the digital forensic unit to agree staged submissions, based on the circumstances of each investigation.

As a result, the force can show reductions in demand for the digital forensic unit, shorter examination times, and reduced backlogs.

Greater Manchester Police's digital forensic unit is developing and using tactics to obtain cloud-based evidence from scenes, often remotely. It provided two case studies to illustrate how crucial evidence relating to investigations had been obtained, which may otherwise have been missed.

Recommendation 3

By April 2024, the National Police Chiefs' Council, supported by the College of Policing, should encourage an increase in the number of dedicated, competent and trained digital media investigators available to advise investigators and at crime scenes.

Prioritisation

This chapter covers:

- examination of digital devices;
- triage processes;
- disclosure; and
- impact on investigations and victims.

The challenge facing policing to meet the demands of digital forensic examinations became increasingly apparent during this inspection. Effective management of demand coming into digital forensic units (DFUs) is essential and allows proper prioritisation, which makes sure that high-risk crimes receive the priority service required. However, this was found to be lacking in some forces.

During our inspection visits we found a mixed picture. There was no standard process of prioritisation across the forces we inspected and target times for examinations to begin varied widely from force to force.

Examination of digital devices

Although capabilities vary across England and Wales, there are essentially three levels of data examination and extraction from digital devices, namely:

- **Level 1** – configured logical extraction – digital forensic kiosks (DFKs) and mobile capabilities, providing triage and early examination.
- **Level 2** – logical and physical extraction – digital forensic units or laboratories, or forensic service providers.
- **Level 3** – specialist extractions and examinations – central digital forensic laboratories or forensic service providers.

Level 1 examinations: digital forensic kiosks

Devices that have been seized need to be assessed to reach a decision on whether they should be examined for evidence. DFKs can be used to help with this assessment. They use software applications to preview and, when necessary, extract data from a range of digital devices, including mobile phones, SIM cards and hard drives. Using these software applications as part of the initial assessment makes prioritising digital devices more efficient.

Forces aren't using these kiosks as effectively as they should, and this is affecting victims and the quality of investigations. Forces need to improve how they co-ordinate and supervise the use of this equipment and those who operate them.

Importantly, DFKs are generally accessible to frontline officers, allowing for prompt review of seized devices. However, there are limitations. No single extraction system guarantees recovering all stored material. Level 1 kiosk examinations are generally the least reliable.

We found that generally the staff trained in the use of kiosks did this in addition to other roles, and that they worked in various departments. This means that to undertake digital examinations using the kiosks, these staff must be taken away from their other work. Securing help from these staff often relies on goodwill and them being allowed time away from their primary role. We also found some occasions where there was little supervision or support for staff conducting these examinations or management of the equipment – the situation was described to us as "the wild west".

We found that kiosks often operated outside the management structure of DFUs. In fact, we found that they weren't under any recognisable management structure in most cases. Their use can assist and direct investigations, and reduce demand within DFUs, but only if managed correctly. Many forces couldn't tell us how many trained staff were active, what their workloads were, or the number of devices awaiting examination. During focus groups we heard examples of staff going directly to their DFU, unless they knew someone who was trained and available.

Forces need to gain a better understanding of their kiosk demand. Some of the forces we visited were taking central control of their kiosks, allowing them to better understand all digital forensic demand. We believe better control and central co-ordination of kiosks and other functions associated with digital forensic examination is required. In most forces there are no departments better placed to take on this co-ordination function than the force forensic science units.

Recommendation 4

By September 2023, the National Police Chiefs' Council and all forces within England and Wales need to include the management of digital forensic kiosks in their governance and oversight frameworks.

Level 2 examinations: digital forensic units

We have already explained how DFUs have developed, often from small standalone teams into large units with highly trained staff and expensive equipment that are capable of high-quality device examinations. However, some of these units are overstretched from the volume of requests for this type of examination.

Level 2 examinations are more complex, requiring specialist techniques, equipment and trained staff. These examinations are generally conducted in force DFUs – all forces we visited had their own DFU submission processes.

Level 2 examinations can encompass a range of crimes, including volume crimes. And in some cases, low-level crime, where the only evidence available is from digital sources, for example neighbour disputes and online harassment.

Level 3 examinations: digital forensic units or forensic service providers

Level 3 examinations are mainly reserved for the most serious or complex investigations, such as cyber-related crimes. This type of examination is frequently used for digital devices with some difficulty to the examination, such as broken or encrypted devices. These examinations are carried out by experts in DFUs, or via an external forensic service provider. These examinations, by their very nature, can be protracted and costly. While the volume at this level is lower, we found all forces had enough capacity to meet the demand for level 3 examinations.

Level 3 examination work may benefit from forces working together to provide staff and technology. Much of the equipment required is expensive and won't be in use all the time, so sharing access should be explored. We discuss improving collaboration in our chapter on future plans.

Triage processes

Every force we inspected had a system in place to prioritise examination of devices submitted to DFUs, and to expedite urgent cases. There were different processes in each force, but most took account of the severity of the crime and the immediate risks involved. We found little evidence of the victim being considered as part of these processes. In general, a risk assessment would also consider the threat, harm and risk posed by the suspect to the victim, any other members of society and themselves. This level of assessment is missing in most forces.

The systems we saw assigned a grade to each submission such as high, medium or low. Urgent matters involving immediate risk to life were correctly prioritised as high. However, we found limited evidence that this initial assessment was reviewed. If a review did take place, it was usually at the instigation of the officer in the case, rather than any formalised process for such a review being scheduled.

Getting this right is essential, as cases that are initially assessed as high may quickly become less important, and those prioritised as low can need more urgent attention, should the threat to a victim increase. This risk assessment process has been adopted in other demand queues such as call handling and traditional forensic submissions. We urge local and national leaders to adopt a similar approach in digital forensic queues and prioritisation.

All forces we inspected had a service level agreement (SLA) between the investigator and DFU, which provides a target date that a device would be examined by. Target times to start examinations are based on the grade allocated during the submission process. We found that these targets varied considerably between forces. In some cases, examinations of devices graded as low priority were started in days, yet elsewhere devices in similar cases weren't scheduled to begin for up to 18 months in line with the SLA. This means that some victims and witnesses suffer a poorer level of service depending on the force area they live in. This is little more than a postcode lottery for victims. One example provided was the submission of a suspect's device for voyeurism. It was submitted in February 2020 and the report wasn't returned until September 2021. This delay attracted criticism from the Crown Prosecution Service (CPS). In another example investigators spoke of a stalking case that was particularly sensitive. That case was still unresolved and the delay for extraction was more than 12 months. The investigator went on to say that the CPS was considering discontinuing the case.

Even when devices have been subjected to a prioritisation process, the actual content isn't known until they have been examined. Any undue or unreasonable delays have the potential to expose the public, victims and the force to unnecessary risks. For example, in one case, evidence relating to child abuse was recovered months after submission as it had been graded as low priority, in accordance with the SLA. In another example, a medium-priority case, there was an offence of indecency involving children and the suspect lived close to several schools. No examination had taken place, even five months after submission. This was despite the suspect being on bail and considered high risk.

Each force needs to make sure that there is sufficient oversight of the risk assessments carried out by DFU supervisors, at key stages of investigations. Such risk assessments should be recorded and take into account any risks to the victim or wider public.

Disclosure

During our fieldwork visits we heard examples and some frustration around perceived unrealistic demands made by prosecutors in the CPS. Investigators explained that sometimes the CPS requested too much information on a "just-in-case basis", causing multiple examinations and potentially unnecessary delays to investigations. Requesting too much information also added unnecessary demand on DFUs and case officers who had to review the extra material.

The Criminal Procedure and Investigations Act 1996 sets out how investigators must record, retain and reveal to the prosecutor material obtained during criminal investigations. This forms part of a process known as disclosure. The CPS describes the Act as having been drafted for an analogue age; the demands of digital evidence have created unforeseen challenges to investigators and prosecutors.

In recent years revised guidelines on disclosure have been released by the Attorney General to help investigators and prosecutors manage digital evidence. The Attorney General acknowledges that it was difficult to predict how important digital evidence would become in the investigation of crime in the past decade. The new guidelines outline which digital strategies should be included on the disclosure management documents, setting out details of sampling techniques, any key word searches and how resulting material was examined.

During this inspection we met national policy leads within the CPS. They explained the current position and how policies reflected the difficulties that exist in the management of digital evidence before and during court proceedings. We believe misunderstandings with prosecutors have at times contributed to problems. Investigators should be clear about the level of examinations used and any limitations, and phrases such as “full download” should be avoided by all parties.

The CPS told us that investigators and prosecutors should, when possible, have early contact and agree the approach to digital evidence. This should include discussion about all the devices seized, the level of examination so far undertaken, the material and evidence so far obtained, and any further examinations that are necessary. At all times investigators and prosecutors should act proportionately, taking account of the specific circumstances of each investigation. Any decisions to not examine devices should be explained to defence teams. We agree with the CPS’ view and would encourage all investigators to follow this advice.

Innovative practice: Working closely with the Crown Prosecution Service on digital requirements

We did find examples of positive practice in some forces we visited. The Essex Police child protection team has agreed with its Crown Prosecution Service (CPS) that advice will be obtained early in an investigation. This extends to discussions relating to digital parameters, ensuring proportionate examination of devices for suspects and victims. In the City of London Police, a digital forensic unit supervisor agrees a staged submission process with the CPS, based on the circumstances of each investigation. Since being introduced, demands from the CPS have reduced and the knowledge of officers has increased. This approach is like that used by many traditional forensic science units.

Difficulties with disclosure should be more identifiable once forces have established proper governance and oversight regimes. We think any specific concerns should be resolved locally through criminal justice boards, using current national policies and memorandums of understanding.

Impact on investigations and victims

Evidence generated by digital forensics can be persuasive and is routinely considered as a main line of enquiry by investigators and prosecutors. We have explained that demand isn't always understood and how this can lead to delays in the examination of devices, slowing down the criminal justice process. These delays adversely affect the quality of investigations and can directly affect victims, witnesses and suspects. Some victims of the most serious crimes are being let down.

In one force we were told that an officer was called to court on eight occasions to give evidence in bail hearings because of digital forensic delays. In some cases, magistrates refused to extend bail, resulting in high-risk offenders being released without any restrictions. Whenever this happens victims are failed and may be exposed to risk, making safeguarding more difficult. This is wholly unacceptable.

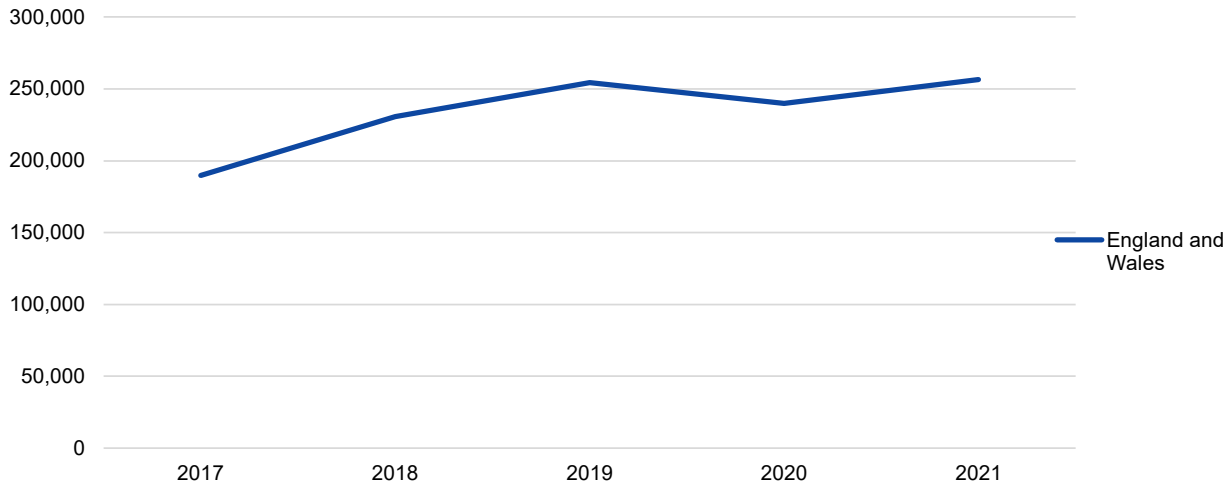
We found disparities in service across the forces we inspected, and we were told that the same disparities existed across much of England and Wales. The effect of the different ways police forces approach the management of digital forensic evidence effectively creates a postcode lottery for victims of crime. Our inspection revealed that if you live in certain parts of the country, the time taken to examine your device is likely to be a few days. In many other parts of the country this is likely to be months, if not over a year. This can't be right and shouldn't continue.

There are many reasons why victims and witnesses withdraw support for investigations. This may be illustrated by the increased use of outcome 16 over recent years. We were informed that delays caused by digital examinations were a contributory factor to victims losing faith in the criminal justice system and withdrawing their support for a prosecution.

These delays and backlogs in the police dealing with digital devices and evidence has been widely reported in the past few years. The problem isn't improving for victims and undermines public confidence. We were told by many investigators throughout this inspection that delays in digital forensic services undermined their investigations and affected the relationship with victims. And there were numerous examples of victims who, because of delays, disengaged with the criminal justice process altogether.

During the past five years there has been a marked increase in the number of cases where victims have disengaged from the criminal justice process (outcome 16). In the year ending 31 December 2017, 189,737 outcomes for victim-based crimes were filed as outcome 16 across forces in England and Wales, while in the year ending 31 December 2021, 256,689 victim-based crimes were assigned with this outcome. The graph below illustrates this increase.

Rolling 12 months incidents assigned an outcome 16 across England and Wales for victim-based crime from 1 January 2017 to 31 December 2021



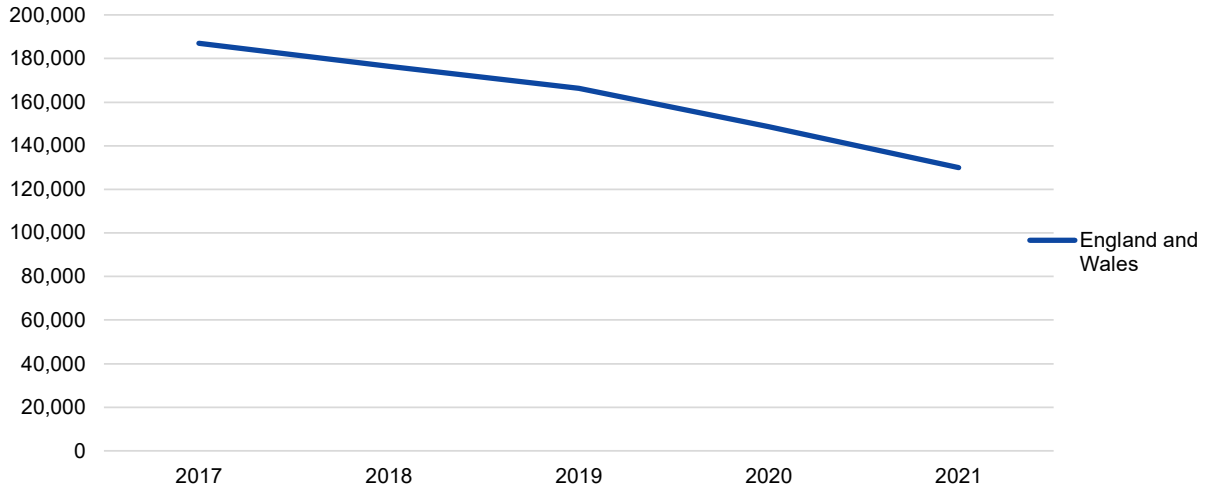
Source: Crime outcomes in England and Wales statistics, Home Office, 2022

The following graph shows a decrease in 'action taken' outcome codes, or positive actions, resulting from police investigations. 'Action taken' outcome codes include the following:

- (1) Charged/summonsed;
- (2) Caution – youth;
- (3) Caution – adult;
- (4) Taken into consideration;
- (6) Penalty Notices for Disorder;
- (7) Cannabis/Khat warning;
- (8) Community Resolution; and
- (20) Responsibility for further investigation transferred to another body.

We can't establish that digital forensics is the sole cause of these trends; however, our evidence suggests it may be a contributing factor.

Rolling 12 months incidents assigned an 'action taken' outcome across England and Wales for victim-based crime from 1 January 2017 to 31 December 2021



Source: Crime outcomes in England and Wales statistics, Home Office, 2022

Please note: Greater Manchester Police wasn't able to provide data from July 2019 to April 2020 and has therefore been removed from the charts above.

Serious sexual offences

In June 2021, Transforming Forensics introduced a £5m project to help forces in England and Wales respond better to rape and serious sexual offences. The project was part of a package of funding and support from the Home Office following the *End-to-End Rape Review Report on Findings and Actions*. Among its recommendations, the review stated that no victim should be left without a phone for more than 24 hours.

The project offered forces an uplift in technology in the following three ways:

1. Mobile digital forensic units, also referred to as 'digi-vans'.
2. Portable kits including digital forensic laptops and specialist software.
3. Kiosk upgrades to improve existing kiosk technology.

While each force plan to use this technology was different, the plans included an assessment of the crime scene and how digital forensics could support the investigation. Some forces are already examining opportunities to roll this service out to other vulnerable victims beyond rape and serious sexual offence cases. While there is still a way to go, we welcome these positive steps and encourage all forces to extend the use of this technology to vulnerable groups.

In recent years victims of sexual offences have raised concerns about the unnecessary examination of their devices during investigations. Most see this as a breach of their right to privacy, particularly when consent for this examination hadn't been given. As a result of these concerns, in September 2021, the Digital Processing Notice (DPN) was reintroduced across police forces in England and

Wales. This means permission has to be obtained to search any digital device belonging to a victim. This would help balance investigation requirements with the need to respect the privacy of victims and witnesses, while also meeting disclosure obligations. We found all forces had a policy and plan to download victims' devices within 24 hours in rape and serious sexual offence cases. At the time of our inspection, few forces were meeting this commitment.

Most forces have increased the use of DPNs to meet the requirements of the Police, Crime, Sentencing and Courts Act 2022. The process is new and not yet fully understood by investigators. To try and address this lack of awareness, most forces intend to integrate completion of DPNs as part of their victims' needs assessment and support. This should make sure that all victims provide consent when it is needed. We will assess the use of DPNs and digital forensic service to victims during future inspections. In fact, we encourage the National Police Chiefs' Council and local leaders to include data around this subject within the governance and oversight frameworks they developed.

Capability and capacity

This chapter covers:

- local capability;
- regional capability;
- external providers; and
- funding.

We have already explained that the understanding of digital demand, and the initial approach that should be taken at crime scenes, need to improve. Only then will it be possible for law enforcement to build enough capability and capacity to effectively secure digital evidence and provide the best service to victims of crime.

Digital forensic units (DFUs) operate in one of the fastest-changing areas of policing. There are constantly developing technologies that can both help policing and sometimes thwart its efforts to secure and preserve evidence. New forms of encryption sometimes used by those making and distributing abusive images of children are just one example of the barriers that sometimes need to be overcome to obtain evidence.

Local capability

During our visits we found evidence of significant investment in DFU capability; too often though this was unstructured and not part of integrated technology plans. While we found differences in capability between forces, all units had access to specialist equipment and extraction techniques. DFUs are undoubtedly providing an improving service, but we found examples of unacceptable delays and long turnaround times.

In general, we found most organisations didn't fully understand what skills and technology they needed to meet demand now or in the future. Some evidence extraction techniques require expensive equipment that may be beyond the reach of some forces. The difficulties of keeping up with new techniques and updating equipment increase the risk that some forces won't be able to keep pace with advances in technology. The Home Office had provided additional funding to some forces linked to investigations of rape and serious sexual offences. While this was welcome, the equipment purchased with this funding hasn't always been used effectively. We found some forces hadn't deployed this equipment, such as

digi-vans, due to a lack of trained staff. Also, we established that not all forces were considered, or were aware of, the funding opportunity. One force stated it didn't have enough rape and serious sexual offence cases to qualify for the funding. Yet it felt it could have used the equipment to improve service for victims elsewhere. Some forces felt the way funding opportunities were communicated was ad hoc. So not all forces were aware of what might have been available to them. We urge the Home Office to work with the National Police Chiefs' Council to make sure funding and resources are being directed to the right areas and communicated to all forces effectively.

We found that those forces with strong leadership in digital forensics showed good performance in managing the demand for examinations. Often this leadership was represented at a national level. Forces that performed less well lacked direct leadership involvement in digital forensic services which, in some cases, resulted in those forces not realising the opportunities available.

We did find evidence of forces trying to innovate to solve some of their problems. Some forces have developed a new way of viewing digital images through a virtual platform. This allows investigators faster and easier access to review the data extracted from devices. They no longer need to book slots to use the systems in the DFU, which previously caused delays and frustrated the investigation.

We found West Midlands Police had invested in two digital crime scene managers, who are part of the wider crime scene investigation department. This is a conscious decision to integrate digital forensic services within traditional forensic disciplines. The alignment of both forensic disciplines is a sensible next step in the evolution of digital forensic services. Most of the people we spoke to stated that this was a good idea.

Innovative practice: Automating the examination of devices for child exploitation investigations

Greater Manchester Police worked with experts from Transforming Forensics over a 12-month period to develop an automated process for the examination of devices related to child sexual exploitation. During the pilot the force halved the time it took to examine devices linked to child sexual exploitation, making the whole process more efficient. This provided clear evidence that it is possible to reduce backlogs and improve the wellbeing of staff, who no longer have to review some abusive images of children. This type of automation, which is also used by the National Crime Agency and a small number of police forces, could be extended to other forces.

The type of automation used by Greater Manchester Police could also be used in other high-volume cases such as fraud and cryptocurrency and cybercrime. But extending the use of automation in the investigation of crime would require national co-ordination, support and funding. If wider use of automation was achieved and accredited, this would make digital forensics in these high-volume areas more efficient.

Regional capability

Disappointingly, we found limited evidence of collaboration between forces or across regions. Most forces were reacting to demand and managing their own response. We also found differences in digital forensic capabilities within and between regions. Most forces are likely to need access to expensive specialist techniques from time to time. But for some forces it would be difficult to justify investment in such equipment and software, including licences, when they have few cases that would require it. We believe there is scope for collaboration within regions that would ensure more efficient and effective access to, and use of, skills and technologies.

Regional organised crime units (ROCUs) focus their efforts predominantly on those involved in organised crime. While their investigations tend to rely heavily on digital evidence, they don't manage the same volume of cases as forces. We found that ROCUs appeared to have a better understanding of their demand. But generally, this was due to the lower volume of cases rather than improved processes.

In the ROCUs we visited we found differences in approach. One unit was able to manage its own examinations. But the others had no digital forensic capability of their own. This meant that investigators had to rely on support from one of their constituent forces. We found that often they went to the force that had the shortest queues, or where they had personal contacts.

Generally, we found that forces hadn't taken account of the demand for ROCU examinations. As ROCU submissions are often complex, involving serious crime, they are frequently processed as a priority. This then affects other lower-priority submissions already waiting to be examined in force DFUs. This isn't only inefficient, but it can also have a negative effect on the queues in that force and on victims of crime.

We were told of an example of a mobile phone being sent to one force for examination while other types of devices, from the same case, were sent elsewhere as the turnaround time was shorter. Neither ROCUs nor forces appeared to understand the effect this additional demand was having locally.

Better understanding and co-ordination of digital forensic services is needed in each force and ROCU. This improved understanding of demand would allow each region to consider how best to build a capability for digital forensic services, with sufficient technology and trained and accredited staff to meet future needs.

External providers

There are several private digital laboratories that provide extra capacity to law enforcement. Most forces had used, or had contingency plans to make use of, these external providers. Often this was to manage spikes in demand or to reduce examination backlogs. We found an inconsistent approach to the use of external forensic providers.

Some forces were reluctant to use these services, while others used them regularly as part of their overall approach to dealing with the demand. One force routinely allocates about a third of its examinations to private laboratories. The National Crime Agency uses them for all its examinations because it believes this is more efficient than building its own capability.

Some forces undertook all examinations internally, explaining that costs of up to £2,500 per phone examination were unaffordable. Others said retaining ownership of examinations made sure that they could control the quality of the evidence produced. We were surprised to find such a lack of confidence in these accredited laboratories among some forces, not least since all forces rely on similarly accredited private providers for other forensics services such as DNA analysis. The external laboratory we visited during our inspection undertook digital forensic and more traditional forensic examinations. Consequently, examinations outsourced to private providers are often sporadic and individual forces are unlikely to get the best prices when using them less frequently, simply to ease their demand in some cases. In one force investigators stated that when the force outsourced digital forensic demand, it received a much better service compared to internal force submissions, both in terms of quality and timeliness of results.

We visited a private provider that had significant capability and was able to carry out all levels of examination. It was also able to attend crime scenes and provide expert advice and testimony, when required. It has longstanding arrangements with some law enforcement agencies that regularly submit work to it, while others only use the private provider in times of crisis. This latter approach is problematic for the providers as they are required to flex to a sudden increase in demand. This demand then generally disappears once the force has moved past crisis point. For obvious reasons, private suppliers prefer a consistent pipeline of work as this allows them to make the most efficient use of their resources and provide the most cost-effective service.

The private sector prioritises making profit, but it also has an important role in helping to shape how digital forensic science can be provided to police forces. There is concern that as forces try to manage demand internally, using external service providers less frequently, private service providers may move from these volatile markets, leaving policing to struggle on its own.

Individual forces currently decide how they use private providers at the same time as minimising the potential risks of becoming too reliant on external suppliers. But it may be time for a national approach to making sure the police service has access to high-quality, cost-effective digital examinations, to protect the long-term interests of policing and improve the service to victims of crime. Such an approach would need the Home Office, National Police Chiefs' Council lead and private service providers to work together.

Regardless, we encourage the involvement of private service providers in national and regional forums, designed to improve the response and technological advances. As with standard forensics it may be more efficient to develop a sustainable hybrid approach over the medium to long term.

Funding

Many in policing don't understand digital forensics. They don't prioritise it and there is insufficient investment to improve the examination of digital devices. This is undermining the criminal justice process. More funding is required if the service is to improve. The Home Office has a part to play.

In recent years additional funding has been available to policing from several sources including the Home Office. This has supported programmes including the response to rape and other sexual offences, and solutions that allow for automatic examination of indecent images. But we found that accessing this funding was difficult and forces weren't always aware of what was available. We were told of examples of funding opportunities, which some forces simply didn't apply for.

We acknowledge that the cost of digital forensic examinations is high – as are particular items of equipment, licences and the environment needed for their use. We found that funding for digital forensics wasn't always linked to force strategies or plans. Often business cases were submitted by DFU managers on an ad hoc needs basis or when extra funding was available. We found little evidence of mid-term or long-term funding plans for digital forensic services. By their own admission, force finance officers and IT managers had little or no knowledge of this area or the link between digital forensics and the quality of investigations. This was distinctly different from their understanding of traditional forensics.

We heard examples of other departments, independent of DFUs, securing force funding to purchase specialist digital examination equipment. This leads to examinations being conducted outside expert control and without accreditation. It also lacks any efficient or effective approach to the coordination of digital forensic examinations.

Recommendation 5

By April 2023, the Home Office should review digital forensic budgets and funding. Future additional funding should support the national digital forensic strategy and be well communicated and easier to access.

Accreditation and training

This chapter covers:

- digital forensic regulator;
- accreditation;
- College of Policing;
- force training;
- recruitment and retention; and
- wellbeing.

Forensic Science Regulator

The Forensic Science Regulator (FSR), originally established in 2007, was given statutory powers as part of the Forensic Science Regulator Act 2021. Under the Act, the regulator must prepare and publish a code of practice to cover forensic science activities in England and Wales.

In August 2022, the regulator published a draft version of the code of practice for consultation. This is largely based on the current non-statutory *Codes of practice and conduct* that has been in place for the last ten years. Digital forensic techniques need to comply with the code of practice and requirements for accreditation to the International Organization for Standardization (ISO, an independent, international, non-governmental organisation that brings together experts to share knowledge and develop voluntary, consensus-based, market-relevant standards that support innovation and provide solutions to global challenges). This compliance isn't new. The FSR set a requirement for digital forensic techniques to be accredited by 2017. While compliance was patchy, many forces and commercial units have now complied with specific requirements. The new codes, however, will bring bigger challenges. Traditional forensic techniques have been accredited in a similar way for many years.

The Forensic Science Regulator Act 2021 allows the regulator to issue compliance notices if it believes a person is carrying on with a forensic science activity to which the code applies, and this creates a substantial risk of adversely affecting any investigation or prejudicing the course of justice. The code is admissible in evidence in criminal and civil proceedings in England and Wales, and courts may consider failures to act in accordance with it, potentially deeming evidence inadmissible.

The Crown Prosecution Service previously clarified that it wouldn't prosecute cases based on fingerprint evidence from unaccredited forensic units. This led to a rush to achieve accreditation. However, at that time there weren't enough resources available to manage the increased demand. Policing should make sure the services it uses and provides comply with the codes of practice and are accredited. This will show competence and transparency in digital forensics. It will also make sure similar mistakes aren't repeated, while providing reassurance to both courts and the public.

Accreditation

The United Kingdom Accreditation Service (UKAS) is the sole national accreditation body for the United Kingdom. It is appointed by the Government to assess against nationally and internationally agreed standards. It is independent of the Government and is self-financing.

Anyone providing a digital forensic science service must comply with the Forensic Science Regulator's codes of practice and conduct, and, where required within the codes, must be accredited to ISO standards. This includes all digital forensic services conducted in digital forensic units (DFUs) or kiosks, or at scenes.

UKAS has provided accreditation assessments in forensic fields for over 25 years. Many established forensic services such as drugs, accelerants, toxicology, fingerprints, DNA, and scenes of crime examinations also require accreditation. Accreditation provides an independent confirmation of competence to perform a defined set of activities.

Any organisation can apply to UKAS to become accredited. Once accredited, organisations are visited by UKAS at least once a year to review their current systems; the visit may be unannounced. Most organisations have a quality manager who works with UKAS to ensure compliance with current standards.

Those we spoke to during this inspection accepted that accreditation was essential to demonstrate competence and accountability. However, representatives from law enforcement and the private sector explained that accreditation processes could be bureaucratic and costly. Attempting to blame UKAS for being unable to manage surges in demand immediately before accreditation deadlines is unfair. In addition, we were told of occasions when UKAS has been asked to undertake assessments when organisations were clearly not ready. This not only wasted the time of technical assessors, but also incurred unnecessary costs.

We heard examples of an accreditation process needing to be completed again simply because a department moved a short distance between offices. The move involved no change to technology or processes, yet we were told the cost was £15,000.

The National Crime Agency is exploring the option of having its accreditation conducted by an international provider rather than UKAS. It believes there are several benefits, including laboratory processes being accredited rather than each individual site. This would reduce the costs and time required to achieve accreditation. As ISO standards are the same worldwide, accreditation can be obtained internationally. Any changes to accreditation processes would need prior approval by the FSR.

We would encourage the FSR and the Home Office, together with other interested parties, to review the existing method of accreditation and compare it to other international services, to satisfy themselves that it is both effective and efficient.

College of Policing

The College of Policing (COP) was established in 2012 as the professional body for everyone who works for the police service in England and Wales. It is an independent arm's-length body of the Home Office.

The COP offers a range of digital forensic and digital investigation training products. These are relevant to the three levels of digital forensic examinations described earlier. The COP has badged its digital investigation modules as 'Operation Modify'. However, it was found that there had been slow uptake by frontline officers in England and Wales.

We still found examples of staff who felt they had insufficient knowledge and information to manage digital investigations or develop forensic strategies. This highlights the need to continually develop and enhance available training, and extend its reach throughout law enforcement. We would encourage leaders within forces to allocate enough time for frontline staff to complete these COP training modules.

Crime investigators currently receive minimal training to manage the digital forensic aspect of their investigations, and many still have limited access to digital media investigators (DMIs). They need more training to develop their skills and knowledge in this area. This would help them to make more effective decisions and build better investigation plans.

We have already explained why the recruitment, deployment and education of DMIs should expand to provide the support investigators need. The COP has developed a programme to train and develop DMIs.

While the quality of initial training for DFU staff is high, we heard that ongoing professional development locally was often ad hoc and unstructured. This was frequently attributed to capacity issues and a lack of development opportunities. The continuous professional development of people involved in the digital forensic examination may benefit from regional or national co-ordination.

Some investigators stated that DFU staff lacked knowledge and experience in the management of investigations and how to meet victims' needs. This often led to a flawed decision-making process on what investigations to prioritise, causing frustration among investigators. We strongly urge the COP to review its digital courses to make sure that sufficient investigative input from the professionalising investigation programme accreditation courses is included, to bridge this gap.

Recommendation 6

By April 2023, the College of Policing should make sure all its digital courses have sufficient focus on investigations and victims' needs.

Force training

We found that quality training was available at both entry level into policing, and in complex investigation roles. However, there were a significant number of officers and staff in non-investigation roles who hadn't received any training in digital forensics. This group of officers and staff needs upskilling, both now and as part of a structured refresher/continuous professional development programme. We recognise that this won't be easy and will inevitably be reliant on e-learning.

Digital forensics is a specialist role within policing. Most of the training available is provided either locally or nationally. But we found little evidence of the service using outside providers to add value to the training offered to staff. This is an avenue that needs exploring nationally and locally. It is essential that the police service uses the skills, technology and knowledge that private business can bring, both now and in the future.

Recruitment and retention

Recruitment and retention of specialist staff is a persistent problem within policing and wider law enforcement. This is often due, in part, to the disparity in salaries between the private and public sector. One staff member said to us: "I did not come into public service to be rich; however, I feel my wages and career progression could be better." Following our inspection, we agree.

Initial recruitment of inexperienced but trained staff, often from universities, is less problematic. However, policing should accept that it will likely lose staff and skills to private business, where there are better wages, conditions and wellbeing on offer. Lack of professional development and career progression were cited as reasons to be tempted by private industry, as well as better pay.

Some forces have tried to address this, but inevitably it has created inconsistencies between forces. The same roles receive different levels of pay in different forces, and unwanted competition has developed as law enforcement agencies offer different

incentives to attract skilled staff. This issue isn't exclusive to digital forensics, and similar issues exist in the fields of cyber investigation and fraud.

There is a need to develop career pathways within policing to allow development, promotion and renumeration beyond what is currently offered. This will allow forces to properly succession plan and minimise the impact of inevitable staff losses.

Wellbeing

Staff working in digital forensics often spend time examining very unpleasant images, which may include reviewing large amounts of child sexual exploitation images. This can have a significant and cumulative effect on some officers and staff. We were pleased to find that all the organisations we visited prioritised staff wellbeing. This included direct referrals to occupational health units on a six-month or yearly basis for all. The effect of this work on officers and staff was also recognised by leaders at many levels.

Staff reported to us supportive supervisors, who understood welfare needs and signposted them for support when appropriate. Most stated that the fact their supervisor worked in the same environment was important, as the supervisor understood the pressures. There were good examples of breakout rooms or safe spaces where staff could take breaks. These rooms had referral notices and contact details for support networks.

Future plans

This chapter covers:

- storage and retention;
- new technology;
- collaboration; and
- evolution of digital forensics.

Future planning by forces to keep pace with new technology, regularly updated software on mobile devices, artificial intelligence products, and extraction techniques will be difficult. This is especially the case if each force tries to respond on its own. The costs alone may make some innovations unaffordable for some forces. Training, building resilience and creating space for continuous professional development will add to the costs and difficulties even for larger forces.

During our inspection we found few forces with a good understanding of current demand, and none had a clearly developed picture or assessment of what their future demand may look like. In fact, generally we found that any planning to deal with demand lacked proper co-ordination and structure. Where investment was being made it was too often ad hoc and unlikely to deal with immediate challenges, let alone the future.

Storage and retention

Storing the evidence from digital forensic examinations is a big problem for the police service and it is getting worse. The old ways of storing evidence don't work in this digital age. Policing must move to a cloud-based system of storing digital evidence if it is to become more efficient and effective.

Currently most forces use hard drives and servers, located within their estate, to store most digital forensic data. The service has seen an exponential increase in the volume of data that now needs to be held for long periods, as part of lengthy investigations. Many of the forces we inspected were already struggling to store and retain this data.

The problems forces face include the cost of storage, the physical space needed and the requirement to back up the data in a secure way. Everyone we spoke to involved in digital forensic provision stated that the future of storage and digital forensic units examinations will ultimately be cloud-based. During our inspection we found evidence of significant investment in the storage required to retain digital material. This was often in the form of expensive servers and hard drives, which are difficult to search or manage data on. Some forces have considered using the cloud as an alternative. Cloud computing is the on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user. But only one force was using this alternative solution.

The Code of Practice on the management of police information introduced guidance relating to retention, review and disposal of any information held by police. Digital information is covered by these rules and the use of hard storage makes it difficult for forces to comply with these rules. This is mainly due to the information being difficult to locate and isolate on hard-drive storage, resulting in many forces being unable to dispose of material at the right time.

We found that the City of London Police is developing a cloud-based storage solution with an external supplier. Management of police information retention and deletion notices are to be attached to crime systems, making management and deletion easier. Essex Police is also planning to move to cloud-based storage, in collaboration with Kent Police; this approach is to help secure future storage capacity.

Despite the difficulties with traditional storage of large volumes of data, some forces are reluctant to move to cloud-based storage and examination. We heard of concerns about security and legal requirements, and a reluctance to lose control of the system. Forces would benefit from guidance on the legitimacy and security of cloud-based storage and examination solutions, with financial incentives to encourage forces to collaborate in securing these. We believe effective and efficient use of this new technology will only be achieved through leadership provided by the National Police Chiefs' Council lead for digital forensics, working with the Home Office. Otherwise, the service is likely to adopt past practices of individual forces developing solutions that are expensive and short term, and lack any interoperability.

Recommendation 7

By June 2023, the National Police Chiefs' Council lead for digital forensics, the Home Office and relevant support services should provide guidance to all forces on the use of cloud-based storage and computing power.

Effect of new technology

Businesses develop technologies to sell commercially. Law enforcement then finds itself reacting to the way criminals exploit these technologies. The development of online fraud and phishing (sending fraudulent emails to get someone to reveal personal details such as passwords and credit card numbers) highlights this and the devastating effect on victims. Policing needs to adapt to these challenges and work with private businesses to develop capabilities to not only frustrate the criminals, but also turn the technology to their advantage.

The Forensic Capability Network (FCN) was initially designed to be the co-ordinator of this activity and we did find some examples of success. However, we frequently heard that they had struggled to keep up with the challenges and offered forces limited support in developing technologies.

Police forces can't meet the technological challenges alone. It will be expensive and often beyond their understanding and capabilities. There needs to be a co-ordinated effort to work together with private businesses and forensic providers to develop and share skills. This was found in the Metropolitan Police's approach to digital forensics. Within its structure, it sends on average a third of its submissions to private suppliers. This is mainly done to generate a relationship and encourage businesses to develop greater expertise to meet future technological challenges.

These relationships need to be developed nationally, regionally and locally, and in a structured way. They need to be co-ordinated and harnessed at national level to make sure these skills and technologies are used to enhance services to victims wherever they live in the United Kingdom.

Collaboration

We found few examples of forces collaborating with each other to meet the challenges of digital forensics. To keep pace with technological changes, policing needs to work smarter. Collaboration may provide policing with opportunities to standardise approaches, share the costs of investment, build resilience and make financial savings.

Collaboration with external businesses was mainly being developed and managed locally, often in isolation: this is unlikely to achieve best value. We heard examples of decisions being taken to select the cheapest option rather than the most effective solution.

Policing has suffered for many years because forces have adopted different IT systems, limiting interoperability and making it harder to share information. Efforts should be made to avoid repeating these mistakes. This will require leadership and a commitment to work together. Engaging with businesses around procurement

and new technology is likely to bring cost benefits. The National Police Chiefs' Council should be central to these developments.

Each police and crime commissioner and chief constable is responsible for their plans and budgets. However, policing operates in an environment where the cost of new technology is high. The accreditation of services across 43 forces and other agencies is proving near-impossible. Capacity and capability in some forces is causing unacceptable delays in investigations. We believe there are several opportunities for digital forensics to be improved through collaboration. These include:

- shared provision of training and continuous professional development;
- procurement and sharing of technologies, including software and licences;
- joint accreditation of staff, processes and facilities, especially in level 2 and 3 examinations;
- shared estate facilities and data storage facilities; and
- development of new technologies with private industry.

We encourage police leaders to adopt a whole-system approach to meeting the complex challenges that are presented by the digital age.

The evolution of digital forensics

The police service has had to adapt to new technology in the past, with DNA being a prime example. But it isn't learning from the past or adapting quickly enough to meet the demands of this digital revolution.

We think that the natural evolution for digital forensic services should be to move them under the leadership and control of other traditional forensic disciplines. All forces have a mature and professional forensic capability that makes sure evidence is gathered correctly and presented effectively at court. This doesn't happen currently with all digital forensic examinations. It is difficult to understand why not, given the difficulties faced by most forces in meeting demand.

Throughout this report we have provided evidence of an unstructured, inconsistent and often leaderless approach to meeting the requirements of digital forensic services. And we have highlighted the effect this has had on victims and witnesses. In most of the forces we visited we were left unclear as to who had overall responsibility for digital forensic services. This is generally not the case with other more traditional forensic disciplines.

From this inspection we can find no better blueprint for the evolution of digital forensic services than that provided by existing traditional forensic services. In the early days of DNA, its credibility, collection, storage and presentation at court was often subject to significant legal challenge. In some cases with good reason. We can avoid the mistakes of the past by making sure we use the existing professionalism and maturity of these departments and leaders in how we manage digital forensic services.

If the police service is to become more efficient and effective in how it manages digital forensic services, things must change. The integration of digital forensic services with traditional forensic disciplines won't be easy and will inevitably take some time. We believe that bringing all forensic disciplines under one structure, with national standards and co-ordination, will achieve the improvements that are necessary.

To achieve all the improvements this report recommends, we believe that there needs to be clear leadership and direction. And national leaders from all organisations must work closely with the private sector to develop a new operating model for digital forensics.

To do this, there needs to be a better understanding of what digital tools policing currently has, and what it needs in the future. Key to this understanding is the development of a wider analytical landscape. Only then will it be clear what skills and technologies are needed to provide effective and efficient digital forensic services to the public.

Recommendation 8

By November 2024, chief constables should integrate digital forensic services under their existing forensic science structure.

Recommendation 9

By November 2024, the Home Office should work with the National Police Chiefs' Council, the College of Policing and the private sector to design an alternative operating model that would provide effective and sustainable digital forensic services to support police investigations.

Conclusion

The police have found it difficult to keep up with the pace of rapid advances in digital and social media. In many cases the approach taken in digital forensics has been to react to technology in ways that are too slow, piecemeal and unstructured.

The service is now at a crossroads as to how it will adapt to the challenge digital forensics presents. And how it will make sure it capitalises on the evidence that is available through the effective and efficient examination of digital devices.

It would be a mistake to continue investing more resources in an unco-ordinated way, hoping this will solve the demands of the future. In this report we have suggested a path that police forces, and the wider service (including all other law enforcement organisations such as the National Crime Agency and His Majesty's Revenue & Customs) should follow, if it is to keep pace.

Too often digital forensics has been sidelined. Some police officers simply don't understand the potential of digital forensics in investigations. Nor do they understand what systems and processes are required to get the most from effective examination of digital devices. In many forces a few specialists are trying to manage an overburdened system. In some cases, this is happening with poor leadership, a lack of training and accreditation, and insufficient grip and oversight.

If things don't change, victims will continue to be let down by a system that is struggling to cope with the sheer scale of digital devices that need examination. This will continue to frustrate the criminal justice process and result in offenders not being brought to justice.

The cost of technology, developing skills and finding digital solutions can't be for policing to address alone. Yet we found little evidence of any meaningful collaboration between police, the private sector and the Government to improve areas where they could have a positive impact through co-operation – for example, procurement, training, or service provision.

At present, 43 police forces are working in relative isolation, trying to achieve accreditation in some form of digital forensic examination. This isn't only bureaucratic, but also nearly impossible to achieve and maintain. This needs to change quickly, and collaboration with the private sector must improve to meet the challenges the future will undoubtedly bring.

We have made nine recommendations to improve services in this area.

Annex A – Methodology

Our inspection was carried out in four parts.

Inspection framework

We conducted interviews with a wide range of interested parties and subject matter experts to determine the main themes and areas of concern. These were then included within the inspection framework.

Document review

We reviewed documents provided by the National Police Chiefs' Council, Forensic Science Regulator, United Kingdom Accreditation Service, Crown Prosecution Service, and police forces. These included national strategy documents, finance and resourcing plans, force management statements, training levels and minutes of meetings.

Field inspection visits

The field inspection took place between February and June 2022. We visited:

Forces

- Northumbria Police
- Derbyshire Constabulary
- Lincolnshire Police
- South Yorkshire Police
- West Midlands Police
- Avon and Somerset Police
- Gwent Police
- Essex Police

Regional organised crime units (ROCUs)

- North East Regional Special Operations Unit (NERSOU)
- East Midlands Special Operations Unit (EMSOU)
- South West ROCU
- Tarian ROCU (South Wales)

Other organisations we visited

- His Majesty's Revenue & Customs (HMRC)
- British Transport Police (BTP)
- National Crime Agency (NCA)
- Crown Prosecution Service (CPS)
- One private forensic provider
- Forensic Science Regulator (FSR)
- United Kingdom Accreditation Service (UKAS)
- Bedfordshire Police
- City of London Police (national lead for fraud and cybercrime)
- Greater Manchester Police

Interviews and focus groups

In each force/region we interviewed:

- ACC lead for digital forensics
- Head of finance
- Head of IT
- Head of HR
- Head of digital forensic unit (DFU) / head of forensics
- Lead for International Organization for Standardization (ISO) accreditation
- Technical manager for accreditation
- Head of investigations or protecting vulnerable people (PVP)
- Head of training
- Focus groups with investigators and frontline staff
- Offered to meet with police and crime commissioner (PCC)

Reality test

We visited DFUs and met staff. We did the same at the private forensic provider.

www.justiceinspectorates.gov.uk/hmicfrs