Digital Forensics within the Criminal Justice System: Use, Effectiveness, and Impact

Arising from the Northumbria University Digital Forensics Project

Dr Cerian Griffiths

Emma Piasecki

Dr Sophie Carr

Philip Anderson

Professor Tim J Wilson

February 2024

Table of Contents

Foreword

This report provides innovative insight into the use, effectiveness and impact of digital forensics across the entirety of the criminal justice system.

The data from the Northumbria University Digital Forensics Project identifies:

- the application and impact of digital forensics
- challenges and inefficiencies
- areas in which the allocation of greater resources would affect the greatest increase in impact
- barriers and risks in current practice that undermine the overall aims of the criminal justice system

This project also serves as a pathfinder for subsequent and more resource intensive qualitative and quantitative studies.

This report makes recommendations about future policy reviews and strategic investment for delivering the large-scale transformation required for more effective and impactful use of digital forensics to the benefit of the entire criminal justice system.

Executive Summary

Findings Overview

All findings are based solely upon the data obtained from research participants during the Northumbria University Digital Forensics Project.

1. Digital Forensics Literacy
   Across the criminal justice system, there is a general, and fundamental lack of knowledge and understanding by those not intimately involved in digital forensic practice. This lack of digital forensics literacy ultimately contributes to:
   - the backlog of devices waiting for examination,
   - a misunderstanding of data and analysis during investigations and through to trial,
   - an inability to properly assess reliability and admissibility of digital evidence,
   - poor evidence communication,
   - discontinued prosecutions and the very real risk of miscarriages of justice.

2. Technical and Practical Challenges
   - There is insufficient resource to address the volume of digital forensic material.
   - This lack of appropriate resource, combined with ever-increasing volume, has repercussions across essential processes such as the communication, transfer and presentation of digital forensic data and evidence, disclosure, and other regulatory requirements.
   - Digital forensic activity is not undertaken in a timely or efficient manner, there is a risk that the full needs of the investigation may not be met and that the data or evidence is misunderstood by those expected and required to understand and make appropriate use of it.
   - There is an insufficient number and distribution of appropriately trained digital forensic practitioners within Police Digital Forensic Units and independent private providers - to undertake the necessary extraction, analysis and interpretations required for the effective and reliable use of digital forensic evidence.
   - There is an insufficient number and distribution of Digital Media Investigators, key to assisting police investigators in developing an appropriate, proportionate and successful digital forensics strategy.

3. Digital Evidence and Admissibility
   - Current practice involves limited attention paid to whether digital forensic evidence will ultimately be admissible.
   - There is an absence of attention paid to the crucial question of whether different forms of digital forensic evidence is factual or opinion, the underpinning reliability of the evidence and its limitations.
   - To properly determine relevance, admissibility and weight of digital forensic evidence, and ensure fairness in criminal proceedings, digital forensic evidence must be better communicated to, and understood by, those involved in the prosecution, defence, and adjudication of cases.
   - The rules of disclosure must be properly applied.

- Professionals in every discipline across the criminal justice system shared these concerns alongside the inadequacy of time for proper disclosure processes to be respected, for lawyers to properly consider digital forensic evidence and the inequality of arms between prosecution and defence hindering the defence's ability to adequately examine, analyse and effectively challenge digital forensic evidence relied upon by the state.

4. The Home Office Forensic Impact Points Model
    - Digital forensic activity is most impactful when applied as early as possible in an investigation.
    - Two points of impact are currently missed by the Model: Disclosure and Appeal.
    - There is an underrepresentation of the issues and complexities affecting defence lawyers and experts instructed by them.
    - The drive to better understand, identify and measure the impact of digital forensics is welcome, particularly if this leads to better resource allocation and improvement in digital forensics expertise.
    - Applying relevant metrics should be done with care, avoiding an emphasis on the final outcome of a prosecution.
    - There is a genuine desire and enthusiasm across the criminal justice system for further collaborative, multi-disciplinary research, with academic involvement, to address this complex issue.

Background and Central Findings

The House of Lords Science and Technology Select Committee identified that "Digital evidence is now a key component in many criminal trials…[estimating that]… "90% of crime … has a digital element, in the broadest sense…"[1] The breadth and speed of the development of digital forensics has outpaced the national infrastructure necessary to utilise the capability and capacity of digital forensics fully and efficiently to both prevent crime and detect and investigate suspected criminal activity.

Much of the focus of reviews and research to date has centred on the logistical application of digital forensics, particularly resources within policing. The less documented voices are those seated in the courts, the end users of the digital forensics process, receiving the associated outputs and reports. The Northumbria University Digital Forensic Project has specifically sought to include these key voices and their experiences. This report, therefore, provides a thorough insight into how digital forensics is instructed, undertaken, utilised, and conveyed between those taking an active role in policing, digital forensics and law, including both prosecution and defence representatives.

To better understand how digital forensics is deployed across the criminal justice system, it was necessary to explore:

- how and where it provided impact and
- whether it was used in the most effective manner

[1] House of Lords, Forensic science and the criminal justice system: a blueprint for change, HL Paper 333. Here is the link: https://publications.parliament.uk/pa/ld201719/ldselect/ldsctech/333/333.pdf

The Home Office's Forensic Impact Point Model[2] provided a framework to instigate discussion with representatives from across all[3] relevant professions within the criminal justice system. The outputs from these discussions were analysed to identify not only whether impact was taking place, at the anticipated points, but also to consider whether full value was achieved and what changes could elicit a more effective and efficient delivery towards maximum benefits.

The project team comprised academics with well established professional backgrounds across forensic science, computer science and criminal law, complemented by contributions from those with significant experience of Crown Prosecution Service and Home Office policy and practice.

The key findings from this work present the challenges and provide decision makers with constructive, evidence based recommendations to assist in increasing the impact of digital forensics and informing future resource and policy decisions in the short, medium, and long term.

Methods and Analysis

Northumbria University Digital Forensics Project represents the broadest and most holistic view of the use, effectiveness and impact of digital forensics across the criminal justice system to date. It garners the experiences of professional stakeholders in all disciplines, in all crime types who interact with digital forensics on a daily basis across the life of a criminal case, from initial intelligence gathering to, where occurring, criminal appeal.

The professional stakeholders - twenty six in total - included police officers from four police forces, the National Crime Agency and those involved in counter terrorism, police Digital Forensics Unit investigators, HM Prison and Probation Service, independent digital forensics practitioners, the Crown Prosecution Service, and solicitors and barristers in independent practice with experience of both prosecuting and defending.

The project undertook pre-focus group interviews, online focus groups with mixed groups of professional backgrounds represented, a follow-up survey and a follow up interview. This gathered first-hand experiences of those using digital forensics and direct discussion between users and stakeholders who are often siloed within the criminal justice system.

The resulting data gave findings under four themes:

1. Digital Forensics Literacy
2. Technical and Practical Challenges
3. Digital Evidence and Admissibility
4. The Home Office Forensic Impact Points Model

[2] The Impact of Forensic Science Project: Phase 1 Report, Marie Barrett, 2nd Aug 2022. The Phase 2 Output is within the report and also in Appendix 1.
https://assets.publishing.service.gov.uk/media/62e7dd71d3bf7f75bd257e12/Home_Office_Impact_of_Forensic_Science_Project_Phase_1_Report_for_publication_Accessible_Version.pdf

[3] With the exception of the judiciary who it was felt would be less able to speak candidly about their experiences, and for whom the process of obtaining ethical approval and approval by the Master of the Rolls was deemed unachievable within the timeframes of this project.

Main Findings

Theme 1 – Digital Forensics Literacy

The absence of digital forensics literacy is a barrier which undermines the use, effectiveness, and impact of digital forensics across the criminal justice system. The impact of this barrier is experienced by professionals across the investigative and legal process. Several areas of concern were highlighted and evidenced, grouped into two areas:

- Understanding what potential digital evidence can be obtained from a device or system together with an appreciation of the complexity of the data extraction task and the relevance of the ensuing findings.
- The need for simplified and understandable data and reports, where the results and terminology are explained and communicated with clarity and transparency suitable for a lay person.

Underlying both areas of concern is a general, and fundamental, lack of knowledge and understanding by those not intimately involved in digital forensic analyses. This lack of digital forensics literacy emerged as a significant factor, ultimately contributing to the backlog of devices waiting for examination, misunderstandings of data and analysis, inability to properly assess reliability and admissibility, poor communication of evidence, discontinued prosecutions and the very real risk of miscarriages of justice.

Theme 2- Technical and Practical Challenges

There is insufficient resource to deal with the volume of digital forensics. Volume is generated by the extent of work involved in a single investigation compounded by the number of cases that involve an element of digital forensics. Insufficient resource is evidenced by the insufficient number and distribution of appropriately trained digital forensic practitioners across the criminal justice system - within Police Digital Forensic Units and independent private providers - to undertake the necessary extraction, analysis and interpretations required for the effective and reliable use of digital forensics evidence. In parallel, there is an insufficient number and distribution of Digital Media Investigators, key to assisting police investigators in developing an appropriate, proportionate and successful digital forensics strategy.

Consequences of this insufficiency are that digital forensic activity is not undertaken in a timely or efficient manner, there is a risk that the full needs of the investigation are not met and that the evidence is misunderstood by those expected and required to understand and make appropriate use of it. This lack of appropriate resource, combined with an ever-increasing volume, has repercussions across other very necessary processes and actions such as the communication, transfer and presentation of digital forensic data and evidence, disclosure, and other regulatory requirements.

Theme 3 – Digital Evidence and Admissibility

To properly determine relevance, admissibility and weight, and to ultimately ensure fairness in the proceedings, it is necessary that digital forensic evidence be properly communicated to, and understood by, those involved in the prosecution, defence, and adjudication of a case. It is also crucial that the rules of disclosure are properly applied. At present there is a limited amount of attention paid to whether the digital forensic evidence will ultimately be admissible. There is an absence of attention paid to the crucial question of whether the evidence is factual or opinion, an absence of attention paid to the underpinning reliability of the evidence and its limitations, and how, if admissible, it ought to be properly communicated and presented.

An inappropriate approach to adducing digital forensic evidence in the magistrates' court is evident. Police officers are placed in the position of attempting to bridge the gap between the provision of unexplained data and the need for the court to understand it, by presenting evidence which, whether fact or opinion, is beyond their knowledge.

Professionals in every discipline across the criminal justice system shared these concerns alongside the inadequacy of time for proper disclosure processes to be respected, for lawyers to properly consider digital forensic evidence and the inequality of arms between prosecution and defence hindering the defence's ability to adequately examine, analyse and effectively challenge digital forensic evidence relied upon by the state.

Theme 4- The Home Office Forensic Impact Points Model

All of the identified forensic impact points are relevant to digital forensics activity and are reflective of the turning points in most criminal investigations and prosecutions. Digital forensic activity is most impactful when applied as early as possible in an investigation.

Two points of impact are currently missed by the Model: Disclosure and Appeal. There is also an underrepresentation of the issues and complexities affecting defence lawyers and experts instructed by them.

The drive to better understand, identify and measure the impact of digital forensics is welcome, particularly if this leads to better resource allocation and improvement in digital forensics expertise. Yet this is not without risk. Attempting to apply relevant metrics, amongst a myriad of different systems, drivers and processes, is a concern. In particular, defining successful use of digital forensics is difficult and is not determined only by the final outcome of an investigation or prosecution. There is a genuine desire and enthusiasm across the criminal justice system for further collaborative, multi-disciplinary research, with academic involvement, to address this complex issue.

Recommendations

Theme 1 – Digital Forensics Literacy

1. All data and outputs, provided by Digital Forensic Units and external digital forensics practitioners to police investigators, must be supported by sufficient explanation to allow its significance and limitations in the context of the investigation to be understood.

2. The creation of regularly updated interactive digital literacy training packages designed for individuals anywhere within the criminal justice system delivering knowledge and understanding of both:
   - the capabilities and limitations of digital forensics processes
   - the data produced

   These resources should be role specific and appropriate to individuals within the police, legal professions and judiciary. Further, consideration must be given to the relevance of the training, ensuring its capacity to stay ahead of evolving technological developments and changes.

3. Digital literacy training packages developed for lawyers should be equally available and accessible to the Crown Prosecution Service and defence representatives. To ensure accessibility, Crown Prosecutors must be provided with an appropriate allocation of time to attend and engage and the cost to defence representatives must be reasonable or funded by the state.

4. Consultation with the judiciary, the Royal Society and the Royal Society of Edinburgh, to ensure that any future judicial primer for court encompassing digital forensics addresses the limitations in digital forensic literacy identified by the Northumbria University Digital Forensics Project.

Theme 2 – Technical and Practical Challenges

5. A significant increase in and strategic deployment of suitably trained Digital Forensic Unit Investigators to address the extensive backlogs, increase the current level of activity and prepare for the inevitable continued increase in demand.

6. A significant increase in and strategic deployment of Digital Media Investigators, in police forces and other investigative agencies, to:
   - enhance the quantity, quality and accessibility of the provision of immediate guidance to investigators and
   - ensure more efficient referrals to the Digital Forensic Units and independent digital forensic practitioners to ensure the pursuit of only reasonable lines of enquiry

7. Establishment of a process which encourages and enables effective communication – upstream and downstream – between Digital Forensic Unit practitioners, police and the Crown Prosecution Service.

8. Development of an effective, modern, data platform for the storage and sharing of digital forensics at all stages of the criminal justice process.

9. A review of whether strategic investment in policing co-access to digital forensic resources (equipment and personnel) would address the challenges of:
   - keeping pace with the advances in technology required by digital forensic practitioners and the discipline
   - financial provision and future investment for delivery and training, now and in the future
   - significant backlogs and workloads associated with digital forensic investigation, that compromise efficiency, capacity and capability
   - inequity of assistance across different case types and across forces
   - a national level of service, underpinned by sustainable achievement and maintenance of accreditation requirements
   - reducing the risk and practice of late and incomplete disclosure to the defence

Theme 3 – Digital Evidence and Admissibility

10. Bespoke training for police officers and Digital Forensic Unit practitioners on the criminal rules of evidence and procedure applicable to digital forensic evidence, specifically centred on matters of reliability, fact and opinion evidence, disclosure and admissibility.

11. An urgent review of current practice in the admission and presentation of digital forensic evidence in magistrates' courts to address non-compliance with the rules of evidence and the Criminal Procedure Rules.

Theme 4 – The Home Office Forensic Impact Model

12. The Home Office to add two further Forensic Impact Points to the current model:
   - Disclosure
   - Appeal

13. Given the findings of the Northumbria University Digital Forensics Project, apply the Forensic Impact Points model in a manner that does not seek to quantify impact at each individual impact point but to learn where future policy and investment could generate the greatest impact through the removal of existing barriers and constraints.

14. Undertake a review of the cases identified within Crown Prosecution Service's 'failed prosecutions' data, to identify the key barriers to the effective and impactful use of digital forensics.

Background

1. Considering the pervasive role of digital forensics in contemporary criminal investigations and prosecutions, it becomes increasingly challenging to envision a criminal scenario where digital forensics would not play a contributing role, even if it is not always immediately apparent. The breadth and speed of the development of digital forensics has outpaced the national infrastructure necessary to utilise the capability and capacity of digital forensic analysis fully and efficiently to both prevent crime as well as detect and investigate suspected criminal activity. The resulting crisis was most recently evidenced in the HM Inspectorate report[4] which drew attention to a national backlog of over 25,000 devices, delays that were failing victims and, despite a National Digital Forensic Strategy,[5] "little confidence that the police service had a coherent plan for improving the situation."[6]

2. Much of the focus has centred on the logistical application of digital forensics, particularly resources within policing, with factors such as digital literacy – knowledge and understanding – also emerging as a theme. The unheard, or less documented, voices were those seated in the courts, who are the end users of the digital forensics process, receiving the associated outputs and reports. The Northumbria University Digital Forensic Project has specifically sought to include these key voices and their experiences. This report, therefore, provides a thorough insight into how digital forensics is instructed, undertaken, utilised, and conveyed between those taking an active role in policing, digital forensics and law, including both prosecution and defence representatives.

3. To better understand how digital forensics is deployed across the criminal justice system, it was necessary to explore i) how and where it provided impact and ii) whether it was used in the most effective manner. The Home Office's 'Forensic Impact Point Model[7] provided a framework to instigate discussion with representatives from across all relevant professions within the criminal justice system. The outputs from these discussions were analysed to identify not only whether impact was taking place, at the anticipated points, but also to consider whether full value was achieved and what changes could elicit a more effective and efficient delivery towards maximum benefits.

[4] HMICFRS (2022) 'An inspection into how well the police and other agencies use digital forensics in their investigations' https://hmicfrs.justiceinspectorates.gov.uk/publications/how-well-the-police-and-other-agencies-use-digital-forensics-in-their-investigations/

[5] NPCC & APCC (2020) 'National Policing Digital Strategy: Digital, Data and Technology Strategy 2020-2030' https://www.npcc.police.uk/SysSiteAssets/media/downloads/our-work/digital-policing/national-policing-digital-strategy-2020-2030.pdf

[6] HMICFRS (2022) 'An inspection into how well the police and other agencies use digital forensics in their investigations' p.1

[7] The Impact of Forensic Science Project: Phase 1 Report, Marie Barrett, 2nd Aug 2022. The Phase 2 Output is within the report and also in Appendix 1. https://assets.publishing.service.gov.uk/media/62e7dd71d3bf7f75bd257e12/Home_Office_Impact_of_Forensic_Science_Project_Phase_1_Report_for_publication_Accessible_Version.pdf

4. The project team comprised academics with well-established professional backgrounds across forensic science, computer science and criminal law, complemented by contributions from those with significant experience of Crown Prosecution Service and Home Office policy and practice. These are:
    - Dr Cerian Griffiths – Barrister and Criminal Investigator
    - Emma Piasecki – Barrister
    - Dr Sophie Carr – Forensic Scientist
    - Philip Anderson – Digital Forensics
    - Professor Tim J Wilson – Criminal Justice Policy

5. The project team would like to acknowledge the valuable contribution of Marie Barrett, Forensic Policy Team, within the Data and Identity Directorate of the Home Office. The team would also like to thank Northumbria University for funding this study and members of Exchange Chambers' Fraud Forum for their input into the study design.

6. The greatest thanks must go to the focus group members, who contributed their time, their expertise, their reflections on, and experiences of, the issues raised in this report. That they did so with such enthusiasm, in the spirit of cooperation, and in the pursuit of improving the positive impact of digital forensic evidence across the criminal justice system is recognised and appreciated by the entire project team.

7. The key findings from this work present the broad challenges as well as providing decision makers with constructive, evidence-based recommendations to assist in increasing the impact of digital forensics and informing future resource and policy decisions in the short, medium, and long term.

Methodology

Aims and Approach

8. The purpose of the Northumbria University Digital Forensics Project was to better understand the use, effectiveness and impact of digital forensics across the criminal justice system. In doing so it also sought to identify the challenges faced by those in all disciplines who interact with digital forensics on a daily basis.

9. Unlike existing research in the area, which considers narrower challenges or experiences of digital forensics, this project sought to capture a broader and more holistic view, garnering the experiences of those across the life of a criminal case, from initial intelligence gathering to, where occurring, criminal appeal.

10. This project's approach is unique. It has developed a methodology designed to obtain a comprehensive understanding of the impact and influence of digital forensics across the entire criminal justice system in all crime types. In order to achieve its aims the project harnessed methods which allowed for the gathering of first-hand experiences of those using digital forensics, and direct discussion between users and stakeholders who are often siloed within the criminal justice system.

11. These users and stakeholders - twenty-six in total - included police officers from four police forces, the National Crime Agency and those involved in counter terrorism, police Digital Forensics Unit Investigators, HM Prison and Probation Service, independent digital forensics practitioners, the Crown Prosecution Service, and solicitors and barristers in independent practice with experience of both prosecuting and defending.

12. In line with the spirit of breaking down professional silos, the Northumbria University project team was interdisciplinary. This harnessed the academic expertise of team members from the disciplines of law, forensic science, digital forensics and public policy. This enabled the team to design data gathering methods and the analysis that gives this report the uniquely holistic voice of those professionals in the criminal justice system who deal most frequently with digital forensics.

13. A mixed-methods qualitative approach was adopted, utilising pre-focus group interviews, online focus groups with mixed groups of professional backgrounds represented, a follow-up survey and a follow up interview.

Pre-Focus Group Interviews

14. Given the breadth of participant experience and the desire for minimal interjection by the project team in the sessions, care was taken to design research questions which would allow for discussion between participants, and not reinforce professional silos or create cross-purposes in the interpretation of questions. Feedback on the proposed questions was therefore obtained in advance of the focus

groups via interviews with a range of participants. These interviews served as a 'trial run' of the questions, and in consequence, some of the language in the questions was clarified.

Focus Groups

15. The focus groups asked participants to speak to the following questions:
    1. In your role, what comes within the term 'digital forensics' or 'digital evidence'?
    2. Where do you perceive digital forensics and digital evidence to have the greatest positive impact?
    3. How cohesive is the approach to digital forensics across the criminal justice system?
    4. What are the barriers to effective use of digital forensics and evidence, and the consequences of these barriers?
    5. What would an ideal system of digital forensics and evidence look like for you?
    6. How can the impact of digital forensics and evidence be better evidenced and measured to inform investment decisions?

16. Participants were given no additional visual prompts or information other than when answering question 2 – for which the focus group facilitator shared the image of the Home Office, Forensic Impact Points Model.[8]

Follow up Survey and Interview

17. An open-question survey was sent to participants immediately following the focus groups to allow participants to make further contributions which they had not the time to make in the focus group, or which had occurred to them subsequently. Participants were also offered a follow up interview to further extend their contribution. Consequently, the data collected through the focus groups was complemented by these contributions.

18. This holistic approach, and the mixed nature of the focus groups, generated the extensive cross-professional discussion and debate which resulted in such rich data. This model is well suited to future national and international research studies into similar issues as the multi-role and cross-organisational approach enables engagement and lesson learning across organisations and jurisdictions.

19. A strength of the Northumbria Digital Forensics Project, and consequently this Report, is the academic objectivity brought by an independent academic research team governed by university research ethics. This objectivity, complimented by the professional practice background of each member of the research team, played a key role in the success of the recruitment of participants.

20. Indeed, our ability to publish such extensive findings is only possible because of the trust placed in us as independent academic researchers and the constructive

[8] See Appendix 1

engagement across professional and organisational boundaries by all research participants at our events. When initially explaining our approach to barristers they were at first reluctant to contribute to what was initially seen as a further Home Office consultation, as they considered that their views routinely went unacknowledged. Because of our ultimate editorial control of the contents of the report, however, we hope that we have contributed to bridge building between the Home Office and legal profession.

21. Equally, we wish to acknowledge the constructive engagement with our approach and respect for our independence shown by Home Office officials. Without genuine mutual respect, transparent cooperation, and inventive collaboration there is little prospect of bringing criminal justice into the 21st century in terms of digital forensics.

22. When drafting this report, we noted that the Home Affairs Committee's report Policing Priorities referred to inter-organisational tensions between the police and the Crown Prosecution Service over where the burden of investigation and paperwork should lie.[9] We wish to clearly report that our overwhelming impression from the discussions on which this report is based is that there is tremendous and highly positive potential for cross-organisational and cross-role engagement in problem and solution identification in response to the major challenges resulting from digital forensics.

23. As such, this model (both its methodology and independent and constructive editorial control) is well suited to future national and international research studies into similar issues as the multi-role and cross-organisational approach enables engagement and lesson learning across organisations and jurisdictions.

[9] Home Affairs Committee, '*Policing Priorities: Committee's* Fifth *Report* of *2022–23'*. Available at: https://publications.parliament.uk/pa/cm5803/cmselect/cmhaff/635/report.html

Analysis

24. Given the nature of the data collection, the most appropriate method of analysis for the Northumbria Digital Forensics Project was thematic.[10] In line with good practice advice on thematic analysis, the project team adopted an approach that was systematic, verifiable, and sequential.[11]

25. When identifying themes and coding the data, the entire research team was involved. This is significant in a multidisciplinary team, researching a subject which incorporates the views and expertise of such a diverse range of participants, as it allowed for different professional and academic perspectives to sense check identified themes.

26. In analysing focus group data, the team collectively identified themes which were then applied to the focus group transcripts through a system of iterative coding. This process involved double coding and sequential and reflexive analysis. At least two members of the team coded every piece of data to ensure reflexivity and scrutiny.

27. This coded data was then analysed in more depth, by a different member of the research team to those who completed the initial coding. This iterative and layered process of analysis allowed for involvement of multiple team members with the aim of interpreting the data in a manner in keeping with the project's objective to create a more holistic and horizontal understanding of the use of digital forensics across the criminal justice system.

28. The process of identifying and applying topics or themes to the data freed the findings from the constraints of the questions asked in the interviews and focus groups. Applying a Grounded Theory approach[12] and being led only by what the research participants discussed, the four broad themes identified by the research team form the central findings of this report.

29. Those four broad themes are:
    1. Digital Forensics Literacy
    2. Technical and Practical Challenges
    3. Digital Evidence and Admissibility

    The fourth theme is focused upon the framework arising out of the *Impact of Forensic Science Project*:

    4. The Home Office Forensic Impact Points Model

[10] Strauss, A., & Corbin, J. (1994). Grounded Theory Methodology: An Overview. In N. Denzin & Y. Lincoln *Handbook of Qualitative Research*. (1st ed, Sage, 1994) 273–284; G. Guest, K.M. MacQueen, and E.E. Namey, *Applied Thematic Analysis*. (1st edn., Los Angeles, Sage, 2012).
[11] Krueger, Richard A and Casey, Mary Anne, *Focus Groups. A Practical Guide for Applied Research. (5th edition,* Sage, 2015).
[12] Glaser, B., & Strauss, A. *The discovery of grounded theory: Strategies for qualitative research*. (Chicago: Aldine, 1967).

30. Given the method of analysis the findings from this project are reported, not in line with the questions asked in the focus groups, but on the basis of those four broad themes. Unsurprisingly there are additional issues not specifically isolated as one of the four themes, but which arise on a reading of them all, and many individual issues which bridge numerous, or all, thematic areas. We have tried to include these contributions, where possible.

31. In presenting this work the findings are set out as summarised representations of the contributions of participants supported by anonymised direct quotations where appropriate. This has the benefit of providing a real voice to the participants and illustrates the passion and unfiltered nature they brought to this project.

32. Within the direct quotations we have adopted the following nomenclature to indicate the professional discipline of the individual participant whilst maintaining anonymity:
    - Police – regional and national policing including those in serious and organised crime and counter-terrorism
    - HM Prison and Probation Service
    - Digital Forensic Unit Investigators
    - Independent Digital Forensic Practitioners
    - Lawyers – Crown Prosecution Service, defence solicitors and barristers in independent practice

Theme 1- Digital Forensics Literacy

Levels of Literacy

33. The absence of digital forensics literacy was identified by focus group participants from every discipline across the investigative and legal process as a barrier which undermines the use, effectiveness, and impact of digital forensics in the criminal justice system.

34. Within the theme of digital literacy, several concerns arose – loosely grouped into the following two areas:
    - Understanding what potential digital evidence can be obtained from a device or system together with an appreciation for the complexity of that data extraction task and the relevance of the ensuing findings.
    - The need for simplified and understandable data and reports, where the results and terminology are explained and communicated with clarity and transparency suitable for a lay person.

35. Underlying both issues is a general, but fundamental, lack of knowledge and understanding in those not intimately involved in digital forensic analyses. This is not unexpected and is most likely broadly representative of the general population. Yet this lack of digital forensics literacy emerged as a significant factor ultimately contributing to the backlog of devices waiting for examination, misunderstandings of data and analysis, inability to properly assess reliability and admissibility, poor evidence communication, discontinued prosecutions and the very real risk of miscarriages of justice.

> "The real goal is the understanding of digital evidence at all the stages. It's not just the experts who need to understand digital, its investigators, CPS, lawyers, judges, everyone up the chain. If there's someone who has no confidence in digital findings in that process and don't understand what's going on, that whole chain breaks down."
>
> Independent Digital Forensics Practitioner

36. The absence of digital forensics literacy was frequently cited as the cause of poor investigatory strategies and inappropriate requests made to both Digital Forensic Units and independent providers of digital forensics by investigating officers, lawyers and the judiciary.

" .. we get it internally where, 'well, can you just give us a download of that phone?' And my heart cringes at that word because what – I can download, I can download music, I can download pictures from the Internet, that's download. But I can't download a phone, yet they won't say it, 'to download a computer', but they will, with the phone. No – you investigate a phone because you don't need – well, you won't get everything off it anyway, you never ever will in a readable form, but we can't pursue it that way because of the massive collateral of data, we have to be proportionate in our in our investigation."

Police

"…sometimes in interview the correct questions aren't asked, so we can't prepare any data for officers to review…"

Independent Digital Forensics Practitioner

"We dealt with a case recently, literally only six people involved - we ended up with, I think it was about 9 terabytes of data. And then when the CPS say yeah, if you can just disclose all of that - no. Not possible. Not enough time. Humans have not existed for long enough to read all of that. It's not gonna happen."

Police

"People think they've got a full copy of the phone when it is not necessarily the case, so they might not understand what they're missing, which is quite significant sometimes."

Independent Digital Forensics Practitioner

37. Focus group participants described investigators and lawyers making spurious or unintelligible requests, borne out of concern that evidence could be missed if they hadn't requested '*everything*'. There was a clear desire expressed by professionals across the criminal justice system to improve their own knowledge, as the ramifications of excessive data requests resulted in increased workload and complexity and a risk of missing the most relevant data. This isn't a new observation given the findings of the 2022 HMICFRS report, in the report, "Investigators reported incidents of prosecutors being overly cautious, requesting unnecessary examinations."[13]

[13] HMICFRS (2022) An inspection into how well the police and other agencies use digital forensics in their investigations. p5. https://hmicfrs.justiceinspectorates.gov.uk/publication-html/how-well-the-police-and-other-agencies-use-digital-forensics-in-their-investigations/

"…. you have got the CPS and the defence, and we're lawyers, we're trying to look at the case from a legal point of view, and we haven't really received any training in what is available, what you can get, how easy it is to get, how difficult it is to get, how likely it is to be of real probative value, or whether it's just going to raise little bits and pieces of inference, and we're interacting with the scientists through an officer who really doesn't know about these things."

Lawyer

" ….. from a policing perspective anyway, making sure people are looking at the right areas. So, it's no good, for example, seizing phones for evidence of stuff on Instagram if actually what you need is cloud tokens and RIPA requests. So, getting the right advice and understanding training behind them, I would say is probably the thing that jumps out to me."

Police

38. There was a similar lack of understanding reported in terms of what was then received. This is inextricably linked with two further issues:
    - Poor format of recovered data not provided in a formal manner
    - Inappropriate expectations upon police officers to understand complex data in the absence of an explanation or report from the Digital Forensic Unit

39. This lack of understanding was reported primarily by focus group participants investigating and prosecuting cases and encompasses data recovered from a device either via a digital kiosk (operated by an investigating officer) or received from a Digital Forensic Unit without an accompanying report explaining either the extraction or the data.

40. Criticisms of the data provided to investigating officers and lawyers include the volume of material provided, the absence of any level of explanation, analysis or context and the unnavigable layout. Without explanation, the recipient is left without a proper understanding of what has been done and what it is that they have received. In those cases where analysis or interpretation of the recovered data is required from a suitably trained expert, but such input is lacking, the potential impact of the digital forensics is lost and the risk of misinterpretation by the recipient arises.

41. There are clear admissibility concerns here that are not recognised or addressed. This issue will be further discussed in the context of the third theme of this project: Digital Evidence and Admissibility.

> "It's meant to be like, you provide an SFR 1, they come back with the issues and then you get an SFR2, but that only essentially exists if it comes from a digital forensic investigator, whereas if we just give the phone report to an officer, the only thing that the court then gets is their statements that they've wrote after reading that phone extraction. So yeah, it's - a lot of the time this happens when it's not necessarily reviewed by digital forensic investigator, we've just extracted the data and given it to them, that's when a lot of the issues tend to come in, so a big fix for it would be for us to do more of the investigations, but, like, backlogs, it's impossible. We already accept loads, so it's essentially you know which one deems a digital forensic investigator and which one shouldn't be too technical that an officer would be able to make the reports based on it."
>
> Digital Forensics Unit Investigator

42. There was also much discussion in relation to the absence of support available to those who do not understand the digital forensic data or evidence provided to them. Certainly, some participants volunteered that in their force or organisation, there is no formalised support mechanism, only that available on an ad-hoc individual basis.

> "So, it's very difficult sometimes to find what you're looking for because of the way that the data is presented to you, sometimes you just don't have a clue what you're looking at, and you can ask around, but that's the only way you can really get proper help. You don't have access to analysts who can - sometimes you do, if it's a really big job and you manage to find the right person to help you or to point you in the right direction, but generally we don't have someone who can produce a nice fancy exhibit booklet…"
>
> Police

43. The challenge of communicating complex digital forensic evidence to a defendant in a manner that is fully understandable to all stakeholders persists, even in circumstances where a report (Streamlined Forensic Report (SFR) or full report) is provided. Both solicitors and barristers emphasised the challenge of comprehending digital forensic reports, particularly the technical content.

44. In addressing this concern, lawyers not only raised the obstacles they face in understanding, conveying and challenging the evidence accurately and coherently but also underscored the very real possibility that jury members, magistrates, or judges may encounter similar difficulties.

45. This issue extends beyond legal professionals and raises the broader question of ensuring clarity and accessibility of technical information for all stakeholders involved in the judicial process.[14]

[14] Carr, S., Piasecki, E, and Gallop, A. "Demonstrating Reliability Through Transparency: a scientific validity framework to assist scientists and lawyers in criminal proceedings" (2019) Forensic Science International, 308, pp 1-6.

> “Some of the reports and I'm by no means making accusations to anybody on this call, but some of the reports received could do with being simplified, because when you're dealing with magistrates and juries, in particular, you cannot assume that they will be familiar with all of the terminology that's been used within the statements.”
>
> Lawyer

46. Regardless of the manner in which digital forensic evidence was provided however, both solicitors and barristers volunteered their own limited digital forensic literacy as a barrier to the most effective understanding and communication of evidence at the trial stage. While this persists, there exists a gap between technical complexity and lay understanding and a consequential risk to justice.

> “There are clear reports and there are the ones that are just look like gobbledygook, and you haven't got a clue what somebody is saying. They have to be simple for us all to understand.”
>
> Lawyer

Training

47. The penultimate question asked in the focus groups was deliberately free form: What would an ideal system of digital forensics and evidence look like for you? The freedom for focus group participants to answer this question in whatever way they chose allowed for a mix of responses from the concise to the more discursive. Given the earlier discussions in the focus groups around challenges of the use of digital forensics, the discussion naturally turned to solutions.

48. Irrespective of role, whether within the police, digital forensics practitioners or lawyers, the need for up to date and relevant training was stressed across the focus groups. Here, the focus is upon training for those other than dedicated digital forensics practitioners - to improve overall literacy. Targeted, role specific training was suggested by participants from all disciplines as a means of addressing, at least in part, the absence or low levels of digital forensics literacy across the criminal justice system. This potential solution was suggested by some disciplines as being required by others i.e. digital forensic practitioners took the view both investigators and lawyers require more training, while other disciplines, lawyers in particular, were quick to identify their own limitations in this area and express the desire for appropriate training.

Training for Police and Specialist Officers within National Policing Agencies

49. Within individual forces, policing roles vary from first responders through to senior investigating officers. Participants in the focus groups acknowledged the resultant different layers of police handling of digital material and considered training in relation to high volume and first responder responsibilities in particular. A first responder's role is far more likely to involve identifying, obtaining, and securing digital devices and material, in many circumstances with secondary consideration given to extraction and analysis.

50. Training around the identification and seizing of the 'right' material was identified by several policing participants in the focus groups. The lack of 'baseline training' for all first responder police staff in what is now a significant part of their role, was raised as a gap in basic training.

> "Baseline training is required annually for control and restraint and first aid – but not for evidence gathering from someone's phone."
>
> Police

51. The training required, identified as needed by police for police, was described as necessary to aid better digital investigative strategies and more appropriate requests for and understanding of digital forensic evidence. The point was also made by more than one participant that this needs to be higher quality and more interactive training than that which is currently available.

> "On that I would say training-wise, quality training- so for digital skills it should be an interactive training session, where you're given tasks like given, you know, given a whole load of data and told 'find this', but you've obviously been given the skills beforehand to try it, so that you can work through some exercises and know that you've actually understood what has been told to you, rather than just an online thing that you just click through. It's quality training, ….. low level assessments all the way throughout so that you can check that you've understood..."
>
> Police

52. As highlighted earlier in this section, there is also a clear requirement to provide training to police officers that ensures that they understand the evidence that they are, or are not, permitted to give. This is addressed in further detail in the context of the third theme of this project: Digital Evidence and Admissibility.

> "So, for me, resourcing yes, but training is the main thing, and a recognition of roles and different areas of expertise, and in particular training in, when you're getting towards expert evidence, all opinion evidence is expert evidence."
>
> Independent Digital Forensics Practitioner

53. Alongside identifying their own need for training, lawyers supported the view of police and digital forensic practitioners that the judiciary are in particular need of appropriate training – including at a very basic level. Junior lawyers highlighted their experiences of having to explain rudimentary aspects of digital forensics to senior colleagues and frequently the judiciary. It was a general point of agreement among lawyers that more senior colleagues and many members of the judiciary were less aware of the digital world generally.

> "We had a judge ordering an entire forensic image on a DVD by the end of the day. And these things are not possible. There's just sort of a level of unknown across the whole spectrum, which then bleeds backwards."
>
> Police

Training for Lawyers

54. The provision of more extensive digital forensics training for the Crown Prosecution Service was identified by participants. This training should focus upon i) how and what to request from recovered devices and ii) aiding understanding of recovered data. Participants made clear that in order for training to be effective Crown Prosecutors must be given adequate time to attend and properly engage with this training. Lawyers representing both the prosecution and defence also identified the absence of equality of arms in respect of access to training as a very real concern. Access to appropriate training may be more difficult for the defence given that they do not always have equal access to similar quality and quantity of resources.

55. In identifying their own need for training, lawyers recognised their own limitations in understanding digital forensics not only undermined their ability to explain it to a client or present to a jury, but impacted their ability to appropriately challenge it.

> "Now just make it clear that the training or education I'm talking about isn't for the people who are writing the reports, who are conducting the investigation. I'm thinking more of education towards the end of the cycle, to the ones that have to use the reports, to give them some basic understanding of what these reports are actually saying."
>
> Lawyer

> "It's been presented in court, or if you're defending and/or prosecuting, because of lack of training in relation to digital forensics, we often don't ask the right questions, because we don't know what we're looking at. We may be experts in RASSO, so rape and serious sexual offences, but we're not necessarily an expert in digital analysis. And I do honestly think that there needs to be more resources put into training the end users as well, to ask the right questions."
>
> Lawyer

56. Given the well documented impact the lack of knowledge and understanding of a specialist field or form of evidence by lawyers can have, this is an area which must be addressed.[15]

57. It was also recognised that the responsibility sits with the provider of the data or the author of the report to ensure it is presented in a manner that is comprehensible to all participants in the criminal justice process.[16] The point was made by more than one participant that the digital literacy level of the average juror cannot be assumed.

58. Training should consider working with digital forensic practitioners in the use of real-world scenarios and case studies, allowing participants to apply their newfound knowledge in practical situations helping reinforce theoretical concepts but also enhancing the participants' ability to comprehend and engage with digital evidence effectively. Collaboration with Digital Forensic Unit Investigators and independent practitioners is crucial for developing a training program that aligns with industry best-practices and pedagogical principles.

[15] Law Commission, Expert Evidence in Criminal Proceedings in England and Wales Cm 325, (2011)
Davies, G. and Piasecki, E. No more laissez faire? Expert evidence, rule changes and reliability: can more effective training for the bar and judiciary prevent miscarriages of justice? J. Crim. L. 2016, 80(5), 327-343. https://doi.org/10.1177/0022018316670967
Wilson, T., Bergman, J., Jackson and A., Popov, O Preventing Machines from Lying: Why Interdisciplinary Collaboration is Essential for Understanding Artifactual or Artefactually Dependent Expert Evidence J. Crim. l. 2024. https://doi.org/10.1177/00220183231226087
[16] Carr, S., Piasecki, E, and Gallop, A. "Demonstrating Reliability Through Transparency: a scientific validity framework to assist scientists and lawyers in criminal proceedings" (2019) Forensic Science International, 308, pp1-6 https://doi.org/10.1016/j.forsciint.2019.110110

Recommendations

1. All data and outputs, provided by Digital Forensic Units and external digital forensics practitioners to police investigators, must be supported by sufficient explanation to allow its significance and limitations in the context of the investigation to be understood.

2. The creation of regularly updated interactive digital literacy training packages designed for individuals anywhere within the criminal justice system delivering knowledge and understanding of both:
    - the capabilities and limitations of digital forensics processes
    - the data produced

    These resources should be role specific and appropriate to individuals within the police, legal professions and judiciary. Further, consideration must be given to the relevance of the training, ensuring its capacity to stay ahead of evolving technological developments and changes.

3. Digital literacy training packages developed for lawyers should be equally available and accessible to the Crown Prosecution Service and defence representatives. To ensure accessibility, Crown Prosecutors must be provided with an appropriate allocation of time to attend and engage and the cost to defence representatives must be reasonable or funded by the state.

4. Consultation with the judiciary, the Royal Society and the Royal Society of Edinburgh, to ensure that any future judicial primer for court encompassing digital forensics addresses the limitations in digital forensic literacy identified by the Northumbria University Digital Forensics Project.

Theme 2- Technical and Practical Challenges

Capacity

59. Just as the use of digital devices, digital media, online activity and social media has exploded in the past decade so too has its use as evidence in criminal prosecutions. It is rare now, to envisage a criminal prosecution without a digital element. This is the case regardless of whether the offence charged is one with a distinct online element – be it fraud conducted online or stalking via social media – or a non-digital offence, for example, assault, in relation to which digital evidence such as call data, cell site analysis, CCTV may all be relevant and admissible. It is also the case that the digital element may be more obscure than overt. In these circumstances, it is little surprise that volume is a key issue identified by participants. This could be observed as two distinct issues:
    - the number of devices and amount of data that is potentially involved in a single investigation
    - the sheer number of investigations that involve an element of digital forensics

60. All participants expressed the view, in very strong terms, that there is insufficient resource to deal with volume. Resource, in this context, is primarily Digital Forensic Unit investigators to deal with this volume of work. It was noted by focus group participants that the key is not only the recruitment of new staff but also their retention.

> "so, again resourcing it's just we have to accept that we're not in Kansas anymore, we need to deal with this properly, and unfortunately we're an expensive capability. If everyone can accept that, you know there might be digital facet to pretty much every job nowadays, certainly every terrorism job and hostile state job that we deal with, but probably in every volume crime job as well. If we're accepting that that's a thing, then how are we not accepting that we need to resource it properly?"
>
> Police

> "So, we need to standardise the roles, we need to standardise – salary would be really helpful, so we don't start bleeding staff across to the private sector or to other forces."
>
> HM Prison and Probation Service

61. Insufficient capacity impacts the quality of work that is produced in an individual case and the amount of time that it takes to produce it. Scaled up, this inevitably

leads to the extensive backlogs that all participants spoke of and is well documented.[17]

> "There is no real time for analysis or scope. The labs are so busy getting any product they are not really engaging with the contents of anything particularly difficult beyond, 'here is the evidence you've essentially asked for'."
>
> Police

> "… queue times going massively long and trials getting dropped purely due to the time. While obviously making sure we do a good investigation as well."
>
> Digital Forensics Unit Investigator

> "… this is a general lack of resources that's caused the backlog that's already been referred to, and the knock on effect of the backlog is the amount of time it's taking cases to get before court, during which some of the other supporting evidence, the live evidence in particular, is lost and by the wayside, people's recollections aren't as clear as they were. And it it's all affected by the time it's taking both to analyse the volume of evidence, but also the resources available. I agree there is a definite cost issue."
>
> Lawyer

62. The participants spoke of different digital forensics strategies within forces, aligned to certain crime types, with the more serious investigations receiving a targeted resource. In these crime types, such as murder or serious sexual assault, the investigation is likely to have the benefit of advice from a Digital Media Investigator[18] and the resource of the Digital Forensic Unit to conduct digital forensic extraction and analysis on any recovered devices. Yet there does not appear to be the capacity, within any of the forces, to extend this priority service across all mainstream criminal investigations.

[17] His Majesty's Inspectorate of Constabulary and Fire & Rescue Services *An inspection into how well the police and other agencies use digital forensics in their investigations*. (2022) Available at: https://hmicfrs.justiceinspectorates.gov.uk/publication-html/how-well-the-police-and-other-agencies-use-digital-forensics-in-their-investigations/

[18] The Digital Media Investigator supports major crime, incidents, operations or any investigation that requires specialist digital investigative assistance. They provide assistance and advice in support of live incidents, investigations, gathering intelligence and conducting proactive/reactive investigations where digital technology and data acquisition opportunities exist. https://profdev.college.police.uk/professional-profile/digital-media-investigator/

> “I think one of our major things is just the amount of data we have to go through and how many investigations we're essentially involved in. We have queues years long - well, over a year-long for a standard case, even months for an urgent. And throughout that you still get the ones that you need to do same day. So, all of that just slows it up, and essentially there's - when you think of like the threat, risk and harm of a of a case - like, we don't even necessarily, digital forensic investigators don't get involved in, say, your burglaries, even though they're important. Basically, the risk of our cases, we have so many high, like, importance cases that there's just there's far too many to handle essentially. So that the lower sort of risk ones are the ones that get passed out to our officers to go through. But yeah, just the amount of evidence on phones and laptops and anything like that is just so massive now that it's very difficult to get it across.”
>
> Digital Forensics Unit Investigator

63. There was a broad consensus among police participants that the valuable role of Digital Media Investigator should not be ring-fenced for more serious cases but widely available as an intrinsic part of an investigation, commencing at the crime scene, in all cases with a digital forensic element. The intervention of a Digital Media Investigator at an early stage aids the initial investigative strategy and ensures prioritisation of actions and identification of devices to be triaged or submitted to the Digital Forensic Unit.

> “I think ideal world you'd have essentially like a digital investigator assigned to every case to help make sense of everything that was coming out. It would never happen because of basically there be so many cases it would just, you’d never have enough people. But I know from a XXXX Police Force perspective, sort of, your major operations and everything like that, we essentially get a digital forensic investigator now assigned to the case from the get-go to help with any sort of queries that come in straight away rather than it going to a different investigator every single time. You've got one for that particular scenario, so they know everything that’s going on with that instance, so they can make, like, an assessment straight away, rather than finding out the entire case and then trying to find out what's relevant.”
>
> Digital Forensics Unit Investigator

64. In less serious cases outputs from the digital kiosk are processed and interrogated by the investigating police officer, who then provide their explanation of the data. This part of the investigation does not have the benefit of input from the Digital Forensics Unit, who would ordinarily understand how the digital kiosk had extracted the data and whether there are any limitations that need to be considered when applying the data to the issues in the case.

"A lot of the cases that come through, sometimes they start off at our level and then they turn into something quite big. So, I mean, consequences are, often, we often don't find things that are probably there because we just don't know how to. And I've also been in court and been asked, you know, 'is there any possibility that messages could be missing from this?' And again, I don't know the answer to that question, because if the suspects and the victim are saying that they think maybe there are some messages missing, I don't, I don't know anything about this extraction process, the programme that I'm using to view it, and whether I've been effective in making sure I've really got every single thing off this phone because I've definitely got some contradictory search results before by doing different queries so the consequences can be quite big, cause if that's, if there's a trial and the jury think something's missing, then that could be huge."

Police

65. If this first stage kiosk process is unsuccessful or further data is sought, then the device could be submitted to the Digital Forensic Unit for investigation. Digital Forensic Unit Investigators use their expertise to extract data from digital devices and storage media using specialised tools and techniques. In less serious cases the volume of work in the Digital Forensic Unit is such that they do not have the capacity to explain or interpret or provide a report on the data. The reality is that once the data is extracted, it is handed over to the investigating officer, who must interpret the information and draw conclusions relevant to the investigation. This may involve correlating digital evidence with other pieces of evidence, identifying patterns, timelines, and anomalies, and ultimately using the information to support the investigation's objectives.

66. In Digital Forensic Units the specialist expertise is utilised in ensuring that the extraction process is conducted in a forensically sound manner, preserving the integrity of the evidence, and adhering to legal and procedural guidelines. However, this extraction process is often not explained and no analysis is applied by the expert to the data – presenting a risk that the extraction process is not understood and the analysis is undertaken by a person without the appropriate expertise. There is also the potential that investigative opportunities are missed if the investigating officer is divorced from the extraction process.

"We, as digital forensics practitioners… at some point we are just pushing data to police officers and investigation teams. They are not qualified or equipped to interpret that data, realistically, to extrapolate from the vast volume of that data and provide key evidence, and they could be missing a whole host of information that's sitting in that in that data set that they've been given because they don't know what they're looking at, and that's no disrespect to the to the police officers that are doing that, it's just the serious amount of volume of data that's there."

HM Prison and Probation Service

> “The labs are so busy getting any product they are not really engaging with the contents of anything particularly difficult beyond, ‘here is the evidence you've essentially asked for’. I think we have issues here where the investigator has never seen the phone is asking for things from a forensic lab who don't know the investigation.”
>
> Police

> “Then I've received training on how to extract phones which are then pass to other OICs for their job’s etcetera, etcetera. But none of them have received any training in interpreting the consequences of those extractions being performed. But then when you run through it, even the most rudimentary, as was being said, the messages, the WhatsApp’s, uh, the very simple digital media that we can have available.”
>
> Police

67. One suggestion was the introduction of ‘analysis teams’ to provide a layer of additional support for the investigating officer.

> “We're going to talk about volume a lot, I think, during this – he probably doesn't need great analysis, he just wants the extract and it's there are other teams who really need someone to look at that phone to explain and explain it well for the for the CPS. We could almost do with a separate analysis team across the boards, essentially, so we don't slow down this grinding wheel of getting the device's extracted, so the simple ones get sorted. But when you have a complex one, the labs don't really seem to have time, and the officers don't even think about it as a concept to go back to the DFU if they're stuck.”
>
> Police

> “…but you just said there about having analysis teams. So we do that specifically in Counter Terrorism policing because we recognise that it is just, it's too heavy a burden to give to an investigator or to the lab. The lab is there to do a function and it's not to analyse, there is an exploitation capability. So we need to have a separate capability that does that.”
>
> Police

68. In addition, to the complex capability issues set out above, police in particular reported some operational barriers that significantly undermine the ability of digital forensic evidence to have its greatest impact but which might be considered simple to resolve.

"So, for example, if I want to do a phone download, one of the biggest obstructions for me is getting the phone out of Property, because Property is not 24/7 and I am on a shift pattern. So, I need to wait for my shifts to align with Property, I need to get it out, I then need to get it to the place where it's going, so I need to try and align those dates with where the like or whoever's gonna download the phone - their working hours, which is also not 24/7."

Police

Communication

69. Compounding the challenges arising from volume, the focus group discussions identified that not everyone has contact with the right people, devices, and systems in an accessible manner and at a point that meets the timely needs of the case. This is not only within individual units and police forces but also extends to cross-disciplinary working at the point where an investigation or prosecution spans those within policing and the legal profession.

70. The lack of coherence and communication between disciplines – that is digital forensic practitioners, police investigators and prosecuting lawyers – was stressed by participants.

71. When discussing possible improvements to the use of digital forensics across the criminal justice system, suggestions were made as to mechanisms and processes for better cross-system communication. Participants were keen to see two types of change. The first is a culture change allowing greater communication between Digital Forensics Units, police investigators and prosecutors – both upstream and downstream. This would significantly improve the single communication which occurs when device extraction has taken place, leaving the investigator and prosecutor without opportunity to ask questions or discussion to aid their understanding of the findings.

"I'd like digital forensic evidence to look like – a lot more communication between the people doing it and the people bringing in devices; some form of system where you can have more than one visit back and forth, so the actual details of the case can be thrashed out."

Police

"Better interaction between the investigation team and the digital forensics team, with an oversight team, helps investigators make decisions which helps digital forensic experts provide the content they want. It is not a magic wand but is one of the little things that could be done to add 5% or 10% improvements…"

HM Prison and Probation Service

72. The second change is the development of an effective, modern, data platform for the storage and sharing of digital forensics at all stages of the criminal justice process. In addition to easing communication and reducing delays it would avoid the current practical problem related to poor presentation of data and the passing of data in inappropriate formats. Numerous participants described passing around USBs, discs and vast swathes of paper. Apart from the inconvenience, this presents obvious data handling risks.

> "I'll say some of the difficulties as well is – essentially, we'll look at all the digital evidence, we make the reports, and then basically it goes through maybe three different hands before it gets to court. …how we would get the data across to the court system or a better way of like presenting data. Which I said, such as, like, the review platform, if we had a nice review platform like that, I feel it would take away a lot of the ambiguity of people trying to explain data when we could literally write it as it is."
>
> Digital Forensics Unit Investigator

> "For a start, could I ask that all police forces actually adopted the same platform. Because – it's a small niggle, but it causes so much trouble within the system that when you're talking about CCTV or any digitised evidence of that nature, Northumbria, Durham, Cleveland, every force in the UK is using a different system, and then you can build into that common platform and DCS and all of the other major platforms that the criminal justice system uses – they don't interact with each other."
>
> Lawyer

> "Like an online review platform, essentially – whereas I find my evidence put it onto an online review platform, that got sent to the officer who can pass it on to CPS so they can basically review if that was relevant to the investigation, much easier, rather than passing USBs and discs and everything around, so just an online system that's basically tailored towards digital evidence as well, not something that's just like a SharePoint for documents, but something that you could essentially use to store digital evidence on. I know it's something that we're looking at, but I don't think it's not like a nationwide sort of thing that's been looked at."
>
> Digital Forensic Unit Investigator

73. A significant level of investment is necessary, across the criminal justice system, to modernise and meet the needs of current IT capability and digital forensic evidence. This was not only evident from the perspective of presenting evidence at court but also when transferring and conveying digital forensic data and evidence between individuals in different roles and disciplines.

Technological Challenges

74. Underlying the significant concern with the volumes associated with digital forensics is the very real issue of the fast-paced changes in technology and software. Those working at the coal face of digital forensics spoke of the 'arms race'.

> "… mobile phones is it's a constantly changing beast, and so one of my lines I often use is 'something I can do today, I might not be able to do tomorrow, but something I can't do today I may be able to do tomorrow'. And so that in itself is a challenge…"
>
> Police

> ".. we're consistently and constantly every day in a technical technological arms race. … one day we're ahead the next day, through an update of an app and you see how often your own phones like update their apps are like oh is another update. As a user I don't see any difference whatsoever. What was that are getting different emoji. Brilliant. I've now got a crying emoji or something. But what you don't realise in the background is that like the entire background data table has changed, which immediately makes us go dark. So, we are then very much waiting then for our commercial solutions to be able to update as well. And that's a really real challenge."
>
> Police

> "And we have a multitude of products and a multitude of tools that do a multitude of things. Not one product will give you the same result as another one. Which is a problem. Having an investigator realise that, having CPS, the judicial system, realise that, obviously we've highlighted that on previous questions where we've examined a mobile phone today on a particular piece of software, next week we get an update on that software, or the phone gets an update, or the application gets an update on the phone. We then don't see the context of potential messages or content within the particular area that we're looking at, 'but you got it last week or you had it last time', and that's a conversation that comes quite a lot. And that's down to the arms race."
>
> HM Prisons and Probation Service

75. The requirement to keep pace with technological advances is a necessity not an option. The ramifications of which have significant impact. Firstly, there are costs associated with purchasing and maintaining new equipment and software. Secondly the requirements to ensure users and digital forensic activities can demonstrate compliance with the Forensic Science Regulator Code of Practice[19] and requirements for accreditation.

[19] Forensic Science Regulator Code of Practice, Version 1, published 13 March 2023, revised 27 April 2023 https://www.gov.uk/government/publications/statutory-code-of-practice-for-forensic-science-activities

Regulation and Accreditation

76. The role of the Forensic Science Regulator (FSR) commenced in 2007, with the remit to deliver an appropriate quality standard system that provided reliable forensic science provision to the criminal justice system of England and Wales. This system includes discipline specific Forensic Science Activity (FSA) standards that are mapped to internationally recognised laboratory measurement standards and guidance (ISO/IEC 17025) and aligned to the principles of the FSR's Code of Practice (FSR Code). Now in place as a statutory system, this process is regulated via individual forensic science service providers (units/companies[20]) demonstrating, through independent UKAS accreditation, that they have an appropriate quality management system in place that meets the requirements of the FSR's Code for the particular set of forensic science activities (or sub-activities) that they are delivering.

77. These requirements include method validation, competency testing and auditable procedures; all designed to demonstrate that appropriate methods are used to analyse material and that the results and limits of that analysis are fully understood by those practicing the work. Since the enactment of the Forensic Science Regulator Act 2021, where statutory regulation applies, it is compulsory in England and Wales for all persons providing expert forensic science evidence to declare whether i) they are UKAS accredited for the work they are undertaking and ii) compliant with the FSR Code.

78. The consensus across the focus groups was that there was a role and benefit to regulating the work undertaken in the discipline of digital forensics but that this was not without its tensions. There was recognition that regulation and accreditation was necessary to provide a level of standardisation to the professional discipline. It has delivered the advantage of helping to prevent incompetent individuals/companies remaining in, or entering, the marketplace.

> "…when we're bidding on tenders, they're specifically requesting a specification for accreditation. And if you don't meet that specification, you're not allowed to bid. So, it's encouraging people to become accredited, …."
>
> Independent Digital Forensic Practitioner

79. Much discussion centred on the relevance to digital forensics of the chosen ISO/IEC 17025 standard, as well as the costs and time taken to enact and demonstrate compliance to achieve UKAS accreditation and recognised conformity with the FSR Code. Many participants spoke of the waste of effort and resource in multiple forces undertaking identical validation exercises separately.

[20] Including Police Digital Forensic Units and Independent Digital Forensic Providers

80. This tension was coupled with inter and intra force variety on what areas and analysis fell within the remit of these requirements alongside the rapidly developing nature and capabilities of the 'digital' landscape.

> "There's a lot of forces using similar or the same software, but they all have to scientifically essentially validate it. So, we've got every force cross country doing checks on the same bit of software, which is time consuming and seemingly pointless."
>
> Police

81. Many participants, directly involved with the accreditation process, did raise the costs associated with this as a significant barrier, with the concern that not all can afford this financial outlay. This was observed by those working within police forces as well as those in the private sector, with the added fear that many units are only accredited for a limited scope of forensic activities. This highlights two risks:
    - that there will be a limited number of units (force and private providers) accredited to deliver on the full range of activities needed for more complex casework
    - will those with limited scope be driven out of the marketplace, leading to a lack of capacity across the sector

> "…I think it [accreditation to the ISO standards] does fit the bill – the downside of it is it takes a massive amount of time, it costs a ton of money, and it is absolutely crazy to maintain – you basically need a team of people to maintain it and that is a big barrier."
>
> Independent Digital Forensic Practitioner

82. The FSR Code requires all forensic science disciplines to be accredited to the same group of ISO standards concerned with competencies for testing and calibration.[21] Amongst the participants, there was a difference of opinion on whether these standards were 'a good fit' for digital forensics.

> "There are other ISO standards that we could have used …. we're actually getting less evidence or intelligence because of these standards and actually we could mislead the court."
>
> Police

83. Whilst this isn't the place to discuss the appropriateness, or otherwise, of the standards mapped to the accreditation process, it is necessary to note that the participants directly concerned with undertaking digital forensic activity spoke of an unclear fit and understanding - inadvertently hindering their approach to their work.

84. As digital capabilities progress at speed, the application of digital forensics is expanding beyond its genesis in mobile phones and computing. Other concerns were

[21] ISO 17025/17020 is the main international standard for any laboratory, regardless of size or extent of scope, to demonstrate technical competency for testing and calibration practices, providing independent assurance of reliability.

the FSR's distinction between digital 'analysis' and 'investigation'; the validation of 'tools' versus 'methods', and the cost (expense and time) to re-validate updates to software tools - these decisions ultimately influence the activities considered under accreditation and therefore the form of work undertaken and provided to the criminal justice system.

85. It is notable that the FSR defines anyone undertaking a Forensic Science Activity (FSA), in this case FSA-DIG-100,[22] as a practitioner. This would classify a frontline officer as a 'practitioner' when they are undertaking activity on a digital kiosk. However, there appears to be significant inconsistency. The FSR code compliance also defines this work as technical (factual) reporting; "the reporting of findings based solely on the technical competence of the individual' and suggests that no inferences/explanation (opinion) are drawn from the findings."[23]

86. It was reported that compliance had possible unintended consequences in behaviours and outputs as practitioners struggled to balance sound regulatory principles with inadequate funding.

> "It (accreditation) does force very narrow minded thinking at certain times if it's not carefully approached, because everyone just sticks to the 123 that's written procedure rather than what's the best way to approach something and it's not particularly to take away from the positive verification side of things, that, it's very good at validation and things like that and confidence, but other elements it just holds things back – even something as simple as having to re-evaluate every – sometimes they have a software update with their own software, we have an update every month and how do you keep up with that. Well, the answer is they don't, they just keep using the old less perfect version."
>
> Independent Digital Forensics Practitioner

> "One of the things you've got to be careful of is terminology in terms of interpretation, because there's a big thing around FSR codes and the interpretation of results. So, I think digital forensics, in terms of what we do, is more looking for the data and then presenting it, and I think that keyword there is presenting, and not interpreting, because that's a whole different ball game in the terms of accreditation."
>
> Independent Digital Forensics Practitioner

87. These points illustrate systemic tensions within digital forensics, particularly when considered in the context of the different levels of extraction activities undertaken by different roles – investigating officers using digital kiosks versus investigators within the Digital Forensic Unit. Compliance with accreditation requirements influences the

[22] FSA-DIG-100 Data capture, processing and analysis from digital storage devices – within The FSR Code of Practice, Version 1, (2023) at 108.3.13

[23] The FSR Code of Practice, Version 1 (2023) p359 "An example would be where a digital forensic practitioner has used a specific software tool to extract data from a mobile phone. A factual report explains what the practitioner has done and the findings, such as a list of the files of a certain type that were retrieved. It offers no opinion on how the files came to be on the device or whether any of their content is relevant to a fact in issue in the case".

quality of extracted data as well as how, and who, relays that information to the Crown Prosecution Service and others. The effect of how police classify their activities and the level of police resourcing within digital forensics in conjunction with FSR compliance has ramifications on both the format and quality of digital evidence presented to court that has significant implications for the integrity of criminal justice.

Disclosure Challenges

88. Significant disclosure challenges were identified by participants from all professions. This aligns with concerns raised in recent years by the Serious Fraud Office, "One of the biggest challenges right now is disclosure… the current disclosure framework was designed before the advent of mass digital data."[24] Despite efforts to address the challenges of disclosure, such as the 2020 Attorney General's Guidelines[25], research participants from across the professions reported how ensuring that relevant digital evidence is disclosed in a timely manner is a continuing and ongoing challenge, especially when dealing with large datasets and complex forensic analyses.

89. Digital forensics practitioners, investigators and prosecutors identified the main difficulty as volume in an individual case. The challenges of dealing with the management of large volumes of digital material are compounded by the need to be sensitive in the handling of data relating to complainants and witnesses. Despite the pressures created by volume, digital forensics practitioners recognised the importance of compliance with disclosure obligations as a key part of their role.

> "..how do you sift large volumes of data and what are your disclosure requirements and how do you use that usefully within an investigation or an evaluation?"
>
> Independent Digital Forensic Provider

90. The lawyers were more alert to the reality that deficiencies in disclosure may undermine the fairness of a trial and the consequent safety of a conviction – which is not in the interests of the defendant, the complainant or public confidence and trust in the criminal justice system.

[24] https://www.sfo.gov.uk/2022/09/05/sfo-director-lisa-osofsky-gives-keynote-speech-at-cambridge-symposium/
[25] Griffiths, C. (2022). Getting people thinking and talking: An exploration of the Attorney General's 2020 guidelines on disclosure. The International Journal of Evidence & Proof, 26(4), 359-380. https://doi.org/10.1177/13657127221124362

> "we're always told that we should consider disclosure from the get-go and right from the start of the case, especially in terms of considering a disclosure strategy and working with other stakeholders and organisations to think about, for example, the parameters of phone download or to put in place the strategies so that it's really clear from the start. And also engaging with - I suppose again from the CPS perspective, engaging with defence as well to think about what the issues are and then come up with a sensible strategy."
>
> Lawyer

91. Across disciplines, the focus group discussions identified numerous broad practical challenges. Alongside volume, these included the complex technical nature of the evidence, the diverse range of data, difficulties in identifying and agreeing appropriate and reasonable search terms or parameters, comprehending, and interpreting the information, the critical importance of timely disclosure, and the constraints posed by limited resources.[26]

92. It was agreed generally across participants that the sheer volume and diversity of digital data from emails and images to the more complex file metadata and encrypted files, managing the variety of digital evidence and ensuring all relevant materials are disclosed in a comprehensible manner is a substantial task.

93. A number of policing participants lamented the complexities and contradictions of applicable legislation, codes and guidelines and their inconsistent - sometimes irreconcilable - use, application and objectives.[27]

> "In terms of the disclosure, there's been changes, recent changes, where we have digital processing notices which limit the data that can be made available. So basically, they say to provide reasonable grounds of enquiry as to why this data is needed to try and streamline the investigation process and reduce the amount of data that's being provided to prosecution and stuff. And one of the interesting things is from a disclosure perspective, that when the prosecution present that they've conducted an examination in accordance with a digital processing notice, and as a result restricted the examination to particular artefacts, from a defence perspective, they request all of the data. Which is quite interesting, really, because the whole point of the digital processing notices is to not invade the privacy of the victim, or suspect, in the case."
>
> Independent Digital Forensic Practitioner

[26] Anderson, P., Sampson, D. & Gilroy, S. Digital investigations: relevance and confidence in disclosure. *ERA Forum* **22**, 587–599 (2021). https://doi.org/10.1007/s12027-021-00687-1

[27] Criminal Procedure and Investigations Act 1996: Criminal Procedure and Investigations Act 1996, Code of Practice; Attorney General's Guidelines on Disclosure (2022), ACPO Good Practice Guide for Digital Evidence (2012), Crown Prosecution Service Disclosure Manual (2022).

94. Both police and Digital Forensic Unit Investigators also lamented the impact on disclosure of differences in outputs generated by different approaches and software packages.

> "I think this comes back to something ***** mentioned earlier about the difference between Basic Command Unit and specialist. So, specialist crime wouldn't, or at least I wouldn't be advising them to and the digital strategy advisor and MFR wouldn't be advising them to do a triage or level one first, because, you know, this is forensics, we don't want two different copies of the same device that that show slightly different things. Because MSAB will read slightly different parts of the phone than Cellebrite, GreyKey will do something slightly different. Everyone will do something slightly different, and the last thing we want is multiple copies of a device existing. It's gonna create issues for you in disclosure and review of that device."
>
> Police

95. One policing participant described how, in their experience, the concept of proportionality is restricting appropriate investigation and risks misuse as a means of managing workload and reducing demand.

> "Sorry, I just want to add to what ****** was saying about the interaction with the new guidance around proportionality, and as has been said, the days of fishing expeditions are over. And ***** doesn't mind me saying that he's encountering difficulties with it in a relatively resource rich environment. I think the way it's been taken and interpreted locally is obviously, because of the resourcing issues around digital forensics, effectively it's being used as a good justification as to why we can't follow a line of inquiry that we might have followed before, simply as a way of managing work, of managing the amount of material we produce in a case. So like, phones not being examined, that we probably would have before, and while obviously there's questions about intrusiveness and it does allow us to manage risks to some extent, and I've got cases where phones were examined under the previous guidance where there was number question of- say, a rape case, that's primarily what we I investigate - no question of communications between the parties, defendant has raised that he is a homosexual. What would probably now be described as a fishing expedition and therefore not be authorised under the new guidance, is download his phone and found that he is accessing lots and lots of heterosexual pornography, which undermines his defence that he's raised at interview. And that sort of thing I think is an issue, it's almost being used as a route to manage demand, but we are I'm definitely losing opportunities because of that because that's how it's being interpreted locally."
>
> Police

Recommendations

5. A significant increase in and strategic deployment of suitably trained Digital Forensic Unit Investigators to address the extensive backlogs, increase the current level of activity and prepare for the inevitable continued increase in demand

6. A significant increase in and strategic deployment of Digital Media Investigators, in police forces and other investigative agencies, to:
   - enhance the quantity, quality and accessibility of the provision of immediate guidance to investigators and
   - ensure more efficient referrals to the Digital Forensic Units and independent digital forensic practitioners to ensure the pursuit of only reasonable lines of enquiry

7. Establishment of a process which encourages and enables effective communication – upstream and downstream – between digital forensic unit practitioners, police and the Crown Prosecution Service

8. Development of an effective, modern, data platform for the storage and sharing of digital forensics at all stages of the criminal justice process

9. A review of whether strategic investment in policing co-access to digital forensic resources (equipment and personnel) would address the challenges of:
   - keeping pace with the advances in technology required by digital forensic practitioners and the discipline
   - financial provision and future investment for delivery and training, now and in the future
   - significant backlogs and workloads associated with digital forensic investigation, that compromise efficiency, capacity and capability
   - inequity of assistance across different case types and across forces
   - a national level of service, underpinned by sustainable achievement and maintenance of accreditation requirements
   - reducing the risk and practice of late and incomplete disclosure to the defence

Theme 3- Digital Evidence and Admissibility

Admissibility

96. For digital forensic evidence to be relied upon in criminal proceedings it must, like any type of evidence, be relevant and admissible – and not excluded by evidential or procedural rules. Once admitted at trial the weight of the evidence is a matter to be determined by the tribunal of fact – the magistrate or judge in the magistrates' court or the jury in the Crown Court. To properly determine relevance, admissibility, and weight, and to ultimately ensure fairness in the proceedings, it is necessary that digital forensic evidence be properly communicated to, and understood by, those involved in the prosecution, defence, and adjudication of a case. It is also crucial that the rules of disclosure are properly applied.

97. The challenges faced by the criminal justice system and all of those involved in it, in the receipt and handling of new kinds of evidence, are well documented. Forensic science evidence of one kind or another – be it DNA, fingerprints, or ballistics - have posed significant challenges. The additional challenges with digital forensics are the scale of provision and the rate of change. Never has another type of forensic evidence, or indeed all other types of forensic evidence together, so quickly become so firmly embedded in the vast majority of criminal prosecutions across the magistrates' and Crown Courts.[28] It is in this context that digital forensics as an evidence type is now being addressed.

98. The focus group contributions made it clear that there was a limited amount of attention paid to whether the digital forensic evidence would ultimately be admissible. This included an absence of attention paid to the crucial question of whether the evidence is factual or opinion, an absence of attention to the underpinning reliability of the evidence and its limitations, and how, if admissible, it ought properly to be communicated and presented and by whom.

99. The distinction between factual and opinion evidence is a crucial one. While drawing the distinction can sometimes be tricky, as a rule, only factual evidence may be given by a non-expert witness. Where a matter before the court requires expertise, opinion evidence may be given by an appropriate, '*peritus*'[29] expert subject to evidential[30] and procedural rules[31] which place additional responsibilities on the witness to act impartially, providing the court with independent assistance.

100. Several participants from across the criminal justice system expressed the concern that given the practice of extracted information being passed unexplained from

[28] House of Lords, Forensic science and the criminal justice system: a blueprint for change, HL Paper 333. https://publications.parliament.uk/pa/ld201719/ldselect/ldsctech/333/333.pdf

[29] R v Silverlock [1984] 2 QB 766, [771].

[30] The matter on which the expert evidence is called must be one on which the court requires the assistance of an expert (i.e. it is a matter outside of the tribunal's own experience and knowledge) and the evidence must be sufficiently reliable to be admitted Criminal Practice Direction 1.1.1d, Dlugosz [2013] EWCA Crim 2.

[31] Criminal Procedure Rules Part 19.

Digital Forensic Units (or equivalent) to investigators, this distinction is often not considered or respected in practice.

101. The extent to which prosecutors were in receipt of unexplained data or evidence with no appropriate witness to communicate it was highlighted in all focus groups by participants from various backgrounds. Multiple examples were provided of investigating officers attempting to bridge the gap.

> "You know, I've seen plenty of cases where you've got a phones officer who gives you a kind of three-page document, tried to digest hundreds of pages of messages. This is just a recent example, and obviously that officers spent a lot of time doing that, but from a court perspective it's of no use, you can't put an officer's commentary to a witness, so, and that officer's trying to just plug a gap obviously and trying to assist as best they can."
>
> Lawyer

102. Lawyers also reported receiving vast amounts of data, in an inappropriate format, which they were expected to understand and rely upon as part of the case for the prosecution or understand and potentially challenge or rely upon on behalf of the defendant.

> "But in my experience, again that's still and by and large, the way we tend to receive downloads, even on an Excel spreadsheet or on PDF."
>
> Lawyer

103. Many participants gave examples of occasions on which police officers were called to give evidence in circumstances where it wasn't clear whether that evidence was opinion or fact and, in any event, the officer lacked the necessary digital forensic knowledge to understand, or appropriately explain and communicate it or its limitations. This was described to be prevalent in the magistrates' court.

> "And it was also who was producing the reports, i.e. was it a digital forensic investigator, or was it a police officer with no sort of forensic knowledge looking at the data and then making his own sort of ideas as to how that is on there, but sort of portraying it across in his own way, when it's, not necessarily in a digital aspect correct."
>
> Independent Digital Forensics Practitioner

104. Even where the evidence is factual, it requires presentation by an appropriate witness able to understand and effectively communicate it to those who understand it less, or not at all. The failure to adhere to this seemingly simple principle appeared to have been accepted as normal practice in magistrates' courts.

"One of the issues that I have anyway is a lack of understanding really, in terms of the evidence that I get. …. What I do, if I've got any time in advance of a case to look at it, I just think oh well I'll get the OIC to come, I'll put them in the witness box and ask them, but the issue is …. OICs aren't, in the main, experts in this area either, so I don't know either, and we're asking people to look at this evidence and interpret it."

Lawyer

105. In addition to the lack of regard to the rules of evidence and procedure and the risk to the proper adjudication of a case and the consequential risk of a miscarriage of justice, taking this approach was reported to undermine prosecutions.

"I've had police officers come into court to try and explain phone downloads and other technical material that they frankly, don't have any idea more than sort of the average person would be able to, so they can't add value and then that brings its own problems because they will make those admissions and then it – doesn't necessarily in all cases, but it could put doubt in a criminal trial [about] the validity of the actual material because no one's there to actually explain it in terms of how they've come to get it and how and what it means."

Lawyer

106. Experts in independent practice (instructed by both the prosecution and the defence) were vocal in their concerns that analysis of data is conducted, and inferences are drawn, by investigators either provided with data by the Digital Forensic Unit or extracted via a digital kiosk – who do not understand it. These independent experts demonstrated greater awareness of the risk posed by a failure to comply with the rules of evidence and procedure and the FSR Code. The point was made in multiple focus groups that the ability to use a device does not necessarily mean the operator understands the output.

"Call data – you can factually recover it; you can factually normalise it and present it in maps – it doesn't mean that's what the device was doing. Equating expertise with the ability to use a tool, it's a major hazard."

Independent Digital Forensics Practitioner

"When you're getting towards expert evidence, all opinion evidence is expert evidence, and stuff like cell-site, the location of the phone is what you're talking about. It's not in the record – anything you do is inference. Inference is opinion, right? It's expert evidence."

Independent Digital Forensics Practitioner

"And the other one for me, which I continually come up against is inference. And so, for me, you have got a difference between some types of evidence that stand on their own, and there are other ones which don't. And I've heard barristers say that for example, inference is a factless common sense, but it might be a fact you've recovered some data for the device. It doesn't mean it's an accurate reflection of what that device was doing at the time."

Independent Digital Forensics Practitioner

107. Certainly, the practices described by focus group participants above are not practices that can be envisaged in relation to any other type of evidence.

"You just don't do it, you don't have DNA people just saying, 'well, I press this button and I've got this output, over to you to have a look at the profiles'."

Independent Digital Forensics Practitioner

108. Some of the existing concerns relating to the use of Streamlined Forensic Reports and the constant lack of context and potential for misrepresentation [32] were highlighted as an issue by members of the focus groups in relation to forensic digital evidence.

"Context is a key thing – one of the key areas we need to focus on when we're looking at large volumes of data. Because of the backlogs, what we're trying to do is reduce the amount of data which is being presented as evidence, and that's where the context comes in, because if we're looking specifically – if a sexual assault happened on say the 1st May, then they want the communications for the 1st May to the week after, or a couple of days after.

But before that, there may be two months of conversation leading up to that which provide the context in the case, and that's the key thing I think with digital forensics. It's not losing the context by reducing all of this data and trying to streamline the information for the courts so much that ... we end up losing the context and losing the bigger picture of exactly what happened."

Independent Digital Forensics Practitioner

"And that there is ever more… reliance upon digital media and digital forensics in particular – although whether as a result of timesaving or cost-cutting – but unless you really dig deep, the forensic evidence that we tend to receive digitally is pretty much a pared-back, watered-down summary document, unless you kick and scream for more."

Lawyer

[32] Carr, S., Edmond, G., and Piasecki, E., - Science Friction: Streamlined Forensic Reporting, Reliability and Justice. (2018), Oxford Journal of Legal Studies, 38 (4). pp. 764-792. https://doi.org/10.1093/ojls/ggy025

Disclosure

109. Not surprisingly the issue of disclosure of digital forensics evidence was one which troubled several participants – regardless of their role within the criminal justice system. The concerns again here related to volume, in this context the inability to properly consider all digital evidence, discharge the disclosure obligations in relation to it and the subsequent late disclosure of evidence often in an unnavigable form.

110. The impact of disclosure issues upon the prosecution and defence of cases, including very serious cases, was experienced by both prosecution and defence barristers as late as the first day of trial. The potential of a failed prosecution where it might otherwise have succeeded and the very real risk of a wrongful conviction narrowly avoided were very clear from the cases in which participants had been involved.

> "I defended someone who was a good character and remanded on suspicion of armed robbery. A 50,000 page download was served the week before trial. And when we looked through it, it corroborated precisely what he'd said in his defence, and the case was dropped on the morning of the trial.
>
> So the data concerned that wasn't looked at was on the day of the robbery, conversations that got on the day. So that's one of those scenarios where if I'm really honest, it just hasn't been looked at properly. And obviously the consequence of that is if that hadn't been disclosed, that trial could have gone ahead. That man could have been convicted and given a hefty sentence and no one would ever have known about that data."
>
> Lawyer

111. Many participants from a range of represented professions expressed concern for the current gravity of issues impacting upon the current quality and manner of presentation of digital forensic evidence at trial. It is worthy of note that alongside the issues described above, practical presentational issues further undermined the quality of communication of digital forensic evidence, and therefore its impact.

> "One other thing I was going to say is talking about the criminal justice system and digital forensics, if – just thinking about, for example CCTV, and like what fancy things you can do with it and, you know, there's no point being able to do great things with your CCTV and then going into a courtroom where the screen is really poor quality, doesn't function properly, it's in poor location, the jury can't see it properly, they're having to stand up, there's light, you know, the light is reflecting off the screen so they can't see, and then they go into their jury room and their, you know, their screen there is from the dark ages. And so, there's no point presenting this brilliant forensic product and then putting it on the really poor digital systems that are actually in the courtroom."
>
> Police

> "I think as well – I realise there may be obstacles to this, but as we were talking ideal world scenario, consistency of a product in terms of the software that's being used and the way in which the evidence, the data, is presented, the way in which it then becomes an evidential product. We just get a myriad of different formats of this stuff going before juries and it can be pretty chaotic. But I think where it's all come from a phone read, really, it can't be beyond the wit of man to actually do it in a sleek, sophisticated, consistent way, but that does mean that all the different forces up and down the country need to, you know, not have a million different products going on."
>
> Lawyer

Equality of Arms

112. Article 6 of the European Convention on Human Rights considers the principle of equality of arms to be an inherent feature of a fair trial. That is, the accused must be permitted to present his case in a manner which does not place him at a substantial disadvantage vis-à-vis his opponent.[33] Yet it is at the point of trial that the absence of equality between the prosecution and defence can be most keenly felt, depriving the defence of the opportunity to challenge, in good time, or at all, the digital forensic evidence relied upon by the state.

113. The inequality was described by focus group participants to be particularly evident in two respects. They are funding and time. Digital evidence relied upon by the prosecution is funded by the state on a more accessible model than that provided to the defence via funding applications. While the police and prosecution are expected to have a greater period of time at their disposal, given the nature of criminal investigation, a significant imbalance is created by so little time being left to the defence prior to plea and, where appropriate, trial.

114. It was recognised across the focus groups that the imbalance is sufficient to hinder the defence's ability to adequately examine, analyse and effectively challenge the digital forensic evidence relied upon by the prosecution.

> "But that is a bit big thing with defence. So, when we get defence requests, they're always very, very short, so prosecution will have months to conduct an examination – defences. Defence is basically you've got access to the phone, we need it examined next week, we need the results the following day, and then it has to be presented at court'. You know, there's a big difference in time, which is allowed for prosecution and defence. There's always a lot of pressure on defence experts when doing defence examinations."
>
> Independent Digital Forensics Practitioner

[33] (Öcalan v. Turkey [GC], 2005, § 140; Foucher v. France, 1997, § 34; Bulut v. Austria, 1996; Faig Mammadov v. Azerbaijan, 2017, § 19). European Court of Human Rights, 'Guide on Article 6 of the European Convention on Human Rights', para 159 https://www.echr.coe.int/documents/d/echr/guide_art_6_criminal_eng

115. Given the importance of well-informed cross examination as the means to challenge admissible evidence it is necessary that this is conducted by digitally literate advocates with proper and equal access to the digital forensic evidence and where required, the expertise to analyse it, without unfair pressure of time.

> "…if you've got a case, the police and the prosecution will have had quite a lot of time to decide whether to charge. And then once it's charged, you've got – it's before the courts, that's when the defence really get hold of it – and especially if we're talking sex cases, the backlog now is so huge that they would not delay or counter any delay over victim giving evidence in court, because the defence require much more time to analyse something."
>
> Lawyer

116. Ensuring equality of arms concerning digital evidence may involve providing both the prosecution and the defence with access to the same digital forensic tools, experts, and resources. Certainly, the focus group participants acting for both the prosecution and the defence were open to procedures and practices that ensure both parties have reasonable and equitable opportunities to consider digital forensic evidence.

> "Now we have to speak to the defence quite a lot. So, a lot of the time it'll be if there's an issue raised about something that we've said was on a mobile phone extraction, the defence expert, whoever they've appointed to be a digital forensic investigator for them, they get in touch with us and we basically arrange how we're going to get the mobile phone extraction to the defence and that seems to work pretty well. A lot of it's just communication essentially."
>
> Digital Forensics Unit Investigator

117. These impacting issues, addressed in preceding sections of this report span resourcing, capacity, delay, organisational challenges, equality of arms, disclosure and ultimately the presentation and communication of evidence at court. Together they risk, in the view of the participants, creating a miscarriage of justice.

> "I think one of the biggest potential risks with that could be a miscarriage of justice where the evidence that's there is not presented in a way which gives the defendant or the victim best chance of representation."
>
> Lawyer

Recommendations

10. Bespoke training for police officers and Digital Forensic Unit practitioners on the criminal rules of evidence and procedure applicable to digital forensic evidence, specifically centred on matters of reliability, fact and opinion evidence and admissibility.

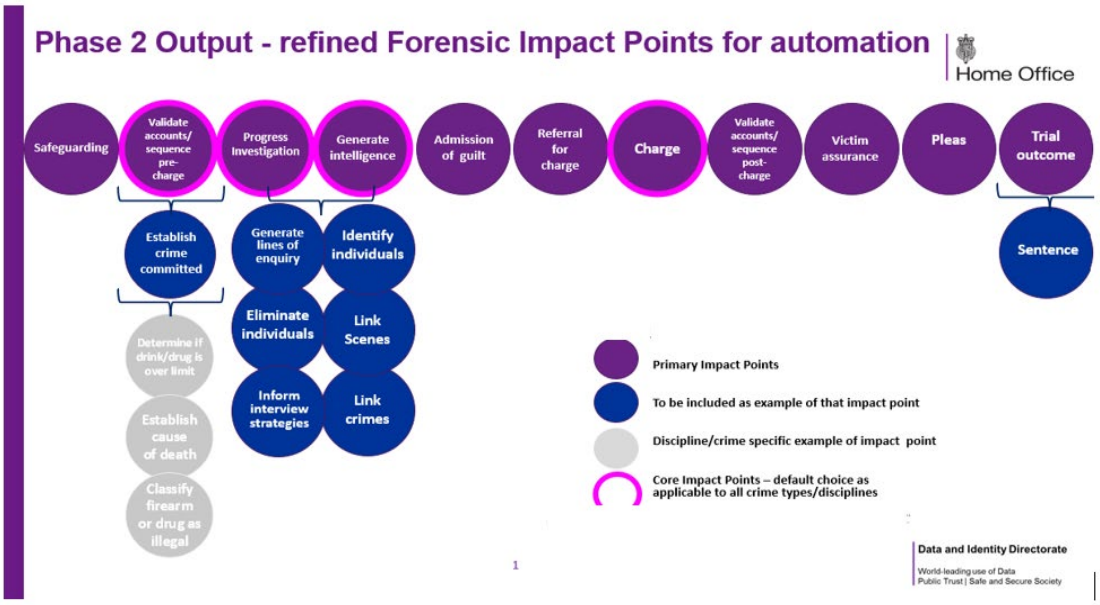
11. An urgent review of current practice in the admission and communication of digital forensic evidence in magistrates' courts to address non-compliance with the rules of evidence and the Criminal Procedure Rules.

Theme 4- The Home Office Forensic Impact Points Model

Measuring Impact

118. In January 2020, the Home Office initiated the Impact of Forensic Science Project with the aim of developing an approach to measure the impact (through effectiveness and timeliness) of any forensic discipline on any crime type.[34] The project developed a Forensic Impact Points tool and model, with the final output shown as an illustration of anticipated forensic points of impact.

Fig. 1 Phase 2 Output – refined Forensic Impact Points for automation[29]



119. The Impact of Forensic Science Project collaborated with both universities and police forces in the development and delivery of research projects which contributed to the design and testing of this tool and model. To date, these studies have been quantitative in nature, and have applied the Forensic Impact Points Model resource to specific offences including homicide[35] and child sexual exploitation.[36] Only two of the six Phase 1 projects have been published. The project has subsequently called for "a more detailed evidence base on the impacts delivered by forensic science which in turn will allow robust measurement of the value it delivers, or could deliver, to the criminal justice system on an ongoing basis."[37]

[34] The Impact of Forensic Science Project: Phase 1 Report, Marie Barrett, 2nd Aug 2022. The Phase 2 Output is within the report and also in Appendix 1.
https://assets.publishing.service.gov.uk/media/62e7dd71d3bf7f75bd257e12/Home_Office_Impact_of_Forensic_Science_Project_Phase_1_Report_for_publication_Accessible_Version.pdf
[35] Measuring the Impact of Forensic Science on Investigation: Methodological Details, Reflections and Recommendations. Jones and Brookman, 2021
[36] An observational study using the Impact Point approach to measure the utility of digital forensic science in online child exploitation cases. Jackson and Gwinnett, 2021
[37] The Impact of Forensic Science Project: Phase 1 Report, Marie Barrett, 2nd Aug 2022.

120. Northumbria University's project Digital forensics within the criminal justice system: Use, Effectiveness, and Impact (the Northumbria University Digital Forensics Project), responded to this call. The Northumbria University Digital Forensic Project tests and progresses the application of the above model using an approach that exclusively uses qualitative methodologies, drawing on the experiences of the full range of criminal justice professionals[38] in relation to all crime types involving digital forensics - from volume crime to serious and organised crime and counter terrorism.

121. This approach complements the previous quantitative research of the Impact of Forensic Science Project and associated research projects and further generated a rich dataset comprising valuable insights into the daily use and practices of digital forensics across the criminal justice system.

122. In summary, the data from the Northumbria University Digital Forensics Project identifies:

- the application and impact of digital forensics
- challenges and inefficiencies
- areas in which the allocation of greater resources would affect the greatest increase in impact
- barriers and risks in current practice that undermine the overall aims of the criminal justice system

The project thus, offers a valuable pathfinder approach for subsequent and more resource intensive qualitative and quantitative studies.

Response to the selection of Forensic Impact Points

123. The Forensic Impact Points visualisation was shown to participants in both the focus groups and pre-focus group interviews, to inform the discussion on the question which related directly to it. This was: *Where do you perceive digital forensics and digital evidence to have the greatest positive impact?*

124. Across the focus groups, interviews, and survey results, most participants agreed that all the identified Home Office Forensic Impact Points were significant moments of engagement for digital forensics. They also agreed that the points of impact identified were, largely, reflective of the turning points in most criminal investigations and prosecutions.

125. Lawyers took a holistic view of the criminal process, suggesting that all points of impact were of importance.

> "I could make a case for forensic evidence being absolutely critical in each and every one of those bullet points."
>
> Lawyer

[38] With the exception of the judiciary who it was felt would be less able to speak candidly about their experiences, and for whom the process of obtaining ethical approval and approval by the Master of the Rolls was deemed unachievable within the timeframes of this project.

"...forensic evidence...whether it's conspiracies to supply drugs or conspiracies to commit serious sexual offences...frauds, almost every form of offending now has each of those purple points significantly impacted by forensic evidence."

Lawyer

126. Policing participants were equally positive about the identified points of impact and in particular, agreed with the importance of the early core impact points (highlighted in pink on purple), namely validating accounts, progressing investigations, and generating intelligence.

127. There was not full consensus across participants as to which points of impact were most important - or that all were of equal importance, though broad consensus did exist on a number of impact points.

Key Forensic Impact Points

128. There was broad consensus, across all participants, that the earlier impact points, defined here as those to and including charge, were most influential on the basis that the earlier in the process quality digital forensics are provided the more impact it has.

129. In relation to each of the pre-charge impact points there was, perhaps not surprisingly, different views on which was the most significant or most significant to the participant's own role.

130. The first of the impact points, safeguarding, was stressed as a more significant opportunity for impact by some policing staff and those working within digital forensics, particularly digital forensics practitioners working within police forces.

"I've had dozens of cases where we found certain pieces of evidence where people were gonna be in immediate harm, we told the relevant officers and they were out of that harm within the next day or so...there can't be a greater positive than that, really, protecting people."

Independent Digital Forensics Practitioner

131. Police and digital forensic practitioners, particularly with reference to serious and organised crime, identified the 'Generate Intelligence' Impact Point as where, in their field, digital forensics had significant impact.

"…generating intelligence, linking suspects, I do a lot of work with serious and organised crime, and that's as big of a deal as everything else because it helps actually working out where the criminality lies."

Independent Digital Forensic Practitioner

132. Participants from the Crown Prosecution Service understandably stressed the importance of charging as a key point of impact. This is to be expected given the responsibility of the Crown Prosecution Service to make appropriate charging decisions based upon the available evidence.

133. However, while the point of charge was agreed by many participants to be a significant point in the life span of a case, it was considered to be a point at which digital forensics should already have had its greatest impact. In contrast to the first three core impact points (highlighted in pink on purple - validating accounts, progressing investigations, and generating intelligence), the charge was therefore considered less significant by many – including policing participants on the basis that by then they should be in possession of the digital forensics.

> "At that point you should already have everything you need."
>
> Police

> "…front loading of the resources is best."
>
> Police

134. This call for the early intervention of digital forensics to capitalise on impact was echoed across focus groups, and across professions within the criminal justice system, from investigation through to trial.

> "digital forensics ought to be central, even at a pre-charge stage, because they can contain fundamental evidence that if you haven't seen it, completely affect the charge decisions."
>
> Lawyer

> "…but if we can give them as much evidence as we can early on, then it means we can help to reduce the backlog. So that's certainly something that that I look for, if I'm looking at a case and setting an action plan for officers to see if we can get that evidence as early on as we possibly can."
>
> Lawyer

> "…having that content at the very beginning and either going into the first interview or the second interview with the individual and being able to present factual information of the device or CCTV footage or whatever the evidence is, does get rid of those not guilty, not out discussions or statements from individuals, which then pushes it to a trial."
>
> HM Prison and Probation Service

135. Generally, it was the barrister and solicitor participants and those digital forensics practitioners in independent practice who act, or also act, for the defence, who emphasised the significance of digital forensics at the point of plea and the point of trial. Indeed, a number of digital forensics practitioners in independent practice who act for the defence identified the role of strong digital forensic evidence as being pivotal at the point of plea, and in particular in guiding defendants and defence teams in their decision-making around plea.

136. Whilst participant perceptions of the Impact of Forensic Science Project's Forensic Impact Points visualisation were generally very positive, additional points were suggested, and the identified emphasis of the Core Impact Points (highlighted in pink on purple) was questioned by several participants.

137. A number of participants suggested either additions to the secondary blue circle 'examples' or that some were in fact Impact Points in their own right. The suggested addition was the 'disproving of alibis'. Participants felt the disproving of alibis played an essential role in influencing early admissions of guilt.

138. The blue circle examples considered to be Impact Points in their own right were the Linking Crimes and Excluding Individuals early in the process. The absence of early identification of exculpatory intelligence was considered to result in an overlooked positive consequence, the reduction in the use of intrusive investigative methods later in an investigation either against a suspect later found to be innocent, or third parties. This is of heightened significance given recent public concerns around perceived intrusive investigatory measures undertaken around sexual offences, and the perceived impact upon victims.

139. Many participants felt the time in the life of a case most under-represented by the Impact Points visualisation was between plea and trial. This is an exceptionally busy, and time pressured time for defence lawyers and defence digital forensics practitioners.

> "I basically live in a missing gap between pleas and trial outcome."
>
> Independent Digital Forensics Expert

140. The most discussed pre-trial and trial process missed from the Forensic Impact Points is disclosure. Disclosure was raised in every focus group, by all participant disciplines, including those working for the prosecution and the defence. Digital forensics was agreed to be inherently linked to challenges with disclosure. One digital forensics practitioner defined the challenge in the following way.

> "How do you sift large volumes of data and what are your disclosure requirements and how do you use that usefully within an investigation or an evaluation?"
>
> Independent Digital Forensics Expert

141. It was suggested multiple times that Disclosure should be included as a new Impact Point, though exactly where in the timeline disclosure should appear was contested. This is understandable given that there are both pre-charge and post-charge disclosure obligations.

142. Some participants of the focus groups raised the perspective that the Impact Points do not cater for the innocent accused after the point of charge. Some participants expressed the view that on the current approach the Impact Points visualisation assumes guilt to the point of disposal, essentially assuming a guilty verdict.

143. In the same vein, and as further evidence of an inculpatory bias, participants identified the significant absence of appeal as an impact point. Like any other evidence type, digital forensics can contribute to miscarriages of justice. The converse is also true in that it may be that digital evidence, not available or identified at trial, demonstrates that a conviction is unsafe.

> 'What if the person… is actually innocent? …where's the digital evidence for analysing what the family was going to be raising proving their innocence if that's the case? … in my view, there's another potential split, just after charge."
>
> Independent Digital Forensics Expert

144. Overall, the view of numerous participants was that there are two additional impact points which are of such significance that they ought to appear in the Forensic Impact Points. They are Disclosure and Appeal.

Quantifying and Evidencing Impact

145. The purpose of the Home Office Impact of Forensic Science Project is to develop an approach to measure the impact of forensic science (through effectiveness and timeliness) of any forensic discipline on any crime type. With this objective in mind, the research participants were asked to consider how the impact of digital forensics might be measured, and also why this is a useful endeavour. This discussion naturally incorporated consideration of the challenges of measuring digital forensics, and how such measurement might be carried out in the future.

146. All participants generally saw the value of evidencing the impact of digital forensic evidence, particularly where this leads to better resource allocation and improving digital forensics expertise. This need to better understand, identify, and measure the impact of digital forensics was considered especially timely given the increased volume and complexity of digital forensic material.

147. Following on from identifying what constitutes 'impact', is the identification of links in that chain to impact; identifying the successful link is very difficult in respect of the role of digital forensics.

> "If it [digital forensic material] is that intrinsic to every investigation, we're saying it is and we're saying it's not getting any easier and it's getting bigger and bigger – what better way is there to say this is the most important thing going?"
>
> Police

148. The value of thorough research into this measuring endeavour was widely acknowledged. Academic involvement was highlighted as being extremely valuable.

> "Having some investment in there and some academic research into it, certainly with the Soteria Bluestone stuff has definitely paid dividends, so for me it would be widening that net."
>
> Police

149. The most significant barrier to measuring success of the use of digital forensics is the lack of reporting and communication of such impact and the lack of coordination and cooperation between each of the organisations within the criminal justice system.

150. Digital forensic practitioners, located within police forces, in particular conveyed widespread poor reporting of outcomes in investigations and prosecutions and stated that their ability to measure impact is extremely difficult if that outcome is not fed back to those involved earlier in the investigation.

151. This poor communication of outcomes applies both upstream and downstream, with some participants in digital forensic leadership roles stressing how articulating digital forensic impact to non-experts can be difficult, and often digital forensic staff themselves fail to do so. This contributes to a landscape where digital forensics practitioners do not fully explain the positive impact of their processes to those further down the investigatory line, and those involved in later investigation stages fail to report back to digital forensic staff on the impact of their efforts.

152. Resulting from the poor reporting of investigation outcomes is the absence of data. The actual significance of certain types of evidence is not recorded or reported. This is true across the criminal justice system.

153. Another challenge to measuring impact is the need to identify what constitutes a 'successful' use of digital forensics. One focus group took the view that measuring 'successful impact' in digital forensics is a unique challenge. In an area which is moving and changing as quickly as digital technology, more than one participant made the point that success for digital forensic practice could be defined as not going backwards; purely keeping up with the pace of change can be seen to be a success.

154. Across the focus groups, it was agreed that quantification, or even identification of impact can be difficult. One fundamental reason for such difficulty was stated as being the challenge in separating a successful investigation from a successful digital forensics process during that investigation.

"Often you'll see a very, very terrible case that has a good outcome and the person thinks that they're doing a great job and give feedback that yes, digital forensics really helped...on the other side of the coin, you have a very difficult case where digital forensics, they've done everything right, but they haven't quite got the answer that the person at the end wanted, and they'll say... digital forensics has been terrible"

Independent Digital Forensics Practitioner

155. Many research participants, particularly those working within the police and the Crown Prosecution Service, identified a successful investigation outcome as being a conviction. This approach was not accepted across the breadth of research participants. A concern with measuring impactful digital forensics with conviction was identified as being an onus on conviction over everything else. Overly focusing upon convictions as a success metric could result in future miscarriages of justice, as the focus shifts to conviction rather than safe conviction. A further concern raised regarding measuring success by conviction is the oversight of the extra-judicial value of digital forensics such as intelligence gathering or ascertaining no crime has been committed.

156. This failure to identify the role of digital forensics earlier in an investigation was reiterated by other participants who lamented the lack of recognition of digital forensics and police who put successful cases together and then who lose control of that case when it is passed to the Crown Prosecution Service. This lack of recognition of the role of digital forensics in an investigation is compounded where digital forensics are not the only type of evidence, which is mostly the case. Therefore, where digital forensics contributes to an investigation, measuring this is even more challenging.

"In digital forensics, I think it's very hard to recognise the person who's at the top of the chain, because the evidence is so removed at the bottom, they get the extract, it's the investigator's skill who then gets the evidence which gets the win because it's the result at the end of it all."

Police

157. Amongst research participants, it was largely accepted that where the purpose of measurement is to inform investment, performance indicators and quantitative metrics are often relied upon. However, identifying the right performance indicators is imperative.

"if you get the wrong performance indicators, it will destroy performance…there's a massive hazard with this"

Independent Digital Forensics Practitioner

158. This is not to say that performance indicators were not valued by participants, but such indicators can be very powerful and have the potential to set policies which may

not be effective. There was strong feeling across participants that some metrics for measurement were 'dangerous' and misleading, such as the number of devices analysed.

> "PowerPoint, super-duper…snazzy graphs' do not show the impact of digital forensic handling, often it just shows the number of exhibits, or the time taken to process and this can be extremely reductive and misleading"
>
> Police

> "…we fall into a trap of thinking this is easy. So you go, 'you know what, we'll just get some KPIs, what's the things you can measure – exhibits in the blue box in the corner? Right, that's the thing, there you go'. That shows how busy the forensics lab is, and we've managed to land this many prosecutions. Actually, that really isn't great."
>
> Police

159. The potential value of measurements around statistics such as the number of devices seized and analysed was recognised, though not without some caveats.

> "… those statistics of how many devices are attributed cases, how many devices are seized each year, what capability does each police force have to examine those devices, and then looking at the actual figures and seeing that there are way more devices seized than what there is the capability to examine those devices, and that key areas of investment could increase that."
>
> Independent Digital Forensics Expert

160. A significant barrier to national impact measurement is that each police force is different and a one-size-fits-all approach to anything, including measurement, is problematic. It is difficult to compare or standardise across forces, partly because of varying budgets, but also due to different priorities, cultures, and practices.

161. The additional consequence of the failure to track or measure digital forensics impact, is the inability to identify and measure when digital forensic practice goes wrong. Many participants agreed that digital forensics failures are rarely, if ever, spotted. This is equally problematic as it undermines the learning process of how individuals, organisations, and systems can be improved.

162. Whilst all focus groups saw a great deal of discussion around the challenges to measuring the impact of digital forensics, examples from different organisations and different types of stakeholders were identified.

163. For example, whilst the Crown Prosecution Service does not review successful prosecutions, it conducts reviews into 'failed' prosecutions. There is a coded approach to recording whether, for example, a prosecution was discontinued based on digital forensic evidence. Whilst the capturing of data was welcomed by

participants generally, concerns were expressed in how precisely the approach properly reflected the specific issues in the multitude of types of cases it may relate to.

164. Overall participants took the view that data captured by the Crown Prosecution Service should be improved and extended to allow for the positive impact of digital forensics evidence to be evidenced and evaluated.

165. A review of current data, on failed prosecutions involving digital forensics, should be considered to identify any specific or systemic issues underpinning those failures.

166. Whilst an over-reliance upon key performance indicators to measure success or failure was criticised by many participants, some participants, particularly those in management roles, raised the value of performance indicators as measurements of progress both internally for organisations, and externally as comparators with other organisations. In one instance, performance indicators were raised as being useful for comparators outside of 'silos'.

167. More than one participant expressed the view that lessons could be learned from the private sector around the effective use of cost-benefit analysis.

> “From a police perspective, ... they have no idea what it costs to conduct an examination, and they have no idea of how long it takes to conduct an examination, because every single one is different – and they are different, but on average you can calculate it. And it's these figures that could really help to guide where the investment is needed and to improve the forensic service."
>
> Independent digital forensics practitioner

168. In response to the challenge of identifying the impact of digital forensics in investigations, participants from national and regional policing agencies referred to existing attempts to 'stain' digital forensic evidence in order to trace its success (or otherwise) through the life of an investigation or prosecution. This is particularly useful where intelligence from one operation leads to a separate investigation or investigations.

169. This would require going back to first principles to measure what was described as a very difficult thing. These first principles might be as simple as a version of a chain of evidence handling. This sentiment of measuring the impact of digital forensic input from the beginning of the process, from seizure, was echoed across focus groups.

Reflections

170. There was widespread agreement amongst the groups that gaining insight and perceptions from those working on the ground in digital forensics and investigations is essential to understanding what 'works'.

"Nothing replaces a kind of verbal conversation where people can really give good feedback".

Police

171. The value of further qualitative research of the kind undertaken in the Northumbria Digital Forensics Project was also widely suggested by participants, many of whom expressed the view that they had not previously had the opportunity to collaborate across so many relevant disciplines.

172. In keeping with the trust in the project team, and the desire to work with others across the criminal justice system, the participants who signed up to the project expressed their enthusiasm for being involved at every stage of the research. This enthusiasm was largely driven by a recognition of the need to address the increasing challenges of digital forensic use. Additionally, the opportunity to discuss professional experiences in this area directly with stakeholders proved extremely appealing to all participants.

"Having some insight on this [perceptions of the use and challenges of digital forensics] from further along the judicial system than just the police, I would say [is most valuable], so CPS, barristers, judges [it] would be quite interesting to see what their perception of it is when it's presented to a court as well, and what bits sit with them and what bits are potentially missing."

Police

173. Conferences are often seen as the main fora within which to share knowledge, but again these are often discipline specific. This research project's focus groups were multi-disciplinary which proved to be extremely effective in facilitating discussion of experience and good practice. In every focus group, there were examples of knowledge sharing and cooperation which was taken forward outside of this project. There was therefore a direct professional benefit to the participants. This benefit was more immediate than the opportunity to influence policy going forward and for many participants, their investment of time in this project paid off.

174. Specific suggested methods for future research into digital forensics included:
- quantitative studies involving dip sampling of cases which would reveal the prevalence of digital forensics
- a review of 'failed' prosecution data held by the Crown Prosecution Service
- consideration of a sample of investigations and prosecutions in the context of their progress had they not had the benefit of digital forensics, i.e. negatively identifying the success by considering the investigation without the digital forensic evidence.

175. The consideration of the Forensic Impact Points model, in the context of the broad focus groups, discussions, generated a number of useful findings in relation to the usefulness of the model as a framework for measuring impact and potential improvements to its structure to better represent all significant impact points.

176. The Northumbria University Digital Forensics Project did not seek to quantitatively measure where the most impact occurred in a specific crime type but where the experiences of the users of the criminal justice system told us the allocation of greater resources would affect the greatest change. The universal, broad answer from investigators to lawyers via digital experts was early.

177. The participant contributions firmly made the case that quality digital forensics has its greatest impact when frontloaded – that is digital forensics done properly and in a timely manner. The greatest impacts are in relation to safeguarding, validation of accounts, advancing investigations, linking scenes and crimes, exonerating suspects, generating early admissions of guilt, leading to appropriate charge and generating appropriate guilty pleas.

178. There are obvious significant resource implications in 'frontloading' the provision of digital forensics, particularly in terms of the investment in Digital Forensic Units but the focus group participants took the view that this would generate efficiencies by shortening otherwise unnecessarily long investigations and prosecutions.

179. Alongside the substantive findings arising from this project, the research team noted the real enthusiasm from all participants to be involved in cross-disciplinary discussions, the level of agreement on key challenges and the determination to find realistic and workable solutions to increase the positive impact of digital forensics across the criminal justice system.

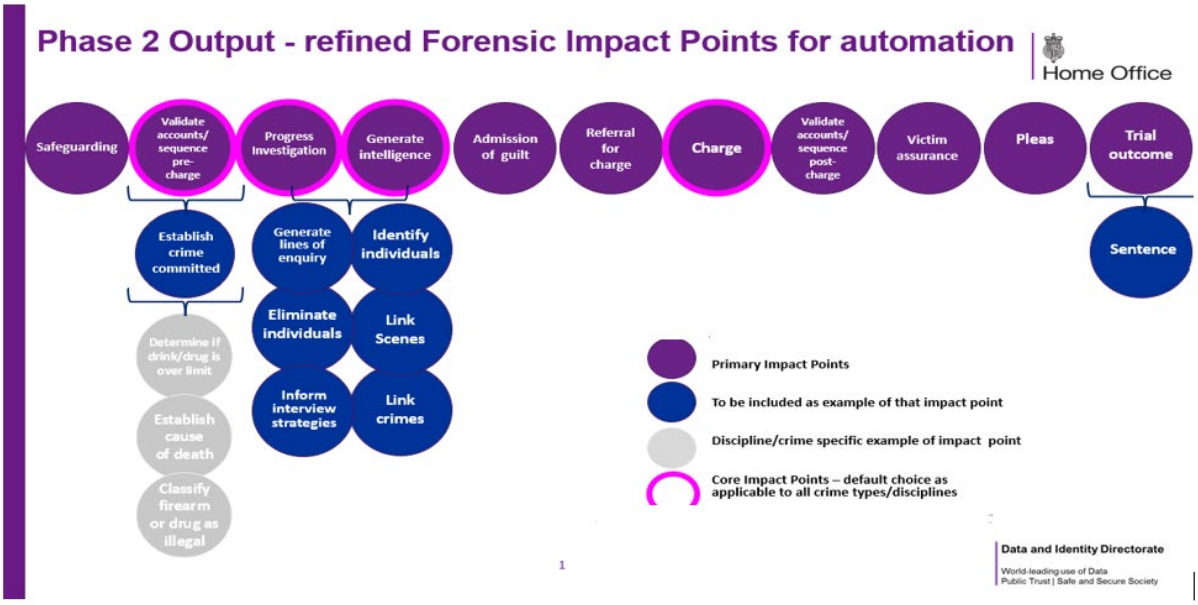
Recommendations

12. The Home Office to add two further Forensic Impact Points to the current model:
    - Disclosure
    - Appeal

13. Given the findings of the Northumbria University Digital Forensics Project, apply the Forensic Impact Points model in a manner that does not seek to quantify impact at each individual impact point but to learn where future policy and investment could generate the greatest impact through the removal of existing barriers and constraints.

14. Undertake a review of the cases identified within Crown Prosecution Service's 'failed prosecutions' data, to identify the key barriers to the effective and impactful use of digital forensics.

Appendix 1- The Forensic Impact Points Model



Appendix 2- Methodology

Mixed Methods Approach

To achieve the objectives of the project, a range of traditional qualitative methods were employed. These included research-design interviews with a range of participants, four mixed-participant focus groups, a focus group follow-up survey, and additional post-focus group email correspondence.

These methods were employed across the life of the project, from project design to data collection and analysis. *Johnson et al* have stressed the value of interactive events as a more fruitful scoping exercise over individual interviews.[39] We decided to harness both interactive events and interviews, largely because the types of participants we wanted to recruit did not have readily accessible national events and we would have to either host or be invited to a large number of conferences, often reserved for members of that body. Instead, we harnessed pre-existing access to externally organised events, and supplemented these with individual interviews across the range of research participants to ensure we captured voices from a wide range of organisations and roles.

Research Design

From its initiation, the project was designed with stakeholder involvement to ensure the most effective methods for capturing stakeholder perceptions of digital forensic use. The project's main design stakeholder was the Home Office, specifically the project lead for the Home Office's, *Impact of Forensic Science Project*.

The concept for the project was also presented to a barristers' chambers Fraud Forum, attended by approximately 40 barristers and solicitors from across the Northwest of England. Both our Home Office contributor, and the forum audience provided essential feedback on such research design questions as methods of data collection (for example, mixed focus groups rather than groups siloed into profession), participant recruitment and involvement, the breadth of the topics to be explored, and the types of research questions. The research questions to be put to focus groups was an essential part of the co-curation of the project.

Given the breadth of participant experience, and the desire for minimal interjection by research staff in the focus group session, the project team were conscious to design research questions which would allow for discussion between participants, and not reinforce professional silos or create cross-purposes in the interpretation of questions.

To create suitably open but targeted questions, feedback on the questions within the focus groups was obtained in advance via interviews with participants from a range of professional backgrounds.

These interviews were designed to 'trial-run' the questions, and in consequence, some of the language in the questions was clarified. This trialling of the focus group questions aligns with the recent broader academic move towards co-curation of research. Research across

[39] Johnson D et al, 'Police Functional Adaptation to the Digital or Post Digital Age: Discussions with Cybercrime Experts' *Journal of Criminal Law*, Vol. 84(5) 427–450, 2020, p428, https://doi.org/10.1177/0022018320955255.

several disciplines is increasingly recognising the value of focus groups that are co-designed and co-curated by participants, particularly those affected by the subjects discussed.[40]

A concern raised within other disciplines around co-curation of focus groups is the over-reliance on participant input which may lead to a blurring of prioritisation for a study, with a danger that its original aims will become so changed that previous work structuring the focus groups could be wasted either wholly or in part[41] with the project's original aims needing to be balanced with seeking, respecting, and responding to participant views. This concern did not manifest itself in the Northumbria Digital Forensics Project, largely because of the research team's prior professional experience which prevented a chasm between an academic preconception of the most fruitful topics for discussion, and that of the participants' daily experience. Consequently, the feedback from research design participants was largely very positive, and suggested changes were confined to wording rather than substance.

As well as asking for participant feedback on focus group questions, the Northumbria research team also gathered feedback on the practicalities of running the groups. These questions related to the online nature of the focus groups, the running time, and the potential for conflict or over-agreement between participants. These topics are discussed in detail below.

The Research Team

In line with the spirit of breaking down professional silos, the Northumbria project team also moved outside of disciplinary silos. Harnessing the academic expertise of team members from the disciplines of law, applied science, digital forensics and public administration, the team consciously designed methods of data gathering and analysis which would allow for cross-disciplinary thinking. The research team are all academics with extensive previous professional experience: two barristers, a forensic scientist, a digital forensics practitioner, and a former senior civil servant. Uniting such professional experience allowed for more practice-based thinking to infiltrate the project design and analysis. Involving team members with varied pre-academic professional experience allowed for the grounding of the research in the reality of criminal investigations and trials.[42] It also allowed for multiple, extensive professional networks to be utilised to ensure participation from the full breadth of criminal justice stakeholders.

The Use of Focus Groups

The extant literature around digital forensics often relies upon surveys, a well-tested method to garner data from a larger number of participants, particularly from professional participants with limited time resource.[43] Given the project's aim to explore experiences

[40] Yeates L., Gardner K., Do J. et al, 'Using codesign focus groups to develop an online community supporting families after Sudden Cardiac Death (COPE-SCD) in the young', British Medical Journal (2022), https://doi.org/10.1136/bmjopen-2021-053785

[41] Slattery, P., Saeri, A.K., & Bragge, P., 'Research co-design in health: a rapid overview of review', *Health Research Policy and Systems* 18:17 (2020), https://doi.org/10.1186/s12961-020-0528-9.

[42] Johnson et al, Police Functional Adaptation.

[43] Wilson-Kovacs et al, Digital evidence in defence practice: Prevalence, challenges and expertise, *The International Journal of Evidence & Proof* 2023, Vol. 27(3) 235–253Hans Henseler, Hans and van Loenhout, 'Educating judges, prosecutors and lawyers in the use of digital forensic experts', *Digital Investigation*, 2018, s76-s82', https://doi.org/10.1177/13657127231171620.

across a system, the way stakeholders perceive the role of digital forensics, and the ways in which stakeholders interact with one another and the wider system, focus groups were identified as more appropriate than individual interviews or surveys.

Focus groups are a well-established method of research across multiple disciplines, and there is extensive research into the potential for, and challenges of focus groups which need not be repeated at length here.[44] One particular facet of focus groups which was ideally suited to the aims of the project was the potential for discussion between participants which is discussed in more detail below.

The Focus Groups: Recruitment, Facilitation, and Knowledge Exchange

Participants

Participants included representatives from four police forces from across England, other law enforcement agencies concerned with serious and organised crime and counter terrorism, police digital forensics practitioners, HM Prison and Probation Service, the Crown Prosecution Service, independent digital forensics experts, defence solicitors and barristers with experience of both prosecution and defence practices.

Participant Recruitment and Involvement

Our recruitment process was multifaceted. and harnessed the pre-existing networks of the research team and the Home Office.

The project initially attracted policing and digital forensics participants but did not attract lawyers. Members of the legal profession were initially contacted through social media and a presentation by the research team to a large legal professional event in the Northwest of England. Feedback at this event was extremely positive about the need for the project, as all agreed that digital forensics were being deployed in challenging ways across the justice system. However, there was reluctance by solicitors and barristers at this event to invest time and resources in a civil service project which many saw as being in a long line of government consultations following which the voice of the legal profession was seen to be ignored. This perception proved difficult for the team to overcome but by utilising pre-existing professional networks of the research team, combined with the opportunity to converse on key issues with practitioners in other relevant fields, solicitors and barristers were recruited as participants to the project.

The participants who signed up to the project expressed their enthusiasm for being involved at every stage of the research. This enthusiasm was largely driven by a recognition of the need to address the increasing challenges of digital forensic use. Additionally, the opportunity to discuss professional experiences in this area directly with stakeholders from across the justice system proved extremely appealing to all participants.

[44] Cresswell, J.W and Plano Clark, V.L., *Designing and Conducting Mixed Methods Research* (Sage, 2018), 46*;* Cyr, J. 'The Unique Utility of Focus Groups for Mixed-Methods Research', *Political Science & Politics*, 50:4 (2017), 1038-42. https://doi.org/doi:10.1017/S104909651700124X

Conferences are often seen as the main fora within which to share knowledge,[45] but the project's focus groups were extremely effective in facilitating discussion of experience and good practice. There was a direct professional benefit to the participants. This benefit was more immediate than the opportunity to influence policy going forward and for many participants, their resource investment paid off. In every focus group, we saw examples of knowledge sharing and cooperation which was taken forward outside of the research itself.

Bringing together participants from across traditionally 'closed' groups such as the police, intelligence services, public and private digital forensics experts, and defence and prosecution teams raised the risk of non-cooperation or participants feeling uncomfortable with engaging in frank and open discussion. Because of this concern, research design of the project was particularly alert to the important of encouraging and facilitating discussion within the focus groups. These concerns proved unfounded. Again, the enthusiastic participation in focus groups was likely due to the topic itself as it would seem struggles with the shift in digital forensics and material is a universal experience across the criminal justice system.

Online Forum

The project's research design stage indicated that online rather than in-person forums would encourage a broader range of participants. Given the breadth of professional stakeholders, their geographical location, and the demands on professional time, online rather than in-person focus groups would ensure more involvement. Pre-focus group interviews indicated that most participants could only attend online and only for short sessions. Expecting police officers, lawyers, and digital forensics experts to dedicate at least a day to a research focus group is unrealistic. A large reason for the success of our participant attendance was down to the online nature of the focus groups which only caused minimal disruption to the working day.

We were aware of the need for balanced participant involvement in online focus groups. Participant engagement has been identified as an issue with online groups in particular,[46] although recent studies suggest that increasing normalisation of online meetings serves to mitigate this effect.[47] We sought to mitigate under-involvement by participants through the research design stage in the careful crafting of open questions which might elicit broader involvement. Involvement of all focus group participants was also maximised through the regulation of focus group numbers[48] with groups of no more than 8 being held. There was also much consideration of strategic facilitation and intervention by focus group moderators; how much to encourage involvement of quieter participants, and when to curb dominant participants or limit less relevant discussion.

A further benefit of online focus groups was the live generation of transcripts for later proofreading, and the ability to record video footage of participants. A contrasting benefit was the preservation of the identity of some of our participants working in serious and

[45] Casey, Eoghan (2019) The chequered past and risky future of digital forensics, *Australian Journal of Forensic Sciences*, 51:6, 649-664
[46] Lobe, Morgan, and Hoffman, 'Qualitative Data Collection in an Era of Social Distancing', *International Journal of Qualitative Methods*, 19. (2020), https://doi.org/10.1080/00450618.2018.1554090.
[47] Halliday M, Mill D, Johnson J, Lee K. Let's talk virtual! Online focus group facilitation for the modern researcher. *Res Social Adm Pharm.* 2021 Dec;17(12):2145-2150, https://doi.org/10.1177/1609406920937875.
[48] Krueger, Richard A and Casey, Mary Anne, *Focus Groups. A Practical Guide for Applied Research. (5th edition,* Sage, 2015). https://doi.org/10.1016/j.sapharm.2021.02.003

organised crime and counterterrorism who could fully participate in the online focus groups, without their identities being revealed.

Focus groups generate different challenges around confidentiality and anonymity from other forms of data collection such as interviewing. Given that discussion is undertaken in groups, participants' anonymity in any publications must be emphasised to ensure participants are forthcoming in that discussion. Protecting the anonymity of participants can be difficult when bringing together professionals from across the criminal justice spectrum; anonymity within the research team can be assured, but this cannot truly be said regarding revelation of identity, involvement, or the nature of contribution by other participants. However, for participants working in sensitive or secret roles, cameras could be, and were, turned off.

Focus Groups: Questions and Materials

The focus groups were designed to last for two hours and asked participants to speak to the following questions:

1) In your role, what comes within the term 'digital forensics' or 'digital evidence'?

2) Where do you perceive digital forensics and digital evidence to have the greatest positive impact?

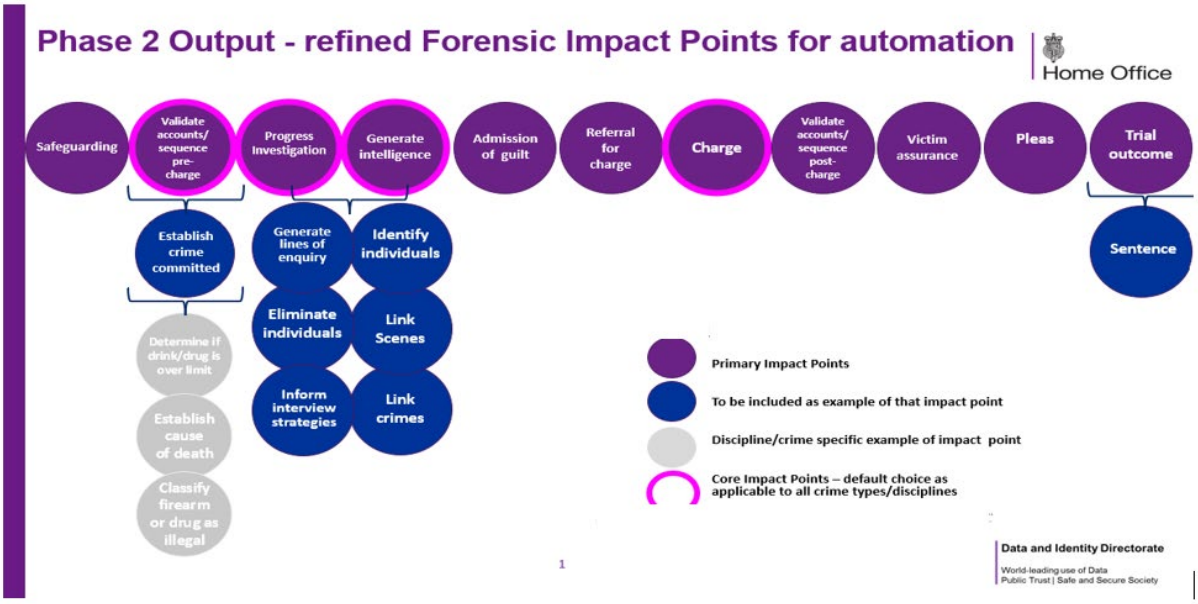
3) How cohesive is the approach to digital forensics across the criminal justice system?

4) What are the barriers to effective use of digital forensics and evidence, and the consequences of these barriers?

5) What would an ideal system of digital forensics and evidence look like for you?

6) How can the impact of digital forensics and evidence be better evidenced and measured to inform investment decisions?

Participants were given no additional visual prompts or information other than when answering question 2, relating to impact points. When introducing question 2, the focus group facilitator shared the following image of the Home Office, Forensic Impact Points.



Follow-up surveys to provide supporting information

Though the project had 'trialled' the focus groups questions using pre-focus group interviews, we predicted that unexpected conversations would arise during the focus groups. This is to be expected, and hoped for, in such a study with multiple participants speaking to such a contentious and current topic.

Given the natural time-constraints of focus groups, we anticipated that not all lines of discussion would be completed within the sessions themselves. Consequently, the data collected through the focus groups was complimented by an open-question survey, sent to participants immediately following the groups, when the conversation was still fresh in their minds. The survey was also designed to allow engagement with unexpected discussions arising within the focus groups.[49]

This survey was deliberately broad and non-leading, and other than asking for details of participant roles, the only 'question' asked was 'Please detail any issues raised in the focus group to which, in hindsight, you would like to add."

As well as the surveys, we also encouraged participants to email the project team with any further thoughts, and this resulted in follow-up interviews with several participants. Again, this reflected how enthusiastic participants were to contribute to the project due to the importance of the topic.

[49]De Vaus, D., & de Vaus, D. *Surveys In Social Research* (6th ed, Routledge, 2013); Rea, L.M and Parker, R.A, *Designing and Conducting Survey Research: A Comprehensive Guide*, (4th Edition, San Francisco 2014) 71-90.