Faculty of Engineering

Digital Forensic Triage Project
Launch Event Report

Dr Catherine O'Brien, Dr Valeria Abreu Minero, Dr Mark Warner, Dr Maria Maclennan, Professor Sarah Morris, Professor Niamh Nic Daéid, and Dr Oriola Sallavaci

Executive Summary

On 27 March 2024, UCL hosted a launch event for the ESRC funded project *'Towards A Smart Digital Forensic Advisor To Support First Responders With At-Scene Triage Of Digital Evidence Across Crime Types'*. Led by Dr Mark Warner at UCL in collaboration with Prof. Niamh Nic Daéid (University of Dundee), Prof. Sarah Morris (University of Southampton), Dr Oriola Sallavaci (University of Essex), Dr Maria Maclennan (University of Edinburgh), and Dr Valeria Abreu Minero and Dr Catherine O'Brien (UCL), the project focuses on non-technical triage of digital evidence at crimes scenes. It aims to work towards the development of a Smart Digital Forensic Advisor (SDFA) to support first responders with at-scene triage. It will explore existing practices, resources, challenges, and identify user needs around the search and seizure of digital evidence in homicide and stalking and harassment investigations across police operating models. The event brought together experts from forensic regulation, forensic science, policing, government, private sector, and academia. The event was an opportunity for the project team to engage across diverse stakeholders, to understand their views of triage, and the challenges they see as being important to consider during the project. The main challenges identified were:

- Defining digital device 'triage' is problematic, as it is not a common term used within forensic science and has different meanings to people across policing and forensic science roles.
- Triaging requires knowledge and skills, and there is a lack of alignment in existing practice across different levels in policing organisations, coupled with a reliance on technological solutions.
- There are challenges related to a risk averse culture, underpinning decision-making and resulting in a 'seize all' mentality.
- Measuring the value of digital devices within the context of an investigation to support triaging is challenging due to lack of data and methods.

The event was held in partnership with another ESRC funded project *'Trust in forensic science evidence in the criminal justice system: The experience of marginalised groups',* led by Prof. Lara Frumkin at the Open University. Running the event in partnership allowed both projects to identify themes and challenges that overlapped. Some of the overlapping themes identified were:

- The risks of collateral intrusion in digital forensics, and its potential to undermine public trust in policing.
- The challenges of defining and communicating terminology used in forensic science.
- The need to embed transparency in digital forensic processes with the aim of increasing understanding and trust in forensics more broadly.
- The increasing prevalence of digital devices in crime requires specialist knowledge to support decision making, but its impact and application relies on trust and credibility.

Please cite this report as: O'Brien, C., Abreu Minero, V., Warner, M., Maclennan, M., Morris, S., Nic Daéid, N., and Sallavaci, O. Digital Forensic Triage Project Launch Event Report (2024).

Economic and Social Research Council

Summary of Themes

Definition of Triage

- The term 'triage' is not a common term in forensic science and has therefore been used and understood inconsistently.
- Digital device triage may occur at different investigative stages.
- There are challenges around measuring the perceived value of digital devices within the context of an investigation.
- Triaging processes should be considered within the context of the entire system of processes and activities involved in digital forensics.

Skills and Training

- There is a lack of alignment in existing practices, skill, knowledge levels, and training across policing organisations.
- While training exists, there is low uptake, which contributes to the disparity in skill and knowledge levels both within and across policing organisations.
- As police officers are using technologies to generate data from devices, there is a need to understand individual competence levels and the appropriateness, accessibility, and usability of existing tools and resources.
- There is a need to balance technical skills with an investigative mindset.

Culture

- Risk aversion across policing, often driven by a fear of missing potential valuable evidence, has resulted in a pervading 'seize all' mentality amongst officers.
- Gaps in knowledge combined with an overemphasis on technological solutions contributes to delayed and offset decision-making.
- Specialist knowledge is increasingly needed to inform decision-making, but its impact and application relies on trust and credibility.

Collateral Intrusion

- Collateral intrusion can impact on public trust in policing and forensic science.
- Today's digital devices are integral to personhood and offer private and intimate insights into peoples' lives.
- There are concerns amongst stakeholders about the disruption caused to victims by device seizure, including the risks of intrusion on irrelevant and personal information during examination and review.
- Triage should reduce the risks of collateral intrusion, which may impact how triage is understood, and trust in digital forensics more broadly.

Project Future

- Triage must be defined clearly to understand what the SDFA can contribute.
- We should go beyond tools, technologies, and processes, and attend to people, resources, and time.
- The project should not make an isolated contribution, and ongoing support and collaboration from the project would be required by stakeholders.

UKRI Economic and Social Research Council

Definition of Triage

- The term ‘triage’ is not a common term in forensic science and has therefore been used and understood inconsistently.
- Digital device triage may occur at different investigative stages.
- There are challenges around measuring the perceived value of digital devices within the context of an investigation.
- Triaging processes should be considered within the context of the entire system of processes and activities involved in digital forensics.

A major theme that emerged during the event related to the meaning and utility of the term ‘triage’, and the challenges surrounding its inconsistent use. Discussions revealed that triage is not a commonly used term in forensic science, and there is discrepancy in its use across forces and organisations, as well as at an individual level. There was constructive debate between stakeholders around when triage as a process could occur, for example, whether it could happen during planning and strategy development prior to seizure, at the crime-scene, or during examination post search and seizure.

Importantly, the question was raised as to whether triage as a term becomes meaningless because of its inconsistent use. Throughout these discussions, what was emphasised was the need to understand triage as part of a whole system of different processes and activities. Stakeholder discussions surrounding the definition, measures, and utility of triage were illuminating for our project, and are something that we will remain mindful of as we continue with our research.

Challenges were also highlighted around measuring the evidential and non-evidential value of digital devices and data within the context of an investigation to support digital device triaging processes. Such challenges included the need to consider the context and significance of individual devices, the differences between search and examination objectives, and the validity of the extraction and analysis of data during triage.

Skills and Training

- There is a lack of alignment in existing practices, skill, knowledge levels, and training across policing organisations.
- While training exists, there is low uptake, which contributes to the disparity in skill and knowledge levels both within and across policing organisations.
- As police officers are using technologies to generate data from devices, there is a need to understand individual competence levels and the appropriateness, accessibility, and usability of existing tools and resources.
- There is a need to balance technical skills with an investigative mindset.

There is a lack of alignment in existing practices, which includes both investigative and technical processes, in respect to skill, knowledge levels, and training across all policing organisations. Despite training in digital evidence being available, stakeholders reported that there is often low uptake which contributes to the disparity in skill and knowledge levels both within and across police organisations. Stakeholders highlighted how this largely emerges from the time pressures frontline officers face, making it difficult for them to find the time to undertake additional training or even fully engage with the mandatory training opportunities they are provided with. From this perspective, stakeholders questioned how we might ensure officers are receiving this information more effectively. One suggestion was whether new courses should be developed, but it was acknowledged that this raises additional challenges, such as whether they would need to be nationally mandated, who would take responsibility for maintaining and operating the courses, and how they would be funded.

Importantly, it was noted that a lack of training for frontline officers can result in:

- The destruction of evidence through improper handling and seizure.
- A ‘seize all’ mentality among frontline officers, which we will discuss in the following section.

It was emphasised that officers are using technologies to generate data from devices, which means we need to attend to their competence and the accessibility of these tools and resources. Furthermore, it was also discussed how emphasis needed to be placed on developing an investigative mindset, rather than relying on tools and technology to reveal and triage evidence.

Culture

- Risk aversion across policing, often driven by a fear of missing potential valuable evidence, has resulted in a pervading ‘seize all’ mentality amongst officers.
- Gaps in knowledge combined with an overemphasis on technological solutions contribute to delayed and offset decision-making.
- Specialist knowledge is increasingly needed to inform decision-making, but its impact and application relies on trust and credibility.

This theme unites several discussions that took place, which centred around a pervasive risk-averse culture, issues relating to decision making and an over emphasis on technological solutions, and a need to better understand the value of specialist knowledge input at an early stage of the investigation.

Significant discussion centred around the impact of culture on decision-making processes across policing. Risk-averse frontline officers display a culture of seizing all digital devices at scene, expecting analysis work to be performed on these devices without articulating what is needed from their examination. This seize all approach is underpinned by the uncertainty surrounding potential valuable evidence and the fear of missing critical information, as well as pressures related to constrained time and resources on the frontline, and skills of frontline officers. While some police organisations have already introduced processes to limit the number of devices accepted for examination based on their investigative and evidential value, the question arose as to how this might be combatted earlier in the process (e.g., at scene).

The proliferation of new digital devices and ways of using them in different types of criminality heighten existing gaps in knowledge. Moreover, frontline officers’ perception that digital forensic examinations will be able to provide solutions, without knowing what is needed from devices, relates to a wider overemphasis on technological solutions. Stakeholders discussed how this could result in officers feeling disempowered and hesitant to make timely decisions, aggravating a setting already characterised by delayed and offset decision-making. A more focused search and seizure strategy will be commensurate to how early input from specialist teams is considered in the investigation. Still, stakeholders pointed out that the extent to which decision-making is informed by specialist knowledge relies on the trust and credibility that decision-makers place on those providing this advice.

Collateral Intrusion

- Collateral intrusion can impact on public trust in policing and forensic science.
- Today's digital devices are integral to personhood and offer private and intimate insights into peoples' lives.
- There are concerns amongst stakeholders about the disruption caused to victims and by device seizure, including the risks of intrusion on irrelevant and personal information during examination and review.
- Triage should reduce the risks of collateral intrusion, which may impact how triaging is understood, and trust in digital forensics more broadly.

The theme of collateral intrusion spoke substantially to the connection between the Trust and Triage Projects. Collateral intrusion can be understood as the encroachment on the privacy of individuals, who are not suspects of a crime, beyond the needs of an investigation. Stakeholders discussed how today's digital devices are integral to life and personhood and offer a private and intimate insight into peoples' lives. This discussion largely concerned challenges around the disruption caused by device seizure, the risks of intrusion on irrelevant and personal information during examination and when returning evidence to officers, and what happens to devices following seizure and examination. Moreover, it should also be noted that the risks of collateral intrusion may be increased by a lack of proper training and the prevalent seize all culture in frontline officers.

Stakeholders discussed how the risk of collateral intrusion could be reduced. They discussed the need to be victim led and suspect focused, which related to a wider emphasis throughout the day on the importance of focusing on people rather than tools and technology in the processes of digital forensics. Additionally, emphasis was placed on the need to conduct examinations quickly and efficiently at scene through selective extraction. This serves to both facilitate the release of devices following triage, cutting down on the backlog of devices that are being kept in storage, and to make the process of digital examination as transparent as possible.

It was noted that, unlike a physical premises search, digital examination occurs largely out of sight, and this can impact victims' and suspects' sense of control; this may be felt particularly astutely for victims. Conducting examinations with the device owner present may allow them to retain some sense of control in this process. Furthermore, in relation to this, stakeholders considered whether communicating the processes involved in digital forensics could contribute to improving trust, and whether this is something the SDFA could contribute to. The discussion about mitigating the risks of collateral intrusion also related to stakeholder concerns around skills and training, as we considered how engaging in such processes rely on knowing what you need to know quickly to avoid losing potential evidence. Finally, questions arose concerning how adopting a focus on reducing collateral intrusion might impact the assessment, seizure, preservation, extraction, analysis, and understanding of data on these devices, as well as our understandings of triage as either a targeted or intrusive process.

Project Future

- Triage must be defined clearly to understand what the SDFA can contribute.
- We should go beyond tools, technologies, and processes, and attend to people, resources, and time.
- The project should not make an isolated contribution, and ongoing support and collaboration from the project would be required by stakeholders.

Stakeholders discussed recommendations for the Triage Project. In respect to understanding and defining triage, this requires understanding what the process of triage aims to achieve. For example, potential objectives of triage discussed included checking a device, preserving data, extracting data, and understanding data. All these objectives pose their own unique challenges and risks, both in an immediate sense and further down the line. Stakeholders pointed out that if frontline officers will be making decisions based on information provided to them by the SDFA, then it is vital the purpose of triage is defined clearly. Establishing a clear focus on what triage aims to achieve will help the project avoid scope creep, and clearly articulate the parameters of the research and any subsequent tool design.

Further, suggestions were made as to what an SDFA might incorporate, such as a dataset of devices being seized and the informative or evidential value they might offer, the motivations to attend crimes scenes, or the types of triage practices that are useful at different crime scene types. Stakeholders highlighted key challenges for the Triage Project, including:

- The volume of relevant and irrelevant data stored on devices.
- Variety and complexity of devices.
- Constant development of new technologies.
- Increasing and complex role of digital technologies in crime.

These pose significant challenges to the project, and the development of a future SDFA designed to assist with triaging. For example, how would a tool be kept up to date to ensure it continues to be relevant and valuable to officers? Importantly, stakeholders emphasised that whatever form the SDFA might take, the Triage Project should not make an isolated contribution, and that ongoing support and collaboration would be required. Overall, stakeholders emphasised that the focus of the SDFA needs to go beyond tools, technologies, and processes, and must attend to people (officers, victims, and suspects), resources, and time, which related to the wider emphasis on moving away from a culture in policing of believing technology is able to solve everything.

The insights and recommendations offered by stakeholders at the launch event will be instrumental in defining the scope of our project, and the discussion included in this report has already been used to refine our interview protocol and to inform the themes we plan to explore in our literature review.

Acknowledgements

We would like to acknowledge and thank all those that attended and contributed to the event, and a special thanks to our keynote speakers:

Carole McCartney: Professor of Law and Criminal Justice at University of Leicester

Alan Tribe: Director of Forensic Operations, Metropolitan Police Service

Gary Pugh: Forensic Science Regulator

Jo Morrissey: Workforce Strategy Lead, Forensic Capability Network

Partners

University of Dundee

THE UNIVERSITY of EDINBURGH

University of Essex

UNIVERSITY OF Southampton

COVER PHOTO: Matt Clayton

ucl.ac.uk/