Effective resource management in digital forensics: An exploratory analysis of triage practices in four English constabularies

Article *in* Policing An International Journal of Police Strategies and Management · December 2019

DOI: 10.1108/PIJPSM-07-2019-0126

CITATIONS
21

READS
253

1 author:

Dana Wilson-Kovacs
University of Exeter
34 PUBLICATIONS **400** CITATIONS

SEE PROFILE

emerald PUBLISHING

Policing: an International J

Effective resource management in digital forensics: an exploratory analysis of triage practices in four English constabularies

Journal:	*Policing: An International Journal*
Manuscript ID	PIJPSM-07-2019-0126.R1
Manuscript Type:	Research Paper
Keywords:	digital forensics, crime investigation, Policing, triage

Please note this manuscript is a revision submitted for the Special Issue of Policing: An International Journal Policing Cybercrime (editor Adam Bossler)

Title:
Effective resource management in digital forensics: an exploratory analysis of triage practices in four English constabularies

Purpose:
Building on the findings of a British Academy-funded project on the development of digital forensics in England and Wales, this article explores how triage, a process that helps prioritise digital devices for in-depth forensic analysis is experienced by digital forensic examiners and police officers in four English police forces. It is argued that while as a strategy triage can address the increasing demand in the examination of digital exhibits, careful consideration needs to be paid to the ways in which its set-up, undertaking and outcomes impact on the ability of law enforcement agencies to solve cases.

Design/methodology/approach:
The findings presented are the result of ethnographic observations and semi-structured interviews. They emphasise the challenges in the triage of digital exhibits as they are encountered in everyday practice. The discussion focuses on the tensions between the delivery of timely and accurate investigation results and current gaps in the infrastructural arrangements. It also emphasises the need to provide police officers with a baseline understanding of the role of digital forensics and the importance of clearly defined strategies in the examination of digital devices.

Originality/value:
This article aims to bridge policy and practice through an analysis of the ways in which digital forensic practitioners and police officers in four English constabularies reflect on the uses of triage in digital forensics to address backlogs and investigative demands. Highlighting the importance of digital awareness beyond the technical remit of digital forensic units, it offers new insights into the ways in which police forces seek to improve the evidential trail with limited resources.

1. Introduction

Digital forensics (DF) has emerged in the last twenty years in response to the ways in which technological developments have impacted on the examination of crime. It encompasses the extraction, examination and interpretation of data from a range of personal and interconnected devices, including mobile phones, computers, navigation systems, gaming consoles and increasingly, the Internet-of-things (IoT). It also extends to communication information and metadata from remote sources (e.g. websites, social media, IP logs) to obtain intelligence for ongoing investigations and provide evidence for criminal proceedings. Once confined to fraud inquiries and child sexual abuse cases, DF has become key to the future of crime investigation (Home Office 2016; Rennison 2015). Critical to supplying evidence for most types of offences, it can help establish sequences of events, patterns of behaviour and alibis. Consequently, law enforcement agencies have encountered an unprecedented pressure to deliver timely and effective digital examinations (Vincze 2016). The rise in the number and diversity of potential sources of digital evidence, the amount of data to be examined, and the complexity of DF processes to extract relevant information compound this issue. The nature of the crime examined also raises further challenges, as computer assisted or cyber-enabled crimes (i.e. traditional crimes with a digital trace element, such as on-line fraud) may consist of different methods than cyber-dependent crimes (i.e. offences where computers have been misused - e.g. hacking) and call for distinct DF skills-sets and approaches.

In the UK, these developments concentrated the focus on how police forces deal with the processing and examination of seized digital exhibits and prompted calls for 'a fundamental rethink of the responsibilities, roles, services, and operating models of forces' (Home Office 2015: 16). The response has been the introduction of triage to address this demand. Often employed in emergency rooms and at disaster sites, triage refers to a prioritisation process where those requiring treatment are grouped according to the urgency of their needs and potential benefits from immediate medical intervention. One use of triage in forensics has been in the context of volume crime, in relation to the selection of the DNA samples from a crime scene that are most likely to bring valuable information to an investigation and remove 'time-wastage' (Julian and Kelty 2015).

In DF, triage involves ranking apprehended digital items in terms of their importance to a case and likelihood that they contain the data required (Pollitt 2013; Rogers et al 2006). Essential to time-sensitive cases, where finding relevant data quickly is paramount, triage is increasingly required to prioritise exhibits because of the number of apprehended devices in a case. Triage involves the use of specialised software packages to automatically identify potential evidence: for instance, in cases where the possession of indecent images of children is suspected, tools running keyword searches speed the detection process. Instrumental to the identification of evidence, triage can be a foundational part of the overall investigative strategy but not a replacement for a full examination (Casey et al. 2013). One of its main advantages is that it can be carried out by personnel with a basic technical knowledge. As such the adoption of triage can help preserve the limited resources of DF laboratories and direct the expertise of DF examiners where it is needed most.

Building on the findings of a British Academy-funded project on the development of DF in England and Wales, this article explores the challenges of triage in situ. It focuses on the experiences of DF practitioners and police officers involved in setting up, carrying out and using the outcomes of its processes in crime investigation in four English constabularies. Drawing on qualitative methods, specifically observations, interviews and document analysis of policy guidelines and local arrangements for the provision of DF support, it explores the technical and administrative dimensions of triage and the pressures of improving the evidential trail with limited resources and police time. Highlighting the inherent tensions between the operational culture of policing and the DF analytical approach, it argues that the effectiveness of triage processes requires organisational flexibility and foresight, a dedicated and informed workforce and tailored resources. The article begins with an outline of extant sociological and practitioner literature on DF and considers the political and economic environment within which DF in policing has emerged in the UK. After introducing the methodology guiding data collection and interpretation, it examines key aspects of triage arrangements in the forces studied. The paper concludes with a summary of the findings, the limitations of the current analysis and reflections on the task of reconciling the tensions between efficient and timely evidence collection and the management of police resources nationally and internationally.

2. (Digital) forensics and policing in England and Wales: a brief overview

For the last three decades, social science scholarship on forensics has focused largely on two related developments: novel technologies such as DNA profiling and the expansion of national DNA databases for the identification and tracking of suspects. While studies on the dynamics between scientific expertise and judicial decision-making have demonstrated how streamlined protocols and distinct methods of identification and evidence interpretation reinforce the scientific standing of DNA profiling (e.g. Jasanoff 1998; Lynch et al. 2010), evaluations on stakeholders' expectations of forensic genetics illustrate how its gold-standard has lent it extraordinary credibility in and outside of juridical settings. Notwithstanding, the prevalent focus of sociological analyses on forensic genetics leaves other

forensic specialisms under-explored (Innes et al. 2005; Lawless 2016), including the application of DF in policing. Likewise, criminological theory has yet to refine our understanding of how digital evidence impacts on crime examination, juridical outcomes and social policies (Holt et al. 2017).

Yet, a burgeoning body of literature on DF, mostly practitioner oriented, reflects the growing importance of this forensic subdiscipline (Lawton et al. 2014; Rogers 2017; Vincze 2016). While DF has its own technical characteristics, the principles of identifying, analysing and reporting on digital traces are similar to those of other forensic disciplines (Home Office 2016). In the US, the work of SWGDE (the Scientific Working Group on Digital Evidence)[i] has established and strengthen the communication between law enforcement agencies and DF practitioners across international communities. In the UK the Association of Chief Police Officers (ACPO) has produced the ACPO Good Practice Guide for Digital Evidence, which lays the foundations upon which police forces in England and Wales have approached the implementation of DF arrangements and processes. Outside official documents and technical guidelines, attention in the UK has been paid to developing competencies, tool testing and verification methodologies for data extraction and analysis (e.g., Marshall et al. 2013), guidance on the admissibility of digital evidence in court (e.g., Collie 2018; Sommer 2010), deliberation on forensic standards (e.g. Tully 2018), socio-legal and ethical aspects (e.g. Horsman 2017) and psychological dimensions, such as cognitive bias (e.g. Sunde and Dror, 2019) and resilience in reviewing indecent images of children (e.g. Jewkes and Andrews 2005). While insights into how DF has been applied in policing in England and Wales are currently missing, this oversight that can be partly explained by the novelty and rapid expansion of the domain. A pervasive government and police view of forensics as supplying mere technical support (Lawless 2016) adds to the difficulty of documenting the role of DF.

The development of DF in the UK has sought to strengthen public and judicial trust in DF and followed the Government's aspiration for a cost-effective service delivery of evidence to police and the courts, suitable ethical oversight and the implementation of quality benchmarks and forensic standards. Guided by codes of practice produced by the Association of Chief Police Officers (ACPO 2012) and the Forensic Science Regulator's Office (2014; 2016), as well as the input of the National Police Chiefs' Council through programmatic documents such as *Policing Vision 2025* (NPCC 2013), and initiatives like the *Digital Policing Portfolio* (2018) and the *Transforming Forensics Programme* (2017), it envisages the standardisation of forensic support services across the 43 police forces, encouraging the local pooling of resources through in-house laboratories, the streamlining of services to promote efficiencies and the creation of a skilled and technically capable workforce.

Although the *Forensic Science Strategy* (Home Office 2016), advances a clear governance system of forensic science support and seeks to regulate delivery, it has been criticised for its lack of a systematic approach and consultation with relevant stakeholders and for devolving powers over service provision to individual police forces. The *Strategy* addresses a fragmented landscape of forensic service delivery where the dissolution of the Forensic Science Service in 2012, alongside with that of the National Policing Improvement Agency, a non-departmental public body aimed at maximizing the value of forensics in policing, led to decentralisation. A climate of economic austerity and continuous budget cuts to forces, with police spending on forensic support services decreasing by 18% between 2010 and 2016 (HCSTC 2017: 8) and the subsequent funding shift towards a market-based provision model, led to uncertainty and the loss of knowledge and expertise (Squires 2015; Hitchcock et al. 2017) and put the quality of investigations and forensic processes at risk (Tully 2018).

Responding to the need to deal with backlogs of digital devices and inconsistencies in the ways in which cases are handled, triage addresses the disparity between service demand and available resources and ensures a more efficient service delivery (Casey et al. 2009, Pollitt 2013). Similar to its deployment in traditional forensics where it is used to make decisions about whether DNA samples will be moved to the next stage of examination (Brown 2015), triage in DF seeks to focus examination

efforts on the exhibits that are most likely to bring key information to the investigation or the most probative value to a case (Harriss and Boast 2016). Standard practice nationally, it helps dealing with an escalating number of exhibits for DF analysis: considering that on average an individual owns seven digital devices (Home Office 2016), each with a growing capacity to store data, identifying key items to an investigation has become increasingly problematic despite the use of specialist triage software and tools. Given that 'reliance on forensic science requires the most efficient use of resources to ensure the maximum return on investment' (Bond and Sheridan 2008: 327), triage represents the solution to coping with the hurdles brought about by the breadth, size and complexity of digital data.

Writing on triage in DF has predominantly focused on practitioner guidelines (e.g. Garfinkel 2013), emphasising the advantages, risks and trade-offs in its adoption (Casey et al. 2013). Its coverage in police practice in England and Wales has received limited attention, with extant analyses highlighting the ambiguities surrounding its use as (1) a set of specific administrative arrangements to prioritise or exclude seized items, (2) the technical processes on which such decisions are based, or (3) a combination of both (Ho and Li 2015, Montasari 2016, Shaw and Browne 2013). Typically, the higher the workload of DF examiners, the more likely triage processes are in place to rank items. Nationally triage practices vary considerably: while some DF laboratories lack a triage process in the examination of computers (Hi and Li 2015), others use triage to decide which cases and exhibits should be examined first, rather than actively eliminate devices from examination (Shaw and Browne 2013). Neither of these approaches have been shown to reduce the volume of exhibits or provides effective support, and a more detailed understanding of existing arrangements is needed.

4. Methodology

The methodological approach adopted here builds on the ethnographic turn in criminology (e.g. Hall and Winlow 2015, Hobbs et al. 2003). The data presented below was collected between January 2017 and September 2018 through 120 hours of ethnographic observations and forty-three semi-structured interviews. The observations took place at four in-house DF laboratories affiliated to four English constabularies and followed everyday activities, such as handing in and processing exhibits, exchanges among DF practitioners, interactions with police officers, and team meetings with members of senior management. They were supplemented by a review of DF sources, including local Service Level Agreements and guidelines for the seizing and analysis of DF devices, national guidance, White Papers, and on-line DF community forums. Informing the analysis were 6 interviews with police officers involved in triage, 32 with DF practitioners (3 technicians, 9 mobile devices examiners, 16 computer investigators - 6 of which were also team managers - 2 senior managers and one performance analyst). Five additional interviews with relevant stakeholders outside the four forces, including representatives of the Forensic Science Regulator's Office, expert witnesses and private providers of DF services, helped situate the findings in a national perspective. Interviews took between 90 and 150 minutes and explored the local challenges encountered in undertaking triage. They were recorded, transcribed verbatim, then open-coded and examined systematically and sequentially, using a thematic content approach (Braun and Clarke 2006). Observational data of the working DF environment at each location and a systematic evaluation of internal documents, organisational settings and police priorities helped refine emergent threads, which were analytically compared between sites and against the testimonies of members of different occupational groups to identify similarities and differences between accounts (Gubrium and Holstein 2009; Riessman 2008). The following discussion illustrates the aggregated themes.

5. Findings: understanding triage in context

The forces studied cover large rural areas, a bustling metropolitan zone and several cathedral cities. Size-wise, two have around 3000 officers each, serving populations of about one and a half million for

each jurisdiction. The remaining two are smaller, each with about 1000 officers serving around 700.000 people. The number of DF examiners varies according to the size of each force: smaller forces have on average 10 practitioners and larger forces 13. The number of police officers delegated with triage duties ranges between 50 and 200 per force. Crime priorities across constabularies are mixed: in 2017, the metropolitan zone experienced the highest number of DF requests in relation to organised crime and drug offences. During the same period, an estimated 80% of submissions in the other three forces related to sexual offences, primarily the possession of indecent images of children.

As a decision-making process, triage has been used in all forces, for a different number of years. While the introduction of triage resulted in a substantial drop in the items sent to DF laboratories, the number of submissions remains high, and backlogs persist, providing further indication that the effectiveness of triage processes require additional scrutiny. Historical challenges add to these circumstances, as each of the DF laboratories is embedded into the local force's infrastructure and subject to its own administrative arrangements. Understandings of best practice vary between forces and methodologically have been difficult to gauge, given the distinct settings. Operational needs, available resources to address demand, and geographical proximity of DF laboratories are some of the variables that historically affected the ways in which triage has been set up.

In the forces studied, the principles of conducting triage follow the guidelines set in the ACPO Good Practice Guide (2012) and seek to provide operational guidance on how to maintain the integrity of the investigative process and ensure that the evidence produced as a result can be used in a court of law. For the four forces, triage is used to narrow down the number of exhibits that would be considered as relevant to submit for in-depth DF analysis. Although this approach carries the risk that evidence may be missed if an exhibit is excluded from examination, this risk is mitigated by the fact that evidence may be found on the other devices owned by the suspect. Formalised in DF policies through targeted protocols and deployed at various points in the seizing and sorting of exhibits for further examination, triage has both technical and administrative dimensions (Shaw and Browne 2013). The former refers to the application of automated searches and specialist software to check whether potential evidence is present on seized devices. The administrative aspect of triage refers to the arrangements made to carry out the technical triage. In this case, trained police officers are tasked to execute the triage of exhibits. Their work is supervised by gatekeepers, typically senior investigating officers, who decide what items to submit, post triage for more detailed DF analysis. While the management of digital submissions for in-depth analysis is overseen by the DF teams, the recruitment of officers tasked with triage duties and the selection of gatekeepers takes place outside the control of DF teams which can impact on the effective undertaking of triage and lead to professional tensions.

5.1. Doing 'all the wrong things for all the right reasons': analytical versus operational approaches to triage

Despite distinct organisational settings, views on the need and reason for triage are similar across forces, with widespread agreement that the process can speed up the selection of exhibits, sharpen investigation and free the time of DF examiners to focus on the analysis of the most significant items. Several participants remarked on how DF in policing evolved in a largely ad-hoc manner and linked this with the diversity of triage arrangements. Most interviewees agree with the view of triage as a data management tool for the elimination of unnecessary items, controlling the flow of devices to the DFU, matching case requirements to evidence searching strategies, and assuring proportionality. One of the forces observed has employed triage in this way since 2007 and witnessed a sharp drop in the number of items sent for in-depth DF analysis. It found that around 70% of exhibits seized did not hold any valuable evidence to an investigation. Consequently, to allow for the detailed examination of the 30% of remaining case exhibits, the elimination of items with no evidential value is seen as paramount:

> [Before triage], there was more business than we could shake a stick at. What we were finding was that we were getting too many exhibits… and a large percentage of those weren't relevant to the case…whatever they were asking us to find wasn't there. So, we were spending a lot of time that we could better spent looking on the exhibits that really mattered. This is the main reason for applying a triage process to filter out…the jobs that aren't really worthy, the fishing trips, the things that aren't proportionate, things like people would be saying 'he looks a bit funny, I think we should be searching him for this stuff'. So we need to focus the OIC's [officer in charge] mind on what's really relevant in the case. (Computer examiner 4, Force 1)

DF examiners acknowledged that while triage can enable the prioritisation of devices, in order to mitigate the likelihood of missing data, police officers must have a clear investigative strategy to allow for proportionate analysis (ACPO 2012). However, this is not always understood by police officers:

> There are some people who will go 'yeah, we'll triage that', but hang on a minute, let's stop and think about this before we triage it, what are we looking to achieve? What do we know? What are we aiming to get out of this? (Computer examiner 6, Force 3)

For police officers, the DF focus on key exhibits and the rationale of seizing proportionately can sometime clashes with their drive to check as many exhibits as possible:

> Because we've got triage, I want to take everything that it can find… if it's all showing as positive and say, that hard drive is ten years' old well, he's been at it for a very long time. Who was in his life ten years' ago? Did he have access to children? Right, I'm even more interested now, let's start looking at all [devices] even the old cameras, getting all the memory cards out. (Officer 3, Force 2)

Such tensions are attributed to an inability to reconcile divergent investigative demands and resource capabilities. The introduction of triage to eliminate exhibits replaced what officers and DF examiners alike refer to the 'golden' or 'Rolls-Royce service' and encountered extended criticism from officers:

> We were being consulted officially at various stages but…we only saw papers after they were done and dusted and decisions made, which left us pretty spikey, pretty spikey… at the end of the day these are the rules and we've got to work with it, we haven't got any say… (Officer 2, Force 4)

Accompanying officers' reluctant acceptance of triage and the implication that not every seized device can be examined, are concerns about achieving a balance between the need to provide the best support in solving cases and the organisational drive to for efficiency and cost-value. Illustrating this is a view of triage as a quick fix to cope with the overarching shortage of resources:

> In the police environment…everyone is understaffed. Not enough people to do the work they're currently doing. Estates make it very difficult because there's a lack of estate as well, and funding for equipment… it's a lot simpler to buy the software, train a dozen people and say, 'problem sorted, we do triage'. (Mobile examiner 5, Force 2)

Notwithstanding, DF practitioners stress the importance of understanding what triage can and can't do, highlighting that while helpful when there is no immediate possibility of a detailed forensic check, triage does not constitute a replacement for a full examination or indeed, is needed when the investigation is supported by strong intel.

> Often people do all the wrong things for all the right reasons. Somebody will submit a phone and they go 'oh yeah, I've taken a screenshot of bits we're interested in' and that's it, they just trample all over the evidence, you know. They don't know, they were doing their best to get the job done…so that's a drawback… (Mobile examiner 1, Force 3)

DF examiners repeatedly noted the inherent limitations of automated searches and triage software pointing out that they are not infallible, in fact, "If the triage tool finds nothing, it doesn't mean that there is nothing, it simply means that the tool found nothing" (Computer examiner 11, Force 4). They also spoke at length about the dangers of treating triage findings as 'evidence'. Clarifying these issues with officers occurs routinely and can be a lengthy undertaking, which confirms the need to inform officers better about the limitations of technical triage, and the importance of an early investigative strategy to inform the triage process.

5.2. The limitations of technical triage

As discussed, technical triage relates to the software tools used select relevant data from seized devices. The choice and adoption of triage packages is driven by economic considerations and guided by utility and price (including license requirements). The growing demand in the examination of mobile exhibits (particularly phones), has rendered triage more challenging due to network capabilities, dynamic operating environments and the volatile nature of data on these devices (Bennett 2012; Mislan et al. 2010). While some officers are aware that triage software cannot reliably capture all data, especially when used on mobile exhibits, knowledge that evidence cannot be always obtained through triage varies considerably.

> You know you're not going to want to triage an abuse job because you might miss something and we're not going to want to miss something on a live abuse case (Team manager A, F4)

Additional questions are raised over the speed and ease of use of different software, with officers expressing the need to enhance technical triage through faster and more accurate detection tools. Relatedly, DF practitioners noted that the technical specifications of some triage packages (e.g. the restricted ability to search deleted files and unallocated disk space) may require that additional checks are performed before deciding whether items should be submitted for or excluded from analysis, a particularly difficult undertaking when triage is used for on-site examinations. Knowing what to seize at a crime scene is a complex undertaking that depends on the type of offence and the information received by those doing the seizure (who are usually specialist police teams with limited DF awareness). Different locations and offences provide distinct opportunities and limitations for carrying out triage: for instance, triage at a victim's location in a homicide investigation can offer better conditions for triage than carrying out the procedure at a suspect's residence in a child sexual abuse case. Making a difference to the former is the presence of Crime Scene Examiners, who can forensically secure the scene and identify the items of potential value to an examination. In the latter case the process is limiting because it lacks a controlled environment for checking exhibits and performing triage analysis. Although triage software can be 'pre-loaded' with keywords and pictures to check the user's storage and internet history files, process time can take days, rather than hours and may render on-site triage impractical:

> With triage there is a time element involved. I don't use it for looking for picture unless I really am in some desperate situation. I very rarely go to the extent because it's so time consuming, when you start you don't know how long it's gonna take (Computer examiner 16, Force 3).

One aspect of triage processes often highlighted in the literature is that DF expertise is not required to perform them. However, even if triage does not call for highly developed technical skills, it still

involves precision (Vincze 2017) and demands that personnel remain familiar with protocols, in order to avoid mistakes that can invalidate procedures and interfere with the authentication of findings or the processing of evidence. The coordination of triage at crime scenes highlights the complexity of the process and the need for a dedicated forensically aware and skilled workforce, a finding that aligns to calls for the creation of Digital Scenes of Crime Officers (Sommer 2013).

The undertaking of technical triage is further embedded in the ways in which triage as an administrative process is set up in each force. This arrangement is coordinated by police forces, and involve police officers, rather than DF laboratories personnel, who are predominantly civilian. Overseeing the process are gatekeepers whose insight is intended to sharpen the investigative strategy and narrow down the identification of most suitable items. Gatekeepers take decisions as to which exhibits are submitted for in-depth examination: they are typically senior investigating officer, mirrored on the DF side by a team manager, tasked with reviewing cases and exhibits before in-depth analysis takes place. While this hierarchical system of checks and balances is intended to ensure the smooth and effective communication between the operational and technical sides of an investigation, in practice it reveals a number of issues.

5.3. Triage officers and gatekeepers: skills and workload acknowledgment

Triage training is routinely offered to frontline officers and many take up the opportunity to enhance their skills. The mix of technical ability and interest in retaining the skills gained are factors affecting its success. Engaging in triage consistently is seen as a pre-requisite of doing it correctly. However, while technically unproblematic, effective triage requires ongoing familiarity with the process, which can be problematic, as officers tend to focus on own workloads or move between roles:

> Often…somebody's got a big case and they want to get it done, so they get themselves trained and (once the case is done) …we never hear from them again. So we have 40 or 50 people on our list, but probably only about 20 are actively doing it. (Computer examiner 9, F1)

From the large number of officers trained in each of the four forces studied, only a few will use the skills gained and even fewer will perform triage effectively:

> You need to be doing it regularly to keep your skills up, because if you don't do it for 6 months, [when] you come back you can't remember and then you are forever on the phone to us, and often [we need to] have face time calls 'right okay, change the setting to this, change this to this'…the people that do triage…should have an idea about phones and tablets and computers…and then you bolt the triage part onto that and then they should be doing it regularly. It's no good somebody being trained and then… doing 2 triages a year… (Team Leader, F2)

Not engaging regularly with the procedure results in a lack of confidence, noticeable when the officers start asking DF examiners for advice. Equally undertaking triage impacts on the workloads of officers tasked with triage duties:

> The triage process means that our investigations are tied down and other things get deferred because this is what we've got to do. Research development gets slowed down because I am spending two to three hours in a day doing triage work. (Officer 1, Force 3)

Fluctuations in the officers' ability to identify and triage exhibits with the most probative value, and mission creep (i.e. asking for additional checks and searches, especially when the triage tools turn

negative results) add to a lack of formal recognition of the time spent doing triage (i.e. a dedicated role), which impacts on the effectiveness of the process:

> The problem we have currently is that all of our triage officers and... gatekeepers are doing this as a favour to the force. It's not their day job, it's not their priority, so this is what they do in their spare time. (Team leader, F1)

Thus, the organisation and monitoring of administrative triage can delay ascertaining which items should be prioritised for detailed DF examination. Similar to the officers carrying out triage, gatekeepers fulfil triage duties in addition to full caseloads without acknowledgment of the time spent in their workloads. Consequently, the gatekeeping can lack oversight, which in turn impacts on the time DF examiners are required to spend sorting outstanding issues, such as whether devices have been triaged correctly. This leads to bottlenecks in submissions to the DF laboratories and subsequent delays in the processing of cases. As such, triage is seen to work best when technically proficient officers dedicate their time to do the job 'in and out', establishing familiarity with procedures and reinforcing accountability and ownership.

While the tensions discussed can be partly attributed to a view of forensics as a service to forces rather than an essential and central component of any investigation (Lawless 2016), the escalation in the demand for DF services and the lack of resources and dedicated personnel impact negatively on the processing of cases. In recent months, in response to the escalating number of mobile devices seized, an attempt to regain ownership of the triage process has been made by delegating Crime Scene Examiners (CSE) with their triage. As these practitioners are both forensic specialists and civilian personnel, the danger of losing triage expertise through officers' lack of availability or capacity is diminished. Moreover, DF managers felt that this step would also strengthen the accuracy of the procedure and its outcomes. However, this measure can only partially address the challenges faced, which extend beyond the remit and capabilities of the DF units.

6. Concluding remarks

It has been long recognised that the rise in the number of submissions of digital devices leads to backlogs, delays investigations and impacts negatively on the criminal justice system (Casey et al. 2009). Triage processes have been introduced in the UK and globally (e.g. Cantrell et al. 2012) to deal with escalating demands, speed up examination and help select the items with most probative value. They do not require extensive technical expertise to run and can be carried out by trained police officers, helping thus to effectively ring-fence the expertise of DF examiners so that they are able to focus on targeted examinations (e.g. van Beek et al. 2016). In the fragmented forensic service landscape of England and Wales, marked by on-going budget cuts to police forces, triage can potentially deliver more efficient support to investigation and successfully balance quality requirements with DF assistance. Drawing on the testimonies of DF practitioners and police officers across four constabularies, the analysis presented here captured their views on triage and the challenges it raises. The findings echo emerging analyses on challenges encountered in policing globally to deal with the surge in digital evidence (Bennett 2012; Ho and Li 2015; Vincze 2016).

Unlike forces that deploy triage to decide which mobile and computer exhibits should be analysed first, the constabularies studied shared a focus on the active elimination of devices from examination following triage. The risk that evidence may be missed if devices are excluded from the examination can be mitigated by robust intelligence, appropriate examination strategies and proportionate investigative lines of inquiry. Given the increased need to use existing digital forensic expertise strategically, focusing the work of mobile and computer examiners on the most relevant items in a

case is key to ensure maximum efficiency. While this is notionally offered by current arrangements, in practice it raises several issues.

Prior to carrying out in-depth analyses, DF examiners need a clear picture of what the investigation of devices seeks to achieve and what they should be looking for in the first place (Gogolin 2010). Triage can help narrow this focus, yet, the success of automated searches depends on many factors, including the device type, the alleged offence, the available software packages, the technical ability of those performing such searches and the clarity of the investigative strategies. In the forces observed, the amount of time dedicated to discussions around which items should be prioritised for triage, the interpretation of triage results, including the negotiations surrounding negative outcomes, directly impact on the workload of DF examiners, and in this respect diminish the efficiency of triage.

Furthermore, reflecting growing national concerns about the ways in which extracted information can be used to prosecute suspects (Sommer 2013), DF practitioners warned of the risk of equating triage outcomes with actual proof of guilt, when the interpretation of results is missing. Commentators elsewhere equally caution against attempts by individuals with insufficient technical knowledge to evaluate evidence (Casey et al. 2013). The danger here, as Collie (2008) notes, is that officers with little training can end up cherry-picking evidence to suit a case. An inconsistent understanding of the limitations of triage can also hinder the articulation of coherent investigative strategies and create tensions between officers and DF practitioners. The lack of technological awareness and ability to liaise with the DF service teams, can easily lead to failures in evidence gathering and interpretation, and in providing testable information, which can have considerable implications for the acceptability of DF evidence in court and the credibility of DF as a scientific discipline.

Given ongoing technological developments such as the rise of the IoT, the monitoring of homes and vehicles, and the emergence of remote Cloud storage facilities (Marshall et al. 2013), police forces need to increase investment in R&D and regularly evaluate the most effective ways of accomplishing triage. To move beyond a "perpetual state of 'catch-up'" (Jewkes and Andrews, 2005: 48) the training of officers should actively seek to retain and exercise the skills gained through triage. Nationally, while efforts have been made to train officers in triage, with the exception of some 'pockets of excellence', a broad lack of skills has been noted (Home Affairs Committee, 2013). Many forces suffer from both a shortage of technically skilled professionals helping with the demand placed on the processing of digital evidence and a lack of sufficient understanding of the skillsets needed to develop the digital capabilities of their officers (HMIC 2017; House of Lords Hansard 2018).

This is reflected in the work of DF examiners interviewed, who contend daily with officers' confusion over triage procedures and what can be submitted for analysis, at what stage, as well as the time and resources needed to extract and interpret the data. The findings emphasise continuing gaps in the infrastructure required to provide officers with up-to-date digital knowledge for effective triage. As Sommer notes, "every detective needs to know the basics of digital evidence - where it is likely to be located, how it can be safely collected and preserved without being contaminated in the process, and the core techniques that are used in analysis" (written evidence to Home Affairs Committee, 2013).

Although triage arrangements differed across the forces studied, tensions regarding the alignment of technical and administrative triage processes were shared. The results of this analysis bring to fore organisational inconsistencies in the provision of triage processes, and especially a lack of acknowledgment on behalf of senior managers and police officers of the time invested in triage and gate-keeping activities. The accomplishment of triage was largely attributed to the commitment of DF and police professionals, rather than the judicious distribution of existing resources. Participants talked about the discrepancies between expectations surrounding the implementation of triage and the incongruities created by current arrangements, with findings highlighting that the effective

delivery of triage is contingent on both technically aware frontline personnel and a workforce protected by appropriate organisational arrangements. Here, the training of triage officers as successful conduits between the operational world of policing and the technical world of DF requires careful consideration. Testimonies revolve around the mixed value of the current system which has little success retaining trained officers, slows down processes and can further create, rather than prevent, bottlenecks. To address the deficiencies in the triage training of large numbers of officers only to lose this expertise when officers moving roles or are unable to use the skills acquired, a dedicated workforce was seen as the best solution by all those interviewed.

Triage sits at the interface of two cultures: operational (police) and technical/scientific (DF), so understanding how it unfolds in practice can offer valuable insights to how the two can organically grow and complement each other. Such an understanding also requires a view of triage as a force-specific tailored response to the pressures of dealing with backlogs, the scarcity of resources and the increasing demand for DF. While this analysis is not intended to offer a generalised understanding of triage across the 43 police forces in England and Wales, in identifying shared tensions between four of them, it advances an understanding of triage as contextual and contingent on several internal and external factors that necessitate further critical scrutiny. The qualitative approach adopted here creates the basis for the development of analytical concepts and theoretical generalizations that can "offer insights for understanding other situations while being historically and contextually grounded" (Feldman and Orlikowski 2011: 1249). Likewise, beginning to document the diversity of current practices and explore the entanglement of local pressures and arrangements, can provide useful for comparison with other national jurisdictions and may help identify alternatives solutions to address the demand for DF analysis globally. This is increasingly needed when considering the future challenges posed by the growing number of IoT devices and the automation of forensic processing (Guarino 2013) vis-à-vis the ability of law enforcement agencies to deal with on-going need for DF examinations.

References

ACPO (Association of Chief Police Officers). 2012. Good Practice Guide for Digital Evidence. Version 5 Accessed 31/05/2018
http://www.acpo.police.uk/asp/policies/Data/gpg_computer_based_evidence_v5.pdf

Bennett, D., 2012. The challenges facing computer forensics investigators in obtaining information from mobile devices for use in criminal investigations. *Information Security Journal: A Global Perspective*, *21*(3):159-168.

Braun, V. and Clarke, V., 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2): 77-101.

Bond, J.W. and Sheridan, L., 2008. A novel approach to maximising the detection of volume crime with DNA and fingerprints. *International Journal of Police Science & Management*, *10*(3): 326-338.

Brown, C.S., 2015. Investigating and prosecuting cybercrime: forensic dependencies and barriers to justice. *International Journal of Cyber Criminology, 9*(1): 55-119.

Cantrell, G., Dampier, D., Dandass, Y.S., Niu, N. and Bogen, C., 2012. Research toward a partially-automated, and crime specific digital triage process model. *Computer and Information Science, 5*(2): 29-39.

Casey, E. 2013. Triage in digital forensics. *Digital Investigation* 10(2): 85-86.

Casey, E., Ferraro, M. and Nguyen, L., 2009. Investigation delayed is justice denied: proposals for expediting forensic examinations of digital evidence. *Journal of Forensic Sciences, 54*(6): 1353-1364.

Casey, E., Katz, G. and Lewthwaite, J., 2013. Honing digital forensic processes. *Digital Investigation 10*(2): 138-147.

Collie, J., 2018. Digital forensic evidence. Flaws in the criminal justice system. *Forensic Science International*, *289:* 154-155.

Feldman, M.S. and Orlikowski, W.J., 2011. Theorizing practice and practicing theory. *Organization science*, *22*(5): 1240-1253.

Forensic Science Regulator 2014. *Codes of Practice and Conduct. Appendix: Digital Forensic Service*s FSR-C-107 Issue 1.

Forensic Science Regulator 2016. *Codes of Practice and Conduct. Appendix: Digital Forensics – Cell Analysis.* FSR-C-135 Issue 1.

Garfinkel, S.L., 2013. Digital media triage with bulk data analysis and bulk_extractor. *Computers & Security*, *32:* 56-72.

Gogolin, G., 2010. The digital crime tsunami. *Digital Investigation*, *7*(1-2): 3-8.

Guarino, A., 2013. Digital forensics as a big data challenge. In *ISSE 2013 securing electronic business processes* (pages 197-203). Springer Vieweg: Wiesbaden.

Gubrium, J. F., and Holstein, J. A. 2009. *Analyzing Narrative Reality*. Thousand Oaks, CA: Sage.

Innes, M., Fielding, N and Cope, N. 2005. 'The Appliance of Science?' The Theory and Practice of Crime Intelligence Analysis. *British Journal of Criminology, 45*(1): 39-57.

Jasanoff, S. 1998. Witnessing DNA in the Simpson Trial. *Social Studies of Science,* 28(5/6):713-740.

Jewkes, Y. and Andrews, C. 2005. Policing the Filth: The problem of Investigating Online Child Pornography in England and Wales. *Policing & Society*, *15*(1): 42-62.

Hall, S. and Winlow, S., 2015. *Revitalizing Criminological Theory: Towards a new Ultra-Realism*. Routledge.

Harriss, L. and Boast, K. 2016. Digital Forensics and Crime. Post Note 520. Houses of Parliament. Parliamentary Office for Science and Technology. London, March 2016. Accessed: 04/02/2017 http://www.parliament.uk/post

HCSTC (House of Commons Science and Technology Committee), 2017. Forensic Science Strategy Fourth Report of Session 2016-17. Accessed: 19/05/2018 https://publications.parliament.uk/pa/cm201617/cmselect/cmsctech/501/501.pdf

Hitchcock, A., Holmes, R., and Sundorph, E. 2017. *Bobbies on the Net: A Police Workforce for the Digital Age*. Reform. Accessed: 20/10/2018 https://reform.uk/research/bobbies-net-police-workforce-digital-age

HMIC (Her Majesty's Inspectorate of Constabulary), 2017. 'State of Policing The Annual Assessment on Policing in England and Wales 2016' Accessed: 19/05/2018 https://www.justiceinspectorates.gov.uk/hmicfrs/wpcontent/uploads/state-of-policing-2016.pdf

Ho, A.T. and Li, S. (eds.) 2015. Digital Forensic Laboratories in Operation: How are Multimedia Data and Devices Handled? In *Handbook of digital forensics of multimedia data and devices*. John Wiley & Sons, Ltd: IEEE Press. Pages 3-37.

Hobbs, D., Hadfield, P., Lister, S. and Winlow, S., 2003. *Bouncers: Violence and governance in the night-time economy*. Oxford University Press.

Holt, T.J., Bossler, A.M. and Seigfried-Spellar, K.C., 2017. *Cybercrime and Digital Forensics: An Introduction*. London: Routledge.

Home Office 2015. Digital Investigation and Intelligence: Policing capabilities for a digital age. Report produced by College of Policing, National Crime Agency, and National Police Chiefs' Council. London: HMSO.

Home Office 2016. *Forensic Science Strategy*. London: HMSO.

House of Lords Hansard 2018. 'Digital forensic services' 12/03, Vol.789, Accessed 19/05/2018 https://hansard.parliament.uk/Lords/2018-03-12/debates/DAB3481A-984E-4123-9EBC-213C458971EC/DigitalForenicServices

Horsman, G., 2017. Can we continue to effectively police digital crime? *Science & Justice*, *57*(6): 448-454.

Lawless, C., 2016. *Forensic Science: A Sociological Introduction*. London: Routledge.

Lawton, D., Stacey, R., & Dodd, G. 2014. *eDiscovery in Digital Forensic Investigations.* Technical Report, CAST Publication 32/14, Home Office: London.

Lynch, M., Cole, S. A., McNally, R. and Jordan, K. 2010. *Truth Machine: The Contentious History of DNA Fingerprinting*. Chicago: University of Chicago Press.

Marshall, A., Higham, S., and Dyhouse, T. 2013. *Digital Forensics Capability Review.* Special Interest Group Forensic Science, June. accessed 31/05/2018 https://www.researchgate.net/publication/269332581_Digital_Forensics_Capability_Review

Mislan, R.P., Casey, E. and Kessler, G.C., 2010. The growing need for on-scene triage of mobile devices. *Digital Investigation*, *6*(3-4): 112-124.

Montasari, R.A., 2016. Formal Two Stage Triage Process Model (FTSTPM) for Digital Forensic Practice. *International Journal of Computer Science and Security 10*(2)*:* 69-87.

NPCC (National Police Chiefs' Council) *Policing Vision 2025*. Accessed 31 May 2018 https://www.npcc.police.uk/NPCCBusinessAreas/ReformandTransformation/PolicingVision2025.aspx

Pollitt, M.M., 2013. Triage: A practical solution or admission of failure. *Digital Investigation*, *10*(2): 87-88.

Rennison, A. 2015. Forensic Intelligence. *Australian Journal of Forensic* Sciences 47(1): 3-5.

Riessman, C. 2008. *Narrative Methods for the Human Sciences*. Los Angeles, CA: Sage Publications.

Rogers, M.K., Goldman, J., Mislan, R., Wedge, T. and Debrota, S., 2006. Computer forensics field triage process model. *Journal of Digital Forensics, Security and Law*, *1*(2): 2.

Rogers, M. 2017. Technology and digital forensics. In M. R. McGuire, M.R. and Holt, T. J. (eds.) *The Routledge Handbook of Technology, Crime and Justice*. Oxon: Routledge. Pages 406-416.

Shaw, A. and Browne, A., 2013. A practical and robust approach to coping with large volumes of data submitted for digital forensic examination. *Digital Investigation 10*(2): 116-128.

Sommer, P. 2010. Forensic science standards in fast-changing environments. *Science and Justice 50*(1): 12-17.

Sommer, P. 2013. Written evidence submitted by Professor Peter Sommer [EC 14]. July, Home Affairs Committee. Accessed: 19/05/2018 https://publications.parliament.uk/pa/cm201314/cmselect/cmhaff/70/70we14.htm

Squires, P., 2015. Beyond contrasting traditions in policing research? In *Introduction to Policing Research*. London: Routledge. Pages: 9-28.

Sunde, N. and Dror, I.E., 2019. Cognitive and human factors in digital forensics: Problems, challenges, and the way forward. *Digital Investigation 29:*101-108.

Tully, G. 2018. *Annual Report November 2016 - November 2017.* Forensic Science Regulator. Accessed 15/09/2018 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/674761/FSRAnnual_Report_2017_v1_01.pdf

Van Beek, H.M.A., van Eijk, E.J., van Baar, R.B., Ugen, M., Bodde, J.N.C. and Siemelink, A.J., 2015. Digital forensics as a service: Game on. *Digital Investigation 15*: 20-38.

Vincze, E. 2016. Challenges in digital forensics. *Police Practice and Research* 17(2): 183-194.

[i] See https://www.swgde.org/ Accessed 1/10/ 2019.