DEEP: Extending the Digital Forensics Process Model for Criminal Investigations

The importance of high quality, reliable forensic analysis – an issue that is central to the delivery of justice - has become a topic for marked debate with scientists, specialists and government bodies calling for improved standards and procedures. At the same time, Law Enforcement agencies are under pressure to cut the cost of criminal investigations. The detrimental impact that this has had on all forensic disciplines has been noted internationally, with the UK’s House of Lords warning that if the trend continues, crimes could go unsolved and miscarriages of justice may increase. The pivotal role that digital forensics plays in investigating and solving modern crimes is widely acknowledged: in Britain, the police estimate it features in 90% of cases. In fact, today’s law enforcement officers play a key part in the recovery, handling and automated processing of digital devices yet they are often poorly trained to do so. They are also left to interpret outputs, with the results being presented in court. This, it is argued, is a dangerous anomaly and points to a significant gap in the current, four-stage digital forensics process model (DFPM). This paper presents an extension to that model, the Digital Evidence Enhanced Process (DEEP), with the aim of fine-tuning the mechanism and ensuring that all digital evidence is scrutinised by a qualified analyst.

Keywords: digital forensics, forensic science, evidence processing, knowledge management

Introduction

In the last ten years, no fewer than nine reports assessing the state of forensic science in England and Wales and offering recommendations to address the challenges have appeared. Two influential reports addressing similar issues have also been published in the United States. In Britain, concerns over the handling and disclosure of digital evidence by police became public three years ago after a number of rape trials collapsed and other sexual assault cases were dropped when it was discovered that vital information on mobile phones had either been missed or had not been entered in prosecution evidence. An enquiry into these and other failures was quickly organised by the House of Commons Justice committee with a range of specialist witnesses being called to give evidence. Among these was the Forensic Science Regulator (FSR), Dr Gillian Tully, who is tasked with regulating forensic science activities within the UK legal system. Following earlier testimony from a digital forensic practitioner pointing out that front-line police officers, with little or no training in digital forensics, were making interpretations of evidential outputs that then went before courts, the FSR agreed: ‘One of the big issues that I see… is that the digital forensics units are quite good at keeping up to date with technology for extracting data and making copies, but they then pass the copies, largely uninterpreted, to police officers, who are not experts and who are not digital forensics people. General policing investigators do not necessarily have
the tools to search that information effectively and understand it.’ She added that
digital forensics now pervades almost every aspect of policing. ‘Frontline officers
are doing all sorts of different types of what we would formerly have called digital
forensics, so there is an issue with how you get any form of control over
something that is so pervasive throughout all of policing.’

A later enquiry was held by the House of Lords’ Select Committee on Science
and Technology, which also heard oral evidence. During one session, the Head of
the Metropolitan Police’s Digital, Cyber and Communications Forensics Unit,
Mark Stokes, estimated that, including cases involving CCTV, communications
data, social media data and cyberattacks, around 90% of crime has a digital
element. He made an equally high estimate for most fraud, murder and complex
rape cases. Stokes described today’s police officers as ‘digital natives’ who could
use social media and current technology but they did not know the constraints and
limitations of that technology. He acknowledged that: ‘Training on what should
be seized and how it should be handled is absolutely critical and there is a lack of
that.’ A core part of police training should be around the digital world, he added.

Enquiries by both houses of Parliament concluded that urgent reforms were
necessary. A report from the House of Commons Justice Committee stated:
‘It is clear, from the evidence that we have heard, that the growth in digital
material presents a challenge to police and prosecutors. We believe that police
forces are not always adequately equipped or properly trained to handle the type
and volume of evidence that they now routinely collect and that this can lead to
errors when reviewing and disclosing material and therefore has the potential to
lead to miscarriages of justice.’

A report from the House of Lords gave the forceful view that all forensic
science in the UK ‘is in a state of crisis’ due to an absence of high-level leadership,
a lack of funding and an insufficient level of research and development. It warned:
‘The delivery of justice depends on the integrity and accuracy of forensic science
evidence and the trust that society has in it.’

Although the House of Lords has highlighted the danger posed to justice by
inadequacies in forensic science in general and the House of Commons has done
the same in respect of digital forensics in particular, no call has been made by
these or other authorities to stop or alter the current practice of allowing regular
police officers to either perform forensic procedures on digital devices or to
attempt to interpret the outputs. Law enforcement agencies have been subject to
severe budget cuts over a number of years, leading to a lack of resources and
appropriately trained personnel. Extending the remit of front-line officers into the
performance of specialist tasks can be seen as one of many cost-cutting exercises.
The authors do not believe that this situation is acceptable but it is what currently
exists and, given the financial climate, what is likely to persist. A solution is
clearly necessary if the cause of justice is to be better served. A step towards
finding that solution, we suggest, is to implement a more informed method of
processing digital evidence.
Discussion

Digital Evidence: The Need for Accurate Analysis

The findings made by both the House of Commons and House of Lords confirm and validate the opinions expressed by practitioners and academics in the field of digital forensics. Stressing the potential impact on a person’s livelihood or liberty, Casey et al. (2018) asserted that the ability to interpret digital evidence accurately is crucial in order to ‘avoid mistakes, missed opportunities, misinterpretations and miscarriages of justice.’ Similar points have been made by Collie (2018), who commented, ‘Digital forensics is meant to be based on science, not supposition… And in every case, somebody’s freedom is at stake.’ Both Casey and Collie have raised concerns over the handling of digital devices by police with minimal training.

‘Typically, police with limited digital forensic expertise have the initial responsibility to recognize sources of digital traces and to apply basic preservation and processing methods. They are at high risk of not realizing limitations in the methods and tools that are available to them, leading to mistakes and missed opportunities.’ Casey (2019) says, adding that this is due to ‘gaps in knowledge’. The risk continues to increase because of the ‘dynamic nature of cybercrime and technology.’

Collie (2018) has highlighted the every-day situation in the UK, where a suspect’s mobile phone is frequently given to a police officer with minimal training to perform a download. The results from the forensic tool used for the extraction, ‘will be handed to someone with even less or, more likely, absolutely nil training in digital forensics: the Officer In Charge of the case (OIC). S/he will look at the outputs… whatever they make of it will go before the court.’

Shaw and Browne (2013) have also drawn attention to the risks involved when inadequately trained personnel perform a ‘technical’ triage i.e. use a commercial forensic tool to target potential evidential data on some digital device. One danger is that the resulting outputs may easily be misinterpreted. Reviewing outputs from this type of automated process requires a ‘fairly high degree of knowledge and experience of digital forensics.’, the authors say. However, the focus of their research is the development of an enhanced previewing system since they assert, given the vast amount of data that is now typically submitted for examination, that the primary concern of the digital forensics community is that evidential data may be overlooked if some exhibits are excluded.

The use of enhanced previewing to assist decision making when assessing exhibits has been considered by James and Gladyshev (2013), too, and found effective. The authors examined the accuracy of forensic examiners’ personal choices when including or excluding exhibits, which were based on experience, as well as the accuracy of automated tools. Overill et al. (2013) have further proposed developing triage template pipelines as a way of narrowing down the volume of data needing full forensic examination. The approaches discussed above are based primarily on improving efficiency rather than quality.
Screening seized devices for the existence of relevant evidence constitutes survey or triage for some authorities and preliminary forensic examination for others. Indeed, the very meaning of the word ‘triage’ has been a matter for debate. In this paper, we follow Casey et al. (2013) in defining the triage process as the: ‘early extraction of information from digital evidence sources.’ Casey et al. also stress the importance of promoting efficiency throughout a whole digital forensic investigation. This means making the most of limited resources, giving support for key decisions at key points and increasing the quality of findings – all aspirations that we aim towards with our proposed model.

Confirmation Bias

As Shaw and Browne (2013) observed, there is a propensity to misinterpret data when inadequately trained personnel try to interpret outputs from digital forensic downloads. Collie (2018), too, has pointed out that an OIC may choose to stress certain aspects of evidence above others if they appear to be useful to the case in hand. One example of an OIC ‘cherry picking’ particular words from web browsing outputs from a mobile phone in support of a criminal charge and also confusing browsing results with user search results was related by Collie to the House of Commons’ Justice Committee.

The risk of confirmation bias has also been raised by Casey (2018) who commented: ‘When forensic examiners concentrate on proving or disproving a specific claim, there can be a risk of confirmatory bias. To mitigate the risk, an increasing number of best practice guidelines are instructing forensic practitioners to evaluate the probability of evidence given on claim versus a given alternative claim.’

Casey (2019) again remarked that: ‘Roles, responsibilities, rewards, plus selection, training and culture all have a major influence on the objectivity of investigators and forensic specialists.’ Adding: ‘Without formalized independence of digital forensics in the investigative process, it is difficult to maintain scientific objectivity of the results.’

Sunde and Dror (2019) have further emphasised the issue of cognitive bias as a source of error in digital forensics. Extensive research has shown that forensics experts are susceptible to bias when making decisions, they report, advocating that practitioners should test and eliminate multiple and preferably competing hypotheses when conducting examinations. This injunction echoes the recommendation made in the FSR’s codes of practice and conduct (2016), that alternative hypotheses should be considered when analyzing cell site evidence.

Sunde and Dror conclude that bias cannot be totally eliminated but procedures to uncover cognitive or human errors are necessary. One means of achieving this would be to have forensic advisors involved throughout the investigative process, as Casey (2019) suggests. This is an issue which we also seek to address since the model we propose aims to maximise input from qualified examiners during the existing triage process.

Citing the problems identified by these and other authors, Horsman (2019) has noted that there is a lack of dedicated research and formalisation of
investigative decision-making models to support digital forensic practitioners. He has proposed a framework designed to help practitioners at all levels to assess the reliability of their ‘inferences, assumptions and conclusions’. Whilst taking numerous aspects of the decision-making process and quality management into account, the model is very complex. It also does not address the immediate problems faced by front-line law enforcement officers in handling and assessing digital evidence. The present paper suggests that the existing four-stage DRPM should be extended to include a routine that improves the model currently employed by law enforcement (LE) when processing digital evidence and helps ensure that data outputs and any deductions drawn from them are checked by a qualified analyst before being presented in a statement or report for court. In the proposed model, both the interpretation of data, i.e. understanding what events occurred and the evaluation of data, whether qualitative or quantitative, is taken to be carried out by a digital forensic examiner. The choice of evaluation methodology is a point for further research and debate and falls outside the remit of this paper.

**Digital Forensic Processing - Best Practice, Triage and Current Model**

Best-practice methods for collecting and securing digital devices have been laid out in numerous guides, the majority produced by LE and government agencies. These include the well-known Association of Chief Police Officers (ACPO) guidelines, first published in 1999 and last updated in 2012. In common with other published guides in this subject area, for example, First Responder reference works published by the U.S. Department of Justice (2008) and the U.S. Secret Service (2009), the ACPO guidelines are primarily aimed at serving officers but are also taken to apply to investigators and practitioners of digital forensics in the private sector. Most of the guides written for LE agencies do not cover the subsequent analysis of data, although the 2012 version of the ACPO guide does contain a brief section, giving views on who should carry out digital forensic analysis and the need for that analysis to be properly targeted towards gathering evidence relevant to the case in hand.

The four aims of the digital forensic process, as identified from these guides and in order of importance are to:

1. Identify the evidence
2. Preserve the evidence
3. Recover the evidence
4. Present the evidence

In the above context, ‘Identify’ is taken to mean ‘know where digital evidence is likely to reside’ i.e., on a computer, mobile phone, tablet, etc. In a business-oriented rendering, von Solms et al. (2006) have listed the four key activities of the digital forensic process as:
1. Securing the evidence without contaminating it.
2. Acquiring the evidence without altering or damaging the original.
3. Authenticating that the recovered evidence is the same as the original seized data.
4. Analysing the data without modifying it.

A visual encapsulation of the commonly employed LE process is given in Figure 1. This is the model which we suggest should be modified and enhanced.

**Figure 1. The DFPM, Current LE Model**

Towards an Enhanced DFPM - Triage

In some crime-related investigations, police officers are tasked with carrying out the first two parts of this process, namely: identifying devices of potential evidential interest and preserving them. In others, particularly those involving mobile phones, they can be tasked with the first three parts of the process, an additional job being to recover data from a digital device. The model can be developed to show this, as in Figure 2.

**Figure 2. The DFPM, Embellished**

It should be noted that an investigating officer may either hand on a device such as a mobile phone to another officer, one who has received some training in recovering data using a ‘kiosk’ forensic solution, or may be trained to do so him/herself. In an alternative scenario, usually where computer equipment is seized, the device will go to a person properly trained to image the equipment. A digital forensic analyst will then examine the image and produce a brief report of findings known as a Streamlined Forensic Report (SFR). The investigating officer
may then use an automated, proprietary forensic tool on the image to look at specific activity e.g. web-browsing.

Whichever is the case, as has been discussed in the background and introduction, we suggest that a gap occurs here in the DFPM, between the last two stages. That gap, we term ‘Process’ and produce a further model to illustrate in Figure 3.

**Figure 3. An Enhanced, Five-Stage DFPM (EDFPM)**

Using this new five-stage model, the current method of working used by LE and discussed above, can be rendered as in Figure 4. In this illustration, ‘Officer 1’ may be the investigating officer or an officer trained to recover data using a kiosk solution. Once a data download from a mobile phone is obtained, any results gained are passed to the Officer in Charge of the case (OIC). Thus, a knowledge gap occurs because, in the case of mobile phones, a qualified analyst may never see any outputs from the device before an attempt at interpretation is made. With computers, a knowledge gap occurs because a qualified analyst carries out only a brief examination of the data and produces an SFR. This short, undetailed report of findings, goes to the OIC who tries to draw inferences from it. An SFR is intended to be for the information of both the OIC, to decide if there is enough evidence to support the charge made, and the solicitor for the Defence, to decide whether the evidence should be challenged or whether the defendant should be advised to enter a Guilty plea. An SFR is not intended to go before a court unless the findings are agreed.

**Figure 4. Current LE Processing Method: the knowledge gap**
The DEEP Processing Model

This section introduces a model for DF processing which has been derived from assimilating and analysing the research literature discussed in this paper and by considering the system that currently exists, as used by LE in the UK. The model is a Digital Evidence Enhanced Process (DEEP). The model fits into the enhanced DFPM, illustrated in Figure 3, at our suggested new fourth stage, the Process stage (Figure 5). It replaces the method illustrated in Figure 4, and aims to fill the knowledge gap that occurs when an OIC untrained in digital forensics is passed a) outputs from an automated download or b) an SFR, by making sure that data of potential evidential interest is seen and interpreted by a trained DF analyst before being passed to an OIC. Where a trained analyst decides that the outputs gained are sufficient to make an informed report in the light of the enquiry, a simple path is followed. Where an analyst decides that the outputs are not sufficient to support an informed report, a loop occurs in which s/he goes back to the original data. At this point, it may be that further analysis allows an enhanced interpretation of the original findings to be made. Alternatively, new findings that require deeper analysis may be made. A report is produced when the outputs relevant to the enquiry are sufficiently explained.

Figure 5. DEEP – where it Fits in the EDRPM
Summary and Conclusion

The use of forensic science in the criminal justice system has reached crisis point. This applies to all disciplines but the spotlight has fallen on digital forensics in particular in the past two years. In the UK, concerns have been raised over the
handling and disclosure of digital evidence by LE and, in several well-publicised
instances, court cases have been stopped or dropped as a result of failures in the
system. Enquiries have been conducted by both the House of Commons and
House of Lords, both of which identified a lack of high quality and robust analysis,
with a consequent detrimental impact on justice, and called for urgent change.

Digital forensics plays a central role in the detection and solving of crimes.
At the fore-front of the detection process, tasked with the recovery of devices that
may contain data of evidential interest, are today’s law enforcement officers.
Increasingly, where mobile phones are concerned, these devices are passed to
officers with little or no training in digital forensics for download. The resulting
output reports are passed to other untrained officers. While computers are
normally imaged and analysed by specialists, only brief findings are passed on to
investigators. As a result of this anomaly, authorities in digital forensics have
explained, mistakes and misinterpretations are made, potentially leading to
miscarriages of justice. At the heart of it is a knowledge gap that needs to be
filled.

A four stage DFPM model has previously been used to encapsulate the aims
of the digital forensic process. This paper suggests that a fifth stage is necessary.
This stage slots into the existing DFPM model at the point where investigating
officers put digital devices into forensic processing. The current LE modus
operandi is modelled in order to identify where knowledge gaps occur. A new
model, DEEP, is proposed with the aim of improving and enhancing the LE
process by ensuring that data of potential evidential interest is seen and interpreted
by a trained DF analyst before being passed to an OIC.

References

Casey, E., 2019: The chequered past and risky future of digital forensics, Australian
10, 138 – 147.
Sci. Int. 289, 154 – 155. DOI: 10.1016/j.forsciint.2018.05.014
Forensic Science Regulator, Annual Report November 2015–November 2016 (6 January
2017): Available from:
Horsman, G., 2019. Formalising investigative decision making in digital forensics:
Proposing the Digital Evidence Reporting and Decision Support (DERDS)
173–217. Available from:
http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/justicecommittee/disclosure-of-evidence-in-criminal-cases/oral/83096.html#Panel1
May, 2019.


Bibliography


Science and Technology Committee, Biometrics strategy and forensic services (Fifth Report, Session 2017–19, HC 800); October, 2019.