DEEP: Extending the Digital Forensics Process Model for Criminal Investigations

Athens Journal of Sciences- Volume 7, Issue 4, December 2020 – Pages 225-240

DEEP: Extending the Digital Forensics Process Model for Criminal Investigations

By Jan Collie[*] & Richard E Overill[±]

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 digital forensics analyst. The consequence of adopting DEEP in actual criminal investigations will be to ensure that all digital evidence is analysed and evaluated to the highest professional and technical competency standards, resulting in the enhanced reliability of digital evidence presented in court which will serve the cause of justice in terms of reduced instances of associated unsafe convictions and/or unjustified exculpations.

Keywords: *Digital forensics, forensic science, evidence processing, knowledge management*

Introduction

In the last ten years, no fewer than eight reports assessing the state of forensic science in England and Wales and offering recommendations to address the challenges have appeared (Tully 2015, 2018, 2019, Government Office for Science 2015, Science and Technology Committee 2011, 2013, 2018a, The Law Commission 2011). Two influential reports addressing similar issues have also been published in the United States (Committee on Identifying the Needs of the Forensic Science Community 2016, Executive Office of the President 2016). 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

[*] Lecturer, The Open University, UK.
[±] Visiting Senior Research Fellow, Department of Informatics, King's College London, UK.

https://doi.org/10.30958/ajs.7-4-3 doi=10.30958/ajs.7-4-3

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 (Guardian 2019). 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 (Justice Committee 2018). Among these was the Forensic Science Regulator (FSR), Dr Gillian Tully, who is tasked with regulating forensic science activities within the UK legal system (Tully 2017). 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 (Science and Technology Committee 2018b). 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" (Justice Committee 2018).

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" (Science and Technology Committee 2019).

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 nevertheless what currently exists and, given the current 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 achieving that solution, we suggest, is to implement a more informed method of processing digital evidence.

Literature Review

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. (2013) 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 (2019) 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 DFPM 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 guidelines and in order of importance are to:

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

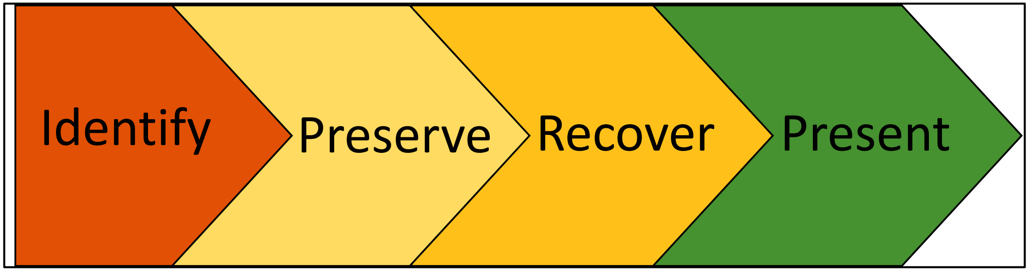
In the above context, "Identify" is taken to mean "know where digital evidence is likely to reside", i.e., on a computer, mobile phone, tablet, etc.

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

Figure 1. *The DFPM (the Current LE Model)*



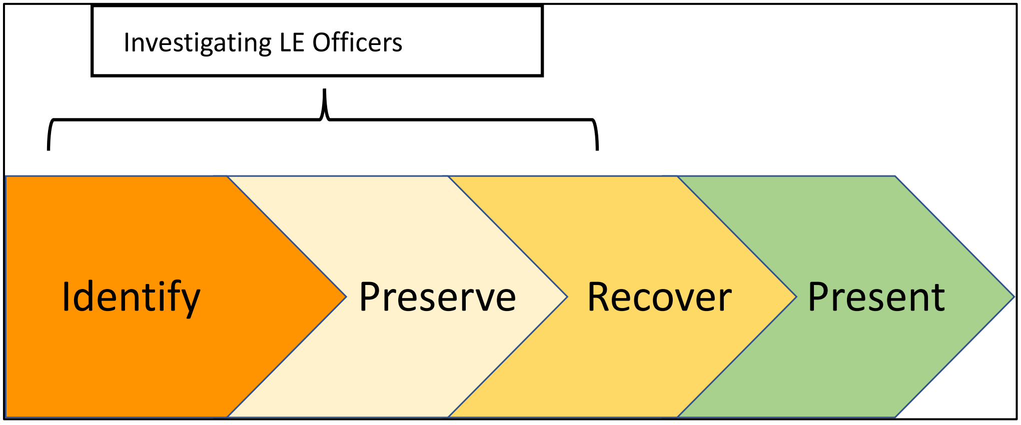
Methodology

In this section we demonstrate the methodological development of the DFPM into DEEP in a series of evolutionary steps.

Embellished DFPM

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, the additional task being to recover data from a digital device. The DFPM can be developed to include this feature, as shown in Figure 2.

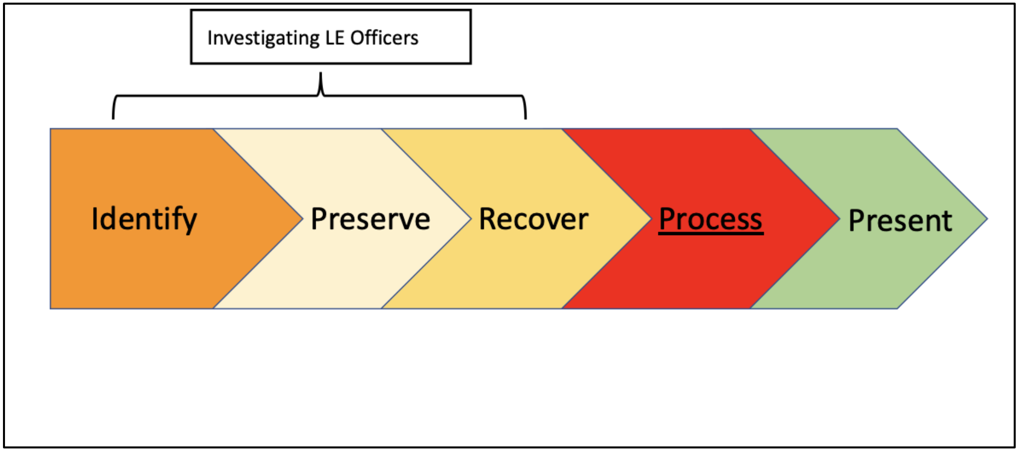
Figure 2. *The DFPM (Embellished)*



It should be noted here that an investigating officer may either hand on a device (such as a mobile phone) to another officer who has received some training in recovering data using a "kiosk" forensic solution, or they may have been trained to do this themselves. In an alternative scenario, usually one where computer equipment is seized, the device will be passed to a person who is properly trained to digitally 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 for specific activity, e.g., web-browsing.

Whichever is the case, as has been discussed in the proceeding sections, we suggest that a logical knowledge gap occurs at this point in the DFPM, between the final two stages. We label that gap "Process" and generate an enhanced model (EDPM), illustrating this in Figure 3.

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



Enhanced DFPM

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 between the prosecution and the defence sides.

Figure 4. *Current LE Processing Method: The Knowledge Gap*

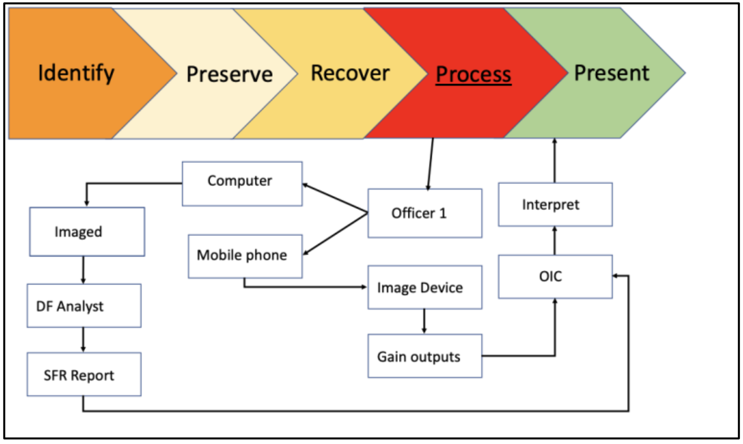


Figure 5. *DEEP – Its Location in the EDFPM*

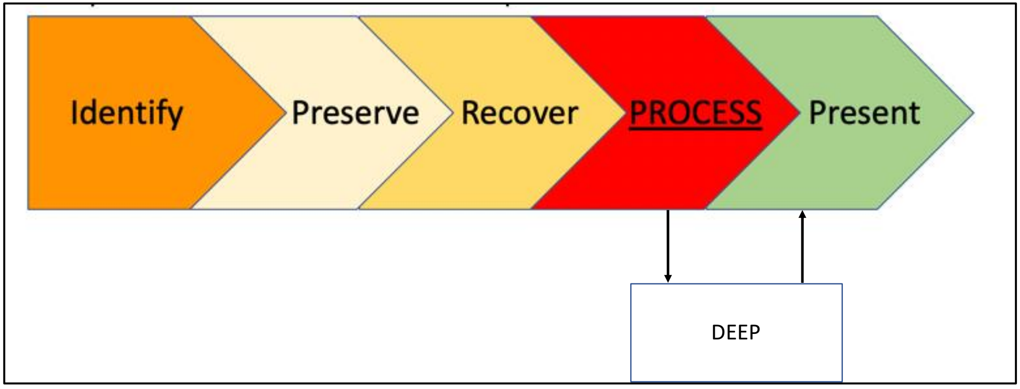
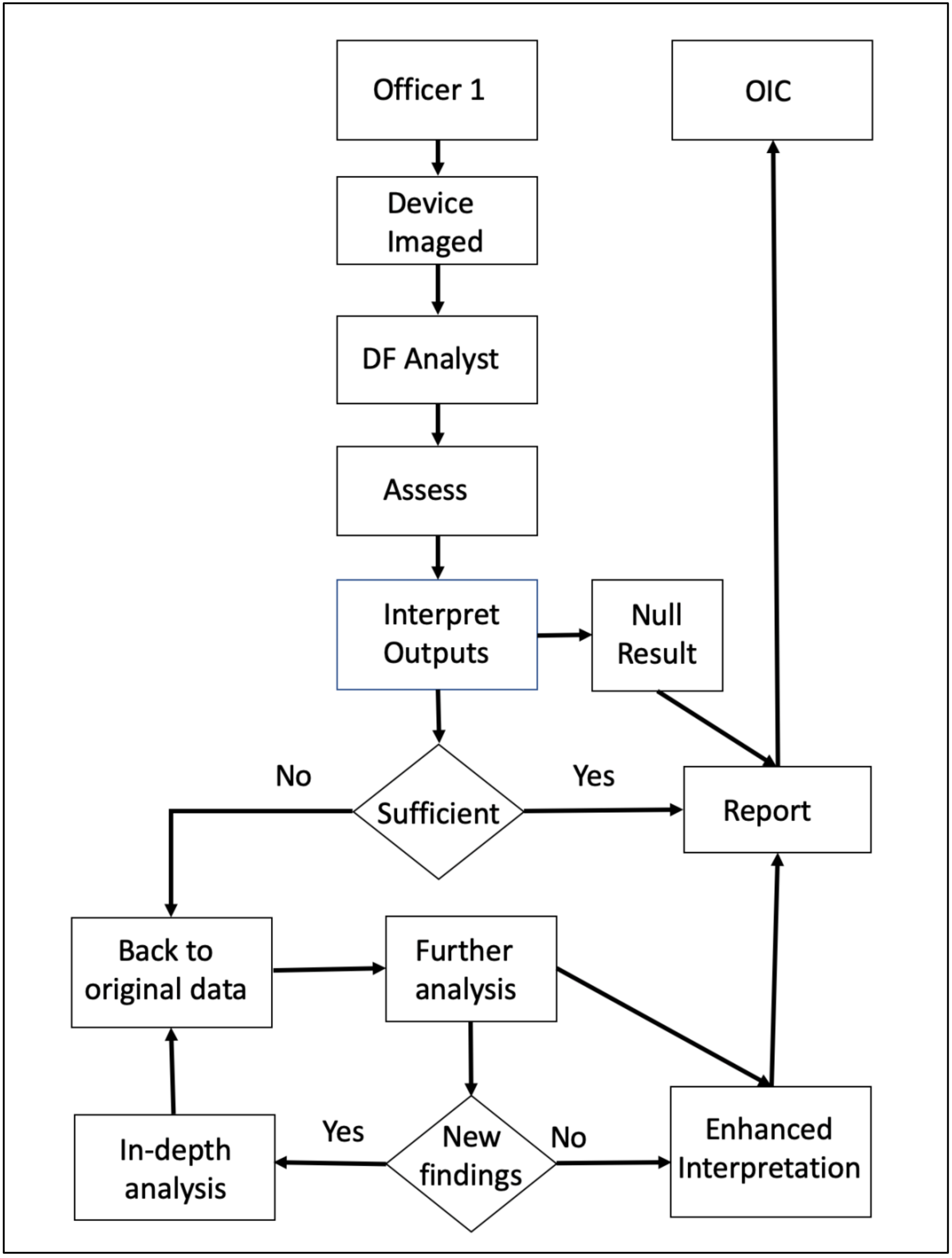


Figure 6. *DEEP – The Digital Evidence Enhanced Model*



Digital Evidence Enhanced Process (DEEP)

We now introduce a model for DF processing which has been derived from assimilating and analysing the research literature discussed earlier in this paper and by considering the system that is currently in used by LE in the UK. The model is termed Digital Evidence Enhanced Process (DEEP), and fits into the enhanced five-stage EDFPM, illustrated in Figure 3, at our proposed new fourth (Process) stage (see Figure 5). It replaces the method illustrated in Figure 4 with that shown in Figure 6, 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 ensuring that data of potential evidential interest is scrutinised and interpreted by a trained DF analyst before being passed to an OIC. When a trained DF analyst decides that the outputs acquired so far are sufficiently convincing to make an informed report in the light of the current enquiry, a straightforward path is followed. However, if the trained DF analyst decides that the currently available outputs are insufficient to support an informed report, a loop is entered in which the analyst goes back to the original data. At this point, it may be the case that further analysis of the original data allows an enhanced interpretation of the original findings to be made. Alternatively, new findings that require further in-depth analysis may be made. A report is produced once all the outputs relevant to the enquiry are sufficiently well explained. Note that, although the title "DF Analyst" appears explicitly only once in Figure 6, it is in fact implicit in the DEEP model that the DF analyst is also involved in the whole of the cycle that is concerned with returning to the original data for further analysis.

Results and Discussion

In this section we demonstrate how our proposed DEEP model operates in a typical scenario based on an actual criminal case with which one of the authors was professionally involved as a digital forensic investigator, in order to display its advantages over the DFPM. This case study provides an illustrative validation of the merits of DEEP over the DFPM.

Typical crime scene scenario: a police officer arrests a suspect at the scene of a crime. The suspect is carrying one phone which the officer takes into custody. Later, at the police station, the officer connects the phone to a "kiosk" facility, which contains the necessary hardware and software to:

a) Obtain a data dump from the phone.
b) Interrogate the data and filter it into categories e.g., messages, web browsing history.
c) Run a keyword search across the data.

The first officer completes steps a) and b) and then gives the outputs from the initial interrogation to the OIC. Using the same software tool as the first officer, the OIC runs a keyword search across the data set. Evidence of potential interest to the enquiry is found in web browsing outputs. This consists of pornographic words and phrases.

The offence that the suspect has been arrested in connection with relates to a claim of child abuse, brought to police attention by the mother and involving a child of the suspect’s family. The OIC has seen words and phrases that suggest both an interest in indecent images of children and an interest in incestuous relationships. The OIC has seen words and phrases that suggest both an interest in indecent images of children and an interest in incestuous relationships. Between 10 to 12 words suggestive of the suspected offence have been found in the majority of rows of a table of outputs produced by the forensic software tool used. The OIC concludes that these are search terms that have been entered into the web browser by the suspect and writes a report for court to that effect.

If the loop stops here, as happens in the existing processing model, the OIC's report goes before the court without further question with the high likelihood of a conviction being handed down by the judge and jury.

If, as in the DEEP model, the phone data dump is passed to a digital forensic analyst to assess and a proper interpretation of the outputs is made at this stage, it will be discovered that the web browser artefacts are not actually search terms but keywords picked up by the browser from the descriptions of content that is hidden in the webpage's HTML code. The keywords are associated with video loop click-throughs that are sited on the pornography web site's main page. These would lead to full-length video content if a user clicked on the links. However, the video loop shorts are content that runs automatically when a user lands on the web site, the user does not actively choose to view the content unless they click the associated link. Furthermore, the keywords associated with the content do not reflect the particular search terms entered by the user into the browser before landing on the pornography website's main page. These findings have important legal implications.

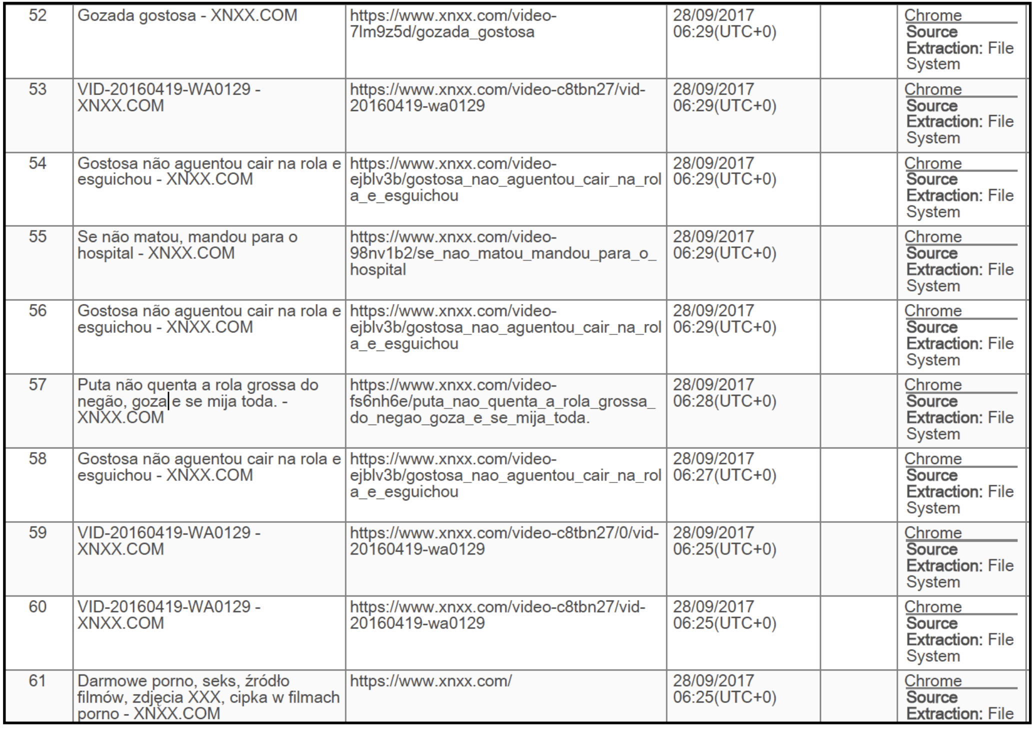
The value of DEEP is further demonstrated when other outputs from the illustrative case used in the above case study are considered.

Figure 7 below is a sample of data which consists of outputs from web browsing activity which has taken place on a mobile phone. It will be seen that the final column contains the source of the data and the third column to the left contains dates and times. Both are revealing to the digital forensic analyst. In this instance, the source is the Chrome browser installed on the mobile phone. Reading from the top down, the dates for the top four outputs (numbered 52–56 in the far left hand column) are all the same, the next recorded time is 1 second earlier, the next recorded time one second before that and the final three times, two seconds before that. What this tells a trained analyst is that this is not browsing activity carried out by the user of the mobile phone –clearly, no one can type an entire phrase in one to two seconds– but system activity which occurs automatically in the background.

Compare the foregoing with Figure 8 below, where the source (final column) is again the Chrome browser. However, the marking 'synced data' will be seen. This means that the activity concerned did not occur on the mobile phone in question but on some other device which synchronises with a shared cloud-based service. Thus, it cannot be said that the device user carried out this activity. It can also be seen that the dates and times, in the third column to the left, vary, in a pattern which is indicative of normal user activity.

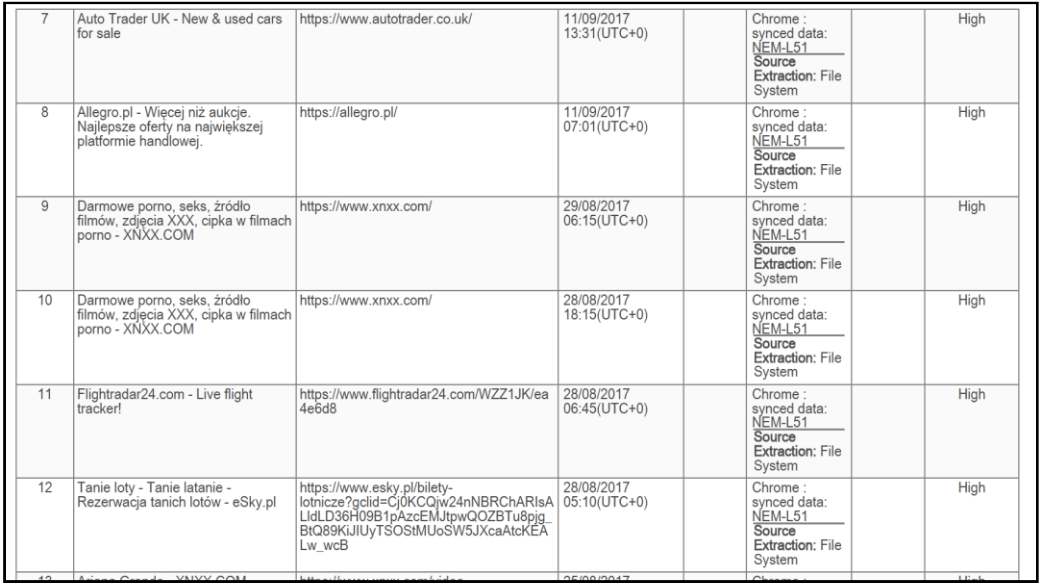
(Note that Figures 7 and 8 contain words and phrases of a sexual nature which some readers may find offensive).

Figure 7. *Initial Analysis*



52	Gozada gostosa - XNXX.COM	https://www.xnxx.com/video-7lm9z5d/gozada_gostosa	28/09/2017 06:29(UTC+0)		Chrome **Source Extraction:** File System
53	VID-20160419-WA0129 - XNXX.COM	https://www.xnxx.com/video-c8tbn27/vid-20160419-wa0129	28/09/2017 06:29(UTC+0)		Chrome **Source Extraction:** File System
54	Gostosa não aguentou cair na rola e esguichou - XNXX.COM	https://www.xnxx.com/video-ejblv3b/gostosa_nao_aguentou_cair_na_rola_e_esguichou	28/09/2017 06:29(UTC+0)		Chrome **Source Extraction:** File System
55	Se não matou, mandou para o hospital - XNXX.COM	https://www.xnxx.com/video-98nv1b2/se_nao_matou_mandou_para_o_hospital	28/09/2017 06:29(UTC+0)		Chrome **Source Extraction:** File System
56	Gostosa não aguentou cair na rola e esguichou - XNXX.COM	https://www.xnxx.com/video-ejblv3b/gostosa_nao_aguentou_cair_na_rola_e_esguichou	28/09/2017 06:29(UTC+0)		Chrome **Source Extraction:** File System
57	Puta não quenta a rola grossa do negão, goza e se mija toda. - XNXX.COM	https://www.xnxx.com/video-fs6nh6e/puta_nao_quenta_a_rola_grossa_do_negao_goza_e_se_mija_toda.	28/09/2017 06:28(UTC+0)		Chrome **Source Extraction:** File System
58	Gostosa não aguentou cair na rola e esguichou - XNXX.COM	https://www.xnxx.com/video-ejblv3b/gostosa_nao_aguentou_cair_na_rola_e_esguichou	28/09/2017 06:27(UTC+0)		Chrome **Source Extraction:** File System
59	VID-20160419-WA0129 - XNXX.COM	https://www.xnxx.com/video-c8tbn27/0/vid-20160419-wa0129	28/09/2017 06:25(UTC+0)		Chrome **Source Extraction:** File System
60	VID-20160419-WA0129 - XNXX.COM	https://www.xnxx.com/video-c8tbn27/vid-20160419-wa0129	28/09/2017 06:25(UTC+0)		Chrome **Source Extraction:** File System
61	Darmowe porno, seks, źródło filmów, zdjęcia XXX, cipka w filmach porno - XNXX.COM	https://www.xnxx.com/	28/09/2017 06:25(UTC+0)		Chrome **Source Extraction:** File

Figure 8. *In-Depth Analysis*



7	Auto Trader UK - New & used cars for sale	https://www.autotrader.co.uk/	11/09/2017 13:31(UTC+0)		Chrome : synced data: NEM-L51 **Source Extraction:** File System		High
8	Allegro.pl - Więcej niż aukcje. Najlepsze oferty na największej platformie handlowej.	https://allegro.pl/	11/09/2017 07:01(UTC+0)		Chrome : synced data: NEM-L51 **Source Extraction:** File System		High
9	Darmowe porno, seks, źródło filmów, zdjęcia XXX, cipka w filmach porno - XNXX.COM	https://www.xnxx.com/	29/08/2017 06:15(UTC+0)		Chrome : synced data: NEM-L51 **Source Extraction:** File System		High
10	Darmowe porno, seks, źródło filmów, zdjęcia XXX, cipka w filmach porno - XNXX.COM	https://www.xnxx.com/	28/08/2017 18:15(UTC+0)		Chrome : synced data: NEM-L51 **Source Extraction:** File System		High
11	Flightradar24.com - Live flight tracker!	https://www.flightradar24.com/WZZ1JK/ea4e6d8	28/08/2017 06:45(UTC+0)		Chrome : synced data: NEM-L51 **Source Extraction:** File System		High
12	Tanie loty - Tanie latanie - Rezerwacja tanich lotów - eSky.pl	https://www.esky.pl/bilety-lotnicze?gclid=Cj0KCQjw24nNBRChARIsALldLD36H09B1pAzcEMJtpwQOZBTu8pjg_BtQ89KiJIUyTSOStMUoSW5JXcaAtcKEALw_wcB	28/08/2017 05:10(UTC+0)		Chrome : synced data: NEM-L51 **Source Extraction:** File System		High
13	Ariana Grande - XNXX.COM	https://www.xnxx.com/video-	25/08/2017		Chrome :		High

Summary and Conclusions

The application of forensic science in the criminal justice system has reached a crisis point. This applies to all forensic disciplines, but the spotlight has fallen on digital forensics in particular during 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 the 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 improvements.

Digital forensics plays a central role in the detection, investigation 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 on 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 highlighted that mistakes and misinterpretations are made, potentially leading to miscarriages of justice. At the heart of this anomaly 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 proposes 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 both seen and interpreted by a trained DF analyst before being passed to an OIC.

The DEEP model has been carefully validated using a typical real-world crime scenario drawn from an actual digital forensic investigation conducted by one of the authors, and has been demonstrated to enable additional digital evidence to be uncovered whose evaluation and interpretation significantly changes the view of the case. Our contention is therefore that if DEEP were to be routinely in operation during criminal investigations, the risk of miscarriages of justice (both unsafe convictions and unjustified exculpations) would be reduced and the cause of justice served.

References

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

Casey E (2018) Clearly conveying digital forensic results. *Digital Investigation* 24(Mar): 1–3.

Casey E, Geradts Z, Nikkel B (2018) Transdisciplinary strategies for digital investigation challenges. *Digital Investigation* 25(Jun): 1–4.

Casey E (2019) The chequered past and risky future of digital forensics. *Australian Journal of Forensic Sciences* 51(2): 1–16.

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

Committee on Identifying the Needs of the Forensic Science Community (2016) *Strengthening forensic science in the United States: a path forward*. National Research Council of the National Academies. Retrieved from: https://www.ncjrs.gov/pdffiles1/nij/grants/228091.pdf. [Accessed May 2019].

Executive Office of the President (2016) *Forensic science in criminal courts: ensuring scientific validity of feature-comparison methods*. President's Council of Advisors on Science and Technology. Retrieved from: https://bit.ly/3gIPE3b. [Accessed October 2019].

Government Office for Science (2015) *Forensic science and beyond: authenticity, provenance and assurance, annual report of the government chief scientific adviser 2015*. Retrieved from: https://bit.ly/2ALZa6z. [Accessed October 2019].

Guardian Online (2018) *London rape trial collapses after phone images undermine case*. Retrieved from: https://bit.ly/2CnRgAw. [Accessed April 2019].

Horsman G (2019) Formalising investigative decision making in digital forensics: proposing the Digital Evidence Reporting and Decision Support (DERDS) framework. *Digital Investigation* 28(Mar): 146–151.

James JI, Gladyshev P (2013) A survey of digital forensic investigator decision processes and measurement of decisions based on enhanced preview. *Digital Investigation* 10(2): 148–157.

Justice Committee (2018) *Oral evidence: disclosure of evidence in criminal cases, HC859.* Questions 173–217. Retrieved from: https://bit.ly/2BMDaJl. [Accessed May 2019].

Overill RE, Silomon JAM, Roscoe KA (2013) Triage template pipelines in digital forensic investigations. *Digital Investigation* 10(2): 168-174.

Science and Technology Committee (2011) *The forensic science service*. Seventh Report, Session 2010–12, HC 855. Retrieved from: https://bit.ly/38N3oHt. [Accessed October 2019].

Science and Technology Committee (2013) *Forensic science*. Second Report, Session 2013–14, HC 610. Retrieved from: https://bit.ly/2ZfcoCd. [Accessed October 2019].

Science and Technology Committee (2018a) *Biometrics strategy and forensic services*. Fifth Report, Session 2017–19, HC 800. Retrieved from: https://bit.ly/3ehDLj4. [Accessed October 2019].

Science and Technology Committee (2018b) *Corrected oral evidence: forensic Science*. Questions 123–131. Retrieved from: https://bit.ly/38MrYse. [Accessed May 2019].

Science and Technology Committee (2019) *Forensic science and the criminal justice system: a blueprint for change*. Retrieved from: https://bit.ly/2ZgW3wN. [Accessed May 2019].

Shaw A, 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.

Sunde N, Dror IE (2019) Cognitive and human factors in digital forensics: problems, challenges, and the way forward. *Digital Investigation* 29(Jun): 101–108.

The Law Commission (2011) *The admissibility of expert evidence in criminal proceedings in England and Wales*. Consultation Paper No 190. Retrieved from: https://bit.ly/2Oe0OB4. [Accessed May 2019].

Tully G (2015) *Annual report November 2014–November 2015.* Forensic Science Regulator. Retrieved from: https://bit.ly/3fhBHJs. [Accessed October 2019].

Tully G (2017) *Annual report November 2015–November 2016.* Forensic Science Regulator. Retrieved from: https://bit.ly/3eghoe2. [Accessed May 2019].

Tully G (2018) *Annual report November 2016–November 2017*. Forensic Science Regulator Forensic Science Regulator. Retrieved from: https://bit.ly/38H6kFu. [Accessed October 2019].

Tully G (2019) *Annual report November 2017–November 2018*. Forensic Science Regulator. Retrieved from: https://bit.ly/3fbLO2i. [Accessed October 2019].

von Solms S, Louwrens C, Reekie C, Grobler T (2006) A control framework for digital forensics. In *Advances in Digital Forensics II, IFIP Advances in Information and Communication* 222, 343–355. Boston: Springer.