A preliminary assessment of latent fingerprint evidence damage on mobile device screens caused by digital forensic extractions

*Graeme Horsman; Helen Page; Peter Beveridge

School of Science, Engineering & Design,
Teesside University,
Middlesbrough,
North Yorkshire,
United Kingdom

Email: g.horsman@tees.ac.uk
Phone: 01642 738130

Abstract
Mobile devices continue to feature heavily in criminal investigations and often bear multiple forms of potentially relevant evidence. In the context of identifying the owner of a device, both latent fingerprints and resident digital data may be crucial to investigations, yet each individual process may have a detrimental impact on the other. Fingerprint development techniques are known to impact device hardware, whilst digital extraction processes can destroy latent prints. This article examines the impact of mobile device extraction procedures on resident screen fingerprints. The impact of bare fingered, cotton gloved, latex gloved and stylus screen press and swipes on latent print destruction are examined. Results indicate that all forms of interaction cause print damage, but to a variable extent. Provisional device handling recommendations are offered.

Keywords: Digital Forensics; Mobile Device Forensics; Fingerprints; Investigation; Crime

1 Introduction

Given the volume, diversity and complexity of modern day crime, many incidents require collaboration between sub-disciplines of forensic science in order to ensure that an effective investigation takes place. Frequently, there is the need to combine digital device analysis with what can be considered more traditional forms of forensic evidence identification and recovery, including DNA and fingerprints. Such recent examples in the United Kingdom (UK) include the examination of Closed-Circuit Television content and fingerprint analysis of relevant chattels at both the recent suspected arson at Nottingham's railway station (BBC News, 2018a) and the Hatton Garden heist (BBC News, 2017).

The need for, and requirements of, digital forensic (DF) evidence are influenced by both crime type and trends in device usage. Although crimes involving digital devices are difficult to quantify due to both direct and indirect involvement (sometimes termed cyber-dependant and cyber enabled (National Crime Agency, n.d.)), the UK Parliamentary Office of Science and Technology (2016) reports that now, digital evidence 'may be present in almost every crime'. When coupled with usage statistics, mobile devices now form a prominent potential evidentiary source in many criminal cases, as noted by the College of Policing (2016, p.7-8) where the acquisition of phone data is a frequent cause of investigation delays and other court-related concerns including disclosure (BBC News, 2018b). There are almost five billion mobile phone users worldwide (Statista, 2018a) with a reported 96% of individuals aged between 16 and 24 owning a mobile phone in the UK alone (Statista, 2018b). With such volumes of usage comes an inferred likelihood of mobile device involvement in various acts of crime, where in such instances the investigation of both resident internal digital data and forms of resident biological and fingerprint evidence may be required.

The type of offence and its surrounding circumstances will influence the forms of evidence recovery implemented within an investigation. An important first step in any investigation involves identifying the owner of any suspect device. In some cases this may be straightforward (for example, where a suspect acknowledges possession of a handset), however, a device which is located but detached from a suspect or victim poses a greater challenge. Whilst a device may hold masses of communication and connection data which may itself be attributable to a individual, accessing this content may take time (subject to laboratory backlogs and investigatory procedures), or in some cases a handset passcode may prevent access completely. As a result, resident fingerprint evidence may provide the only feasible, timely alternative for device identification purposes (BBC News, 2014a; 2014b; 2018c). Therefore at any one point in time, a single device may possess both fingerprint and digital evidence in need of acquisition and interpretation.

This article draws specific reference to the combined forensic practices of DF and fingerprint recovery and analysis, in the context of mobile device investigations. Whilst the collaborative workings between these two disciplines on a single device is in many cases valid, there exists the challenge of ensuring both forensic sciences have an opportunity to carry out their work effectively, acquiring any potentially relevant resident evidence without compromising the evidential opportunities of the other. In terms of fingerprint analysis, minimal disruption to a mobile device's surface is required in order to give maximum potential for print recovery. Yet some fingerprinting methods, for example aluminium powdering (despite being noted as best practice (see Section 2.1.4)), may be destructive, potentially compromising a device's hardware and subsequently any digital data extraction processes. Conversely, mobile device analysts handling and extracting a handset must often interact with it (via it's operating surface) in order to acquire and verify the internal digital content of the device. In this sense, fingerprinting and DF practices can conflict with one another.

Within this work, the impact of a mobile handset extraction on latent fingerprints is analysed. We consider the scenario where a DF practitioner interacts with a device using bare fingers, latex gloves, touch-screen cotton gloves with screen interaction fingertips and via a generic device stylus. Damage to latent prints is discussed with device handling recommendations for DF practitioners offered.

2 Device Handling Procedures

When a mobile device is discovered at the scene of a crime with a reasonable expectation of the device itself or content stored within it being relevant to an investigation, necessary forensic examination will take place. If both fingerprint and digital data associated with the device are deemed to be of relevance to an investigation, and assuming both sets of potential evidence coexist on and within the handset itself, establishing an '*order of investigation*' to ensure maximum evidence recovery is important. However, a lack of clear and definitive guidance on such matters regarding '*who goes first*' makes establishing a suitable protocol difficult, where influencing factors may include the following:

1. *Triage*: Procedural policies for the effective allocation of available resources (Horsman, 2014) may see a device enter a formal processing model, which ultimately determines the type of analysis a device receives first. Further, it is common practice in law enforcement agencies for non-technical officers to carry out a preliminary extraction of devices from 'kiosk-styled' examination pods in law enforcement agencies to identify the existence of any potential evidence regarding devices they have seized as part of an investigation. These processes may take place with little consideration of the application of fingerprint examination strategies.
2. *Crime prioritization*: Crime prioritization is often going to be a determining factor with regards to the order of investigation of a mobile device. In such instances, evidence deemed more relevant to solving or supporting an effective investigation is likely to take priority, potentially to the detriment of others. In addition, cases where the identification of the owner of a device is pertinent and a device is found in a locked state (with no access to the passcode), a fingerprint examination may be a more efficient means of establishing ownership given the existence of backlogs for device examination in many law enforcement and associated institutions (Quick and Choo, 2014; Scanlon, 2016; Scanlon et al., 2017). Although prioritization decisions are likely based on surrounding case circumstances they may not be effective in all cases, therefore consideration for the preservation of both evidence types is arguably necessary.
3. *Available expertise*: A device may receive a form of analysis based on the type of practitioner which first encounters said device. For example, a device found through a scene search which is carried out by DF experts may have digital evidence prioritized and undergo a digital device extraction first, or in some cases, without the consideration for FP evidence. In addition, a scene search or device seizure undertaken by a generic law enforcement officer (non-DF or fingerprint specialist), may result in variation of analysis prioritisation due to localised examination policies.
4. *An afterthought*: Ineffective planning may result in either form of evidence being considered as an afterthought of the other. In addition, subsequent case developments may require further device analysis for other forms of evidence which were not originally examined. Therefore a device which is deemed to first require DF analysis, with a subsequently initiated fingerprint examination, may have had any fingerprint evidence compromised by the DF procedures.

The issue lies with the potential for destruction to be caused by each procedure. This problem is summarised by Androulidakis (2016, p.79) who indicates that digital data extraction may destroy fingerprint evidence, whilst conversely, fingerprint procedures may disrupt the operation of a handset.

In relation to fingerprint recovery, whilst the position is unclear and subject to variables such as the make and model of a device, commentary suggests the use of metallic flake powders, such as aluminium, to recover prints should be prohibited due to the potential for damage being caused to the device (Girard, 2017). This concern has also been previously issued by the Association of Chief Police Officers (2007) in their 'Good Practice Guide for Computer-Based Electronic Evidence' and by Curran et al. (2010) and Casey (2011). Ballou (2010) acknowledges the need for both sources of evidence to be acquired, however they suggest that potentially destructive fingerprint evidence procedures should be second to digital extractions.

2.1 Existing Procedural Guidance

As previously noted, there is limited commentary available for establishing an effective '*order of play*' between fingerprint and digital device examination. Whilst comments surrounding damage may be valid, Murphy (2009) indicates that prevention of "contamination issues" is a key driver, however arguably this could be addressed via a DF practitioner having their fingerprints eliminated from any subsequent investigation. Whilst perhaps not helpful in terms of establishing a definitive solution, the Scientific Working Group on Digital Evidence (SWGDE) provide the following guidance.

> "*Occasionally, there may be a need to conduct traditional forensic processes on a mobile phone (e.g., DNA and latent prints). These are case dependent and should be discussed with the investigator about the need for such evidence as well as the order in which they should be performed. Contact appropriate lab personnel for guidance on processing order to avoid the destruction of forensic evidence.*" (SWGDE, 2013).

Such guidance is mirrored by the European Network of Forensic Science Institutes (2015) (ENFSI) who state.

> *If at the scene there is a likely requirement to work with other forensic departments, for example DNA or fingerprints, then the sequence of work should follow an agreed pre-defined sequence that is dependent on the importance and destructive nature of each forensic process.*

A lack of definitive guidance may lead to divergent examination processes occurring both at a local and international level. Such inconsistencies may lead to variations in the success rates of combined evidence recovery from mobile devices or in some cases, the unnecessary destruction of specific evidence types.

2.1 Damage

There is limited academic commentary available discussing both the robustness of fingerprint evidence during a DF extraction, and the impact of a DF extraction on latent prints on a device's screen. This work aims to address both points. In essence, the key factor for deliberation here is the 'order of evidence volatility', a concept typically associated with digital evidence collection (Brezinski and Killalea, 2002). One should consider that latent fingerprints may be subject to destruction via the extraction procedure itself or simply through handling the device.

2.1.1 Mobile Forensic Extraction Procedure

Mobile device examination is a sub-discipline of DF where procedures are difficult to standardise due to variances in handset makes and models, coupled with multiple operating system instances in operating. Practitioners are often wholly reliant on their forensic extraction software to communicate and extract resident data, with Figure 1 providing an overview of the typical analysis process.

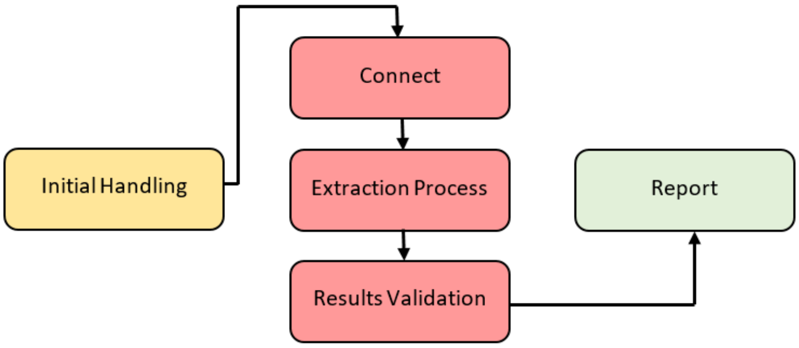

Figure 1: A High-level overview of a mobile forensic examination

Initial Handling: Initial handling is dependent on the context of a device's seizure and journey through an examination process. If a device has been seized onsite, it is subject to both the seizing officers handling and then handling of the examining DF practitioner once it is within the confines of the laboratory. Typically, devices are contained in protective packaging until they are removed at an examination station. Depending on the type of packaging employed it may, or may not, preserve the fingerprint evidence on the device. If seizure is carried out by those lacking knowledge of requisite packaging standards then additional latent print damage may occur. Rigid, non-porous objects such as the devices discussed here should ideally be packaged in a box if subsequent fingerprint examination is envisaged (Fisher and Fisher, 2012).

Localised policies for device seizure may also vary. If a device is found switched on, local practices may dictate that the device is turned off, preventing it from interacting further with outside communication networks whilst also preventing any remote wiping processes. If a first responder handles a device failing to consider latent fingerprints on a device screen, subsequent damage to fingerprints is likely to be caused.

Connect: Once in a laboratory environment (or examination environment if on-scene triage occurs), extraction of a device's digital content is required. Although in some instances non-cable extractions are possible (Bluetooth, Infrared etc.), in the case of most modern handsets, a cable connection is required. This requires various degrees of device handling and whilst a standard USB or equivalent charging/data cable can be connected without touching a device screen, it may not always be done in such a manner.

Extraction: Once a connection has been established, extraction can take place. The extraction process typically requires a practitioner to interact with a device's screen (to varying degrees, based on a handsets make/model and the extraction software in use) in order to configure and commence an extraction. The extraction process is often software wizard driven, but in many cases requires elements of device interaction and the placing of a handset into a certain '*state*' for data extraction. For example, a practitioner may have to enter a handset's passcode in order to get access to the device, navigate device menus, secure it from network connections (remove data/Wi-Fi connections to prevent remote wiping etc.), enable USB debugging and enable process dialog boxes for data extraction to take place (for example, in the case of iPhone devices, a 'trusted connection' may need initiating). All actions require screen contact, typically by hand or through the use of a compatible stylus device.

Results Validation: Once an extraction is complete, the practitioner has two options. First, they can take the results as ‘unverified’, power down the device and repackage it. In this instance, the practitioner is relying on the accurate interpretative quality of the analysis software where any further analysis takes place on the extracted data set. Arguably, this is unsafe practice, leaving a second option of ‘sampled verification’. In many investigation instances, it is unrealistic to validate every piece of extracted data from a handset, but sampling should take place in order to identify any information which may not have been acquired during the extraction process, or extracted with misrepresented metadata (for example, incorrect artefact time stamps). To provide an example, where 100 Short Message Service (SMS) have been extracted, good practice includes the sampling of messages on the handset to ensure the accuracy of an extraction, in terms of quantity of SMS in existence, and to verify that associated metadata is correctly reported. The results validation stage of an investigation has the potential to require a large volume of screen interaction and potential fingerprint destruction.

Extraction Point of Note: Where a handset cannot be extracted via forensic software, a live examination and recording of screen content may be the only implementable option. This method essentially explores the handset’s functionality and data as a main user would, via handset interaction. In this case, the implication of screen engagement for fingerprint recovery may be severe.

2.1.2 Device Handling

In almost all cases of device handling for the preservation of fingerprints, the subconscious actions of a practitioner must be considered. If they are aware of the need to subsequently fingerprint a device, then cautious methods of handling may be implemented. For example, the practitioner could specifically handle a device using methods which do not disturb the large, flat surface areas of a screen where latent and recoverable prints may reside. However the definition of ‘cautious handling’ is subjective and may vary between practitioners. Of concern is the lack of handling guidance available to DF practitioners and the impact this may have on personal protective equipment (PPE) usage.

Best practices for DF practitioners handling mobile exhibits in need of fingerprinting is sparse, typically resulting in the use of latex or cotton gloves by a practitioner. Such measures are often perceived as for the purposes of avoiding device contamination, preventing a practitioner’s prints from being placed on the device’s surface. In reality, this is of limited concern where a practitioner's fingerprints could easily be recorded and eliminated. The primary justification for the use of such measures by a DF practitioner is to either limit or prohibit the destruction of latent fingerprints. Whilst the rationale for gloved approaches is sound, at the time of writing there is no available research in relation to this. As a result, an inference merely exists that the acts of touching the screen by a DF practitioner will likely result in evidence damage, given that fingerprints on smooth surfaces such as glass are typically vulnerable to damage (European Network of Forensic Science Institutes, 2015b).

2.1.3 Damage to the Handset

The discipline operates under the inference that the application of any fingerprint powder to a device creates a risk of damage to internal hardware and functionality if powder ingress occurs. This issue is particularly pertinent where magnetic powders are utilised. However, this should be considered against developments in modern handset technology. Mobile devices are now constructed typically using enclosed cases where the battery compartment can no longer be opened (see for example, Apple and Samsung Galaxy handsets). These have limited points of entry, except for (typically) charging, earphone and speaker entry points which compromise the structure of a case.

2.1.4 Fingerprint Recovery

The majority of mobile phone devices are comprised of one of nine different types of Gorilla® Glass screen (Corning, 2018), including the Apple iPhone which has been manufactured with a Gorilla® Glass screen since 2007 (Apple, 2017). The glass is surrounded by a thin metal strip, which acts as an antenna, and the phone exterior/back tends to be composed of plastic, in either rough, matt or high-gloss finishes.

According to the Fingerprint Visualisation Manual (CAST, 2014), the glass screen of a mobile device is categorised as 'Glass and Ceramics' of the 'non-porous' surfaces. After a visual examination, the cheapest and easiest process for the recovery of fingerprint evidence from this surface type is undertaken with the use of powders, usually aluminium powder. A smooth plastic phone casing, considered as a 'Rigid Plastic', would have fingerprints recovered in the same way. However, depending on the extent of the grain of a rough or matt plastic, powders may prove to be ineffective and vacuum metal deposition or superglue treatment may well be the technique of choice.

Powders will adhere to the aqueous component of fresh fingerprints and to the fatty deposits of sebaceous sweat in older prints where the water has evaporated. Vacuum metal deposition, a highly sensitive technique, relies on the layering of gold deposits, followed by zinc. The zinc creates a grey uniform layer across the item, except where the fingerprints are located (Jones et al, 2001). Superglue vapour (ethyl cyanoacrylate) is believed to catalysed into a white powder by the water and some other components of fingerprints. The deposition of fibrous growths is subsequently dyed with fluorescent dye in order to visualise the fingerprints (Home Office Scientific Development Branch, 2005).

The analysis of the friction ridge detail of a fingerprint is based on: "ridge flow and ridge paths; the location, direction, and spatial relationships of minutiae; and ridge structure" (SWGFAST, 2013). The subsequent determination of the quantitative and qualitative levels of 'detail', and establishment of suitability of the print for comparative purposes, occurs before comparison, evaluation and the formation of conclusions relating to identification (or not). The levels of 'detail' are categorised as: Level 1 - overall ridge flow; Level 2 - individualised and relative arrangements of friction ridge paths and friction ridge events; and Level 3 - ridge structures and their relative arrangements (SWGFAST, 2013). Examination, analysis and comparison are reliant on the competency and expertise of the fingerprint examiner, before an evaluation occurs. The evaluation results in one of four conclusions being reached: 1. exclusion; 2. individualisation, 3. inconclusive; and 4. return to the analysis phase.

The whole process is known as the ACE-V methodology - Analysis, Comparison, Evaluation and Verification. This is not an entirely linear course of action, as previous phases can be returned to. Additionally, a trained fingerprint examiner will understand and take into consideration a range of factors which can impact upon the examination. These include, but are not limited to, the condition of the skin, the pressure maintained during transfer, the substrate onto which the print is transferred and the presence/absence of secretions (SWGFAST, 2013). As there are so many competing variables to consider in fingerprint examination, there is no threshold against which a fingerprint could be classed as 'identifiable' versus one which is not. Therefore, the aim of any procedure being carried out on the device would be to cause the minimal amount of damage to any latent prints.

3 Methodology

In this article, Apple portable devices are the subject of analysis and discussion as reported sales of Apple iPhone devices topped 200 million in 2017 (Statista, 2018g). Whilst considering potential issues for fingerprint recovery post DF analysis, Section 3 offers an analysis and evaluation of the impact of a mobile forensic extraction on a handset's screen. There are two fundamental research questions which are addressed in this work, noted as follows:

1. How destructive is a typical mobile device analysis procedure on latent fingerprints?
2. Can certain methods of device interaction (including bare finger, latex glove, touch screen cotton glove and stylus) reduce latent fingerprint destruction on a device screen?

Section 4 offers test results and is set out as follows. Sections 4.1 and 4.2 offer a device 'screen-map', identifying typical screen interactions in two scenarios. The first (Section 4.1), documents a control test documents the typical screen interactions carried out by a practitioner when forensically acquiring data from an Apple device. The second (Section 4.2) describes what this article coins as 'impact quantification'; an example of the potential resident fingerprints left after a device user has typically utilised popular iOS applications, and the impact of a subsequent device extraction by a practitioner upon these fingerprint regions. Section 4.3 examines the impact of PPE usage by a DF practitioner when interaction with a device screen in order to extract it's digital content. Four scenarios are evaluated - bare fingered extract, using latex gloves, using touch screen cotton gloves and using a stylus.

3.1 Examination interactions with exemplar fingerprints

In order to assess the impact of the four conditions noted above on latent fingerprints on a device, the following methodology was utilised. To provide a large surface area upon which to work, an iPad was used for the deposition of fingerprints (both iPhone and iPads utilise Gorilla® screen glass). After careful cleaning, a series of eight plain impressions were deposited down the length of the iPad screen, with the thumbs being wiped before the first and subsequent depositions. Plain impressions (where fingers are placed flat on a surface without rolling) were used to provide a recognisable target for the interactions. This enabled the interactions to be placed entirely within the body of the latent print using the latent print itself to delineate the damage.

Each print was left for 1 hour before being interacted with in one of the following ways: 1) bare fingered press, 2) bare fingered swipe, 3) latex gloved fingered press, 4) latex glove fingered swipe, 5) touch screen gloved press, 6) touch screen gloved swipe, 7) stylus press, and 8) stylus swipe. The screen press and swipe were used to simulate the two actions a practitioner must typically perform on a device screen in order to interact with it. A passive universal stylus, which included a large tip made of conductive material (7.5 mm diameter), was used rather than a ballpoint pen-like tipped active pen, as these latter devices did not appear to interact and operate the screen of the test Apple device.

The iPads were dusted with Aluminium powder and visual examination was completed using an Integrated Rapid Imaging System (IRIS) and suitable imagery captured for evaluation.

Limitations: - This work has analysed the recoverability of fingerprints from Apple devices which utilize Gorilla® screen glass. Whilst an inference is made that the results offered are applicable to other smartphone screen glass, such a statement cannot be said with certainty and is therefore a limitation of this article. However, the current list of products which possess Gorilla® screen glass is comprehensive and includes most common device manufacturers and device types, including smartphones, tablets, slates, notebooks and wearables (Corning, 2018). Further, our testing focuses on the screen surface of the handset, omitting to consider fingerprint recovery from the sides and back of devices. This decision has been taken in order to reduce the number of variables in need of consideration for testing so that focus could be maintained on fingerprint destruction. Whilst not making the assumption that fingerprints are non-recoverable from surfaces other than the screen, both surface area and device handling (putting a device on a textured surface for example), suggest that there is a greater chance of undamaged fingerprints being resident on a screen, given that this is the surface for interacting with a device. In addition, with an increase in what are described as ‘three-quarter cases’ which protect both the back and sides of a device from damage, thereby leaving the screen accessible, fingerprints on other portions of the device may not be available, particularly if the case consists of a textured, non-printable surface.

4 Results

Section 4 presents the results of both the controlled and actual fingerprint tests.

4.1 Control Test

Figure 2 depicts the touches which occur when extracting an iPhone 7 device (for testing, AXIOM and XRY procedures were utilised). This provides an initial indication of what this article will term ‘screen impact’ which is the result of touching a mobile device screen in order to extract data from it.

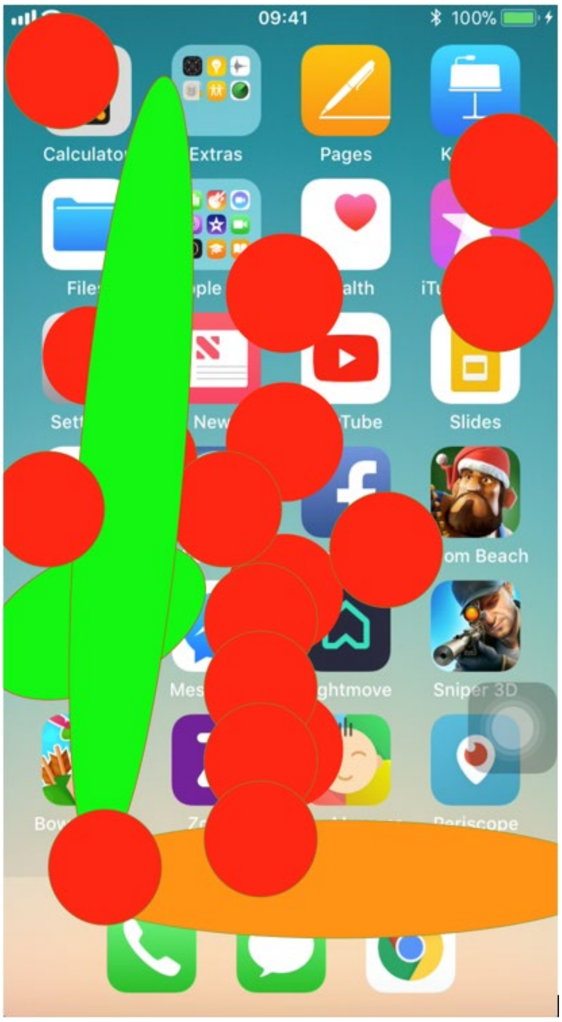

Figure 2: A map of screen touches during a forensic extraction of an iPhone 7. Red marks indicate static mandatory procedural touches. Green marks are handling touches. Orange marks are mandatory touches, but 'moveable' (mandatory navigation touches).

**Points of interest*: Forensic extraction principles will typically maintain the same standard operating procedure for the same make and model of handset. Therefore, extractions for iPhone 7 handsets utilising the same forensic extraction tool will have screen impact characteristics typical of those noted in Figure 2. However, there are three variables which are subject to change during examinations. The first is the imposition of a device handset lock. In the test case presented, a pincode of '2580' was resident on the device, resulting in a central line of mandatory (red) presses due to the location of the onscreen pin-pad. Different device handset locks will result in different mandatory press locations.

Second, device handling touches (documented in green) are due to handling the device throughout the examination (for example, removal from packaging, connecting the device etc.). Whilst arguably, a device can be handled in less impactful ways (for example, holding the sides of a device), this may not always be a prominent thought of the practitioner. In this case, we examined typical device handling procedures where the examining practitioner was under instructions to treat the device '*as per typical procedure*'. Assuming that device handling touches will appear on the handset screen, these are not static and therefore may impact the screen in different locations and sizes depending on how a practitioner typically handles mobile exhibits and factors such as whether they are left or right handed. Finally there are non-static mandatory touches (shown as orange). These touches must be made by a practitioner to navigate device menus (in this case, to swipe to a secondary home screen to enter the ‘settings’ of the device). Whilst these may vary in location, navigation of the device via such touches is needed.

Static mandatory procedural touches (red) refer to screen locations which must be pressed in order to prepare for or initiate an extraction. For example, when an iOS device requires the practitioner to enable a ‘Trusted Connection’, this is typically a prompt in the center of the screen which must be pressed. Other issues include checking iOS versions and disabling networked connections for device integrity purposes.

Whilst arguments for poor handling processes could be made following Figure 2, it must be considered with the fact that there is limited guidance in terms of best practice handling procedures for DF examiners. Therefore handling marks generated during the course of an examination may vary wildly in terms of quantity and placement. Further, DF practitioners are often not knowledgeable of traditional forensic science evidence recovery methods. Therefore, in the absence of training, it would be unfair to place the assumed burden of preserving fingerprint evidence on a device screen without effectively evaluating and educating them on such processes.

Finally, in regards to screen impact, this must be considered against the fact that modern smartphones, including the iPhone, operate a dynamic desktop environment where applications can be created, moved and removed. Therefore, it is difficult to establish with 100% consistency where a practitioner may have to press in all instances due to potential variances in device configurations by the user. Figure 2 also documents a process which is solely for the purpose of extracting device data. No ‘manual verification of data’ processes (see Figure 1) have been mapped, which would significantly increase the volume of practitioner screen touches.

4.2 Assessing Impact: User Fingerprint quantification

Given that Figure 2 documents the typical mobile screen impact following an extraction, such actions must be evaluated against typical device usage and the subsequent deposition of their fingerprints from these actions. Figure 3 denotes the typical screen presses following usage of the Facebook [over 2 billion users (Statista, 2018f)], Twitter [330 million users (Statista, 2018e)], WhatsApp [1.3 billion users in 2017 (Statista, 2018d)] and YouTube [over 200 million video viewers as of 2016 in the United States alone (Statista, 2018c)] applications. In each case, the screen press locations recorded in Figure 3 (translucent marks) are as a result of the user interacting with core functions of each application retrospectively. These marks overlay those of a practitioner who carries out a typical device extraction so that potential areas of destruction can be identified. For example, in the case of Twitter, screen press locations are typical of a user who scrolls down their ‘Twitter-feed’, searches for tweets/users, examines their notifications and private messages, and creates a tweet from their account. As each application maintains a consistently formatted user interface, these regions of impact are consistent for anyone who utilises these applications on a mobile device with a comparable screen size.

Points to note:- The touch maps offered in Figure 3 provide an indication of the marks generated by a handset user, their position and ultimately their potential for destruction by those of a practitioner during a forensic extraction of the device. Whilst there are multiple places a user can leave fingerprints on their device, placement is likely to coincide with key functional areas of their device. As a result, regardless of the volume of usage received on a handset (which may affect the quality of fingerprint recovery), a maximum capacity will be reached before subsequent prints overwrite those in existence**.** It is key to note, that for simplicity purposes, Figure 3's defining of regions of interest assumes that fingerprints may be recoverable from such positions. However in reality it is not this simple. The consistency of application interfaces leads to repetition of tasks which can cause print-on-print damage (multiple prints overlayed, making identification difficult or in some cases, not possible). This means that regardless of damage caused by a practitioner, fingerprints may never have been recoverable in the first instance. Whist all apps maintain their own unique selling points and functionality, most adopt sound principles of user experience and design whilst engaging with standard operating system functions, such as the keyboard. The result of this is an overlap in typical print locations, regardless of the application in use. For example, where a user must type, the iOS virtual QWERTY keyboard covers the bottom third of the device. In addition, key application menu bars and icons are often pinned to both the top and bottom of the screen. As these must be pressed to use these applications, they are key locations for latent fingerprint recovery.

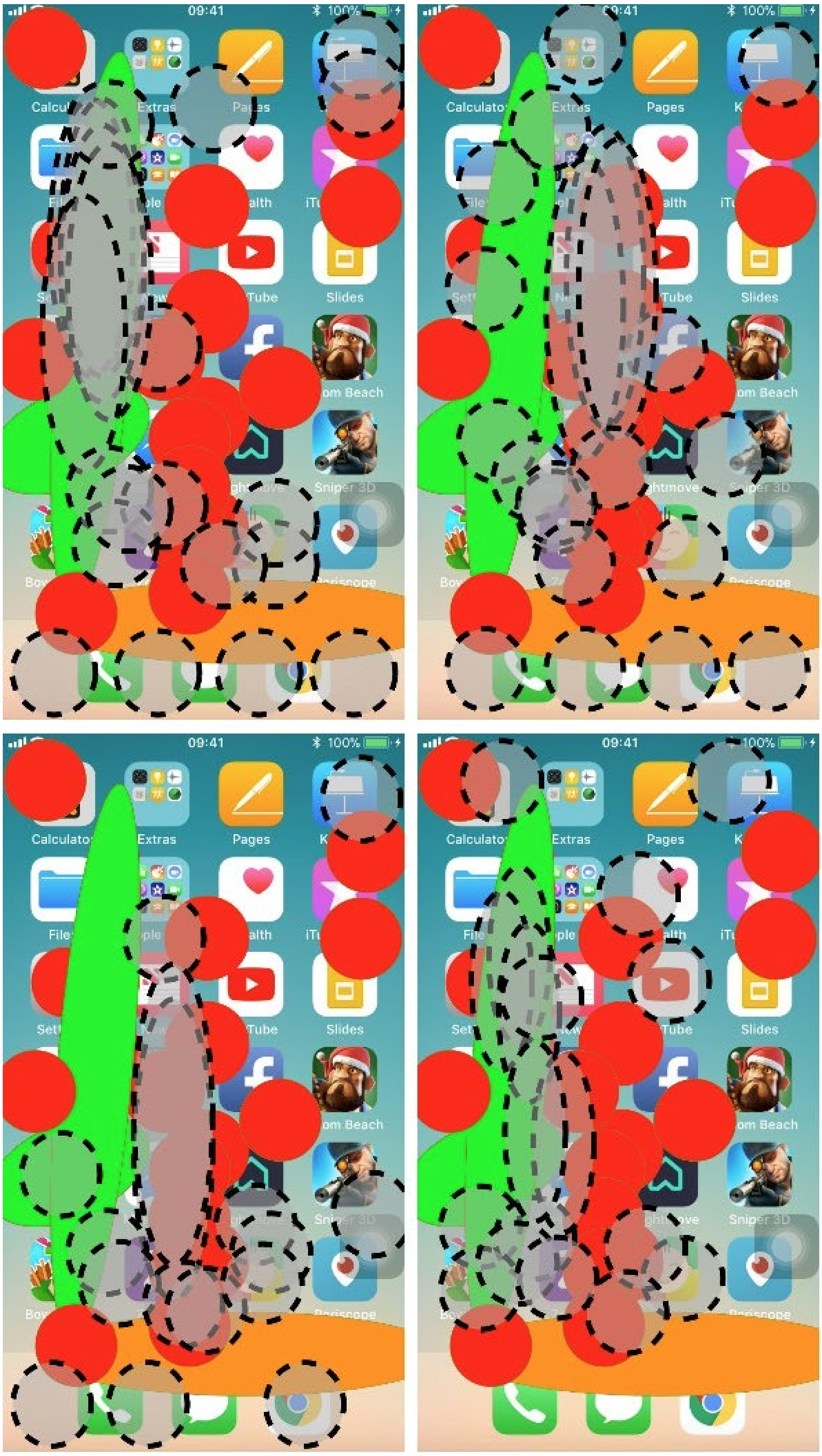

Figure 3: A touch map of Twitter (top-left), Facebook (top-right), WhatsApp (bottom-left) and YouTube (bottom-right). A DF practitioner extraction marks (as noted in Figure 2) are present, where the transparent marks overlaid are typical of a user's interaction with each respective application - indicating potential print-area damage.

4.2.1 Quantification of Destruction

It is important to note that fingerprint experts do not always require full fingerprints in order to facilitate the identification of a print and therefore the analysis presented in Figures 2 and 3 provides an inferred indication of regional areas where destruction may occur. Fingerprint practitioners typically operate on the premise that the greater the quantity of a print recovered during examination, the more likely it is that identification can be made. Table 1 provides a summary of the print recovery locations noted in Figure 3 from each of the four applications. In all cases, there is only one region which would not be impacted upon by a practitioner's extraction prints.

Table 1. Breakdown of full and partial fingerprint locations.

	Facebook	**Twitter**	**WhatsApp**	**YouTube**
No. potential full print locations	1	1	1	1
No. print locations with minor damage	8	6	5	4

4.3 Examination interactions with exemplar fingerprints

This section provides the results following the use of forms of PPE to press and swipe latent fingerprints. The first test examines the impact of a DF practitioner who interacts with a device without any form of personal protective equipment (PPE). A non-gloved examination revealed the impact of print-on-print damage, as well as the damage caused by a bare finger swipe. Other forms of common PPE an examiner may opt to utilise during a device examination include latex gloves, cotton gloves (with screen interaction ability) and a device stylus. All four test conditions have been examined, shown in Figure 4 (colour reversed for clarity).

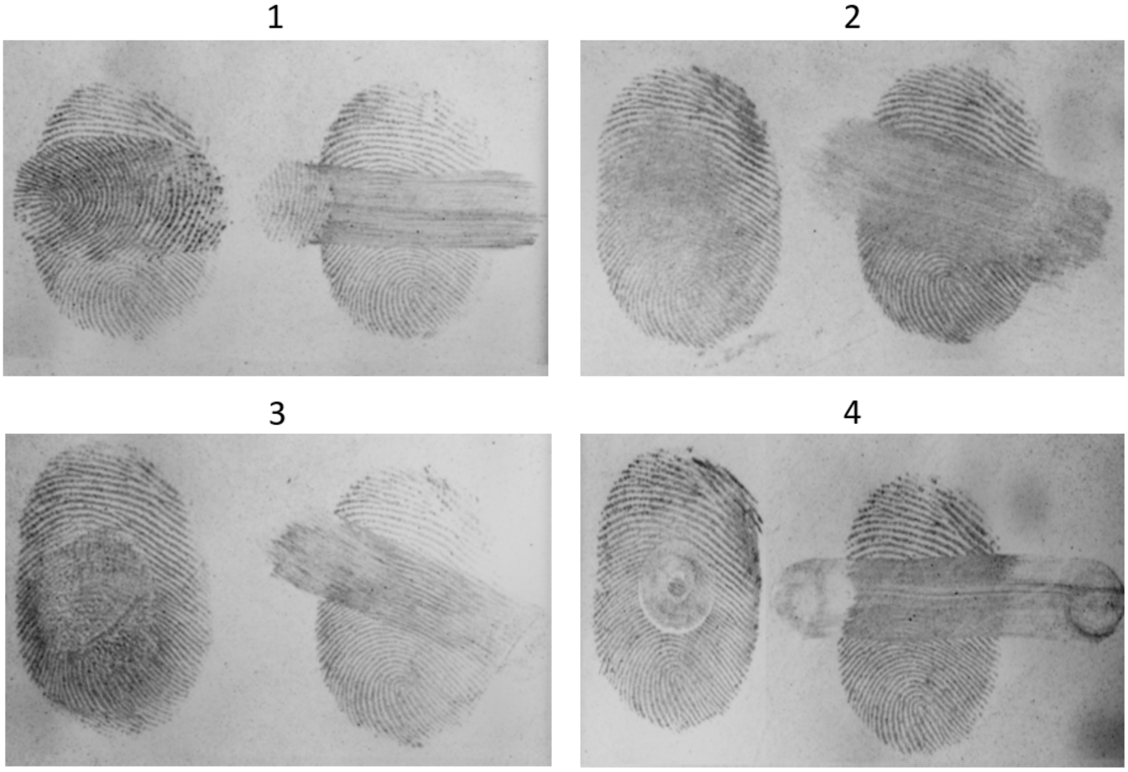

Figure 4: Example fingermarks following subsequent examiner device interaction and aluminium powdering. The effects of a bare finger press and swipe are shown in (1). The effects of a latex glove press and swipe are shown in (2). The effects of a cotton glove press and swipe are shown in (3). The effects of a stylus press and swipe are shown in (4).

Bare finger press (1 - left): This interaction is capable of overwriting the latent print with the examiner's own mark. The exact appearance will depend on the donor mark and the relative orientation of the examiner's fingers in relation to it. The examiner's print is clearly seen at centre left of the much larger plain impression, and is more visible due to a 90° rotation. The problems caused by overlapping marks have been rehearsed elsewhere, notably during the debate about the provenance of Y7 at the Scottish Fingerprint Inquiry (Campbell, 2011).

Bare finger swipe (1 - right): This interaction has removed an area of the latent print broadly equal to the width of the swiping finger in contact multiplied by the length of the swipe. Swipes are easily recognised by the characteristic appearance after fingerprint treatment, which is of convex circular ends connected by a broadly rectangular feature of variable straightness. The circular ends may retain 2-dimensional details of the tip of the swiping object. Here*,* ridge detail from the examiner is visible at the left hand end of the swipe. (The swipes took place from left-to-right in all instances)

Latex glove press (2 - left): The outcome of this interaction is variable even within this single mark. There is an obviously disturbed area with rather ill-defined diffuse edges in the centre of the plain impression where the latex glove has been pressed, but close examination at high magnification shows that the degree of disruption of the ridge detail, although severe, varies.

Latex glove swipe (2 - right): This interaction typically removes an area of the latent print broadly equal to the width of the swiping latex glove in contact multiplied by the length of the swipe. As noted in *(1 - right)*, swipes are easily recognised by the characteristic appearance after fingerprint treatment.

Cotton glove press (3 - left): The outcome of this interaction is variable even within this single mark. There is an obviously disturbed area with rather ill-defined diffuse edges in the centre of the plain impression where the cotton glove has been pressed, but close examination at high magnification shows that the degree of disruption of the ridge detail varies from complete obliteration to still recognisable ridges.

Cotton glove swipe (3 - right): This interaction typically affects an area of the latent print broadly equal to the width of the swiping cotton glove in contact multiplied by the length of the swipe. As before, swipes are easily recognised by the characteristic appearance after fingerprint treatment. In this instance however the degree of disruption is again variable, along the length of the swipe, from complete obliteration to clearly recognisable ridges.

Stylus press (4 - left): This interaction damage is limited to the circular stylus tip area. The particular stylus used here has a 7.5mm diameter soft, hollow rubber tip and it tends to turn inside out on contact so that it becomes convex to the surface, resulting in a domed space which is in contact with the latent print only around the stylus perimeter. This results in survival of ridge detail within the stylus tip area, albeit somewhat degraded in this instance.

Stylus swipe (4 - right): This interaction typically affects an area of the latent print broadly equal to the diameter of the swiping stylus in contact multiplied by the length of the swipe. Again the swipe is easily recognised by the characteristic appearance. Close examination shows that while disruption is severe it is by no means total. A short length of at least seven ridges is visible in the lower center of the swipe.

5 Conclusions

Preliminary findings indicate that all four approaches (bare finger, latex glove, touch screen cotton glove and stylus) result in some damage to the latent print. This damage varies in both the degree of obliteration of the latent print and the area of the print which is obliterated. In all instances, the act of swiping is many times more damaging to the latent print than pressing. This result is not unexpected, given the act of swiping across a latent print automatically covers a greater area in comparison to a press. The approach that resulted in the least damage to the latent print was through the use of the stylus. Overall, the other approaches (latex glove, cotton touch screen, bare finger) can be grouped as one, being appreciably more damaging than the stylus, at least within this limited study.. Combining the practical data with the control tests, it is clear that the process of digital evidence extraction has an impact upon the latent prints on the device being extracted. Although a FP examiner does not always need a complete print in order to use it for identification purposes, as previously outlined the aim would be to limit, as much as possible, the potential for damage to occur. The number of partial prints inferred from the touch maps shows that there are many FPs which are likely to be damaged by a DF extraction procedure, and thus the examiner should try to ensure that this damage is kept to a minimum. Thus, in order to minimise damage to latent prints on the surface of a device during digital evidence extraction, a stylus should be utilised, limiting interactions to presses rather than swipes where possible. This approach would minimise the disruption to the mobile device's surface, thereby giving the maximum potential for recovery of fingerprints.

The use of a stylus to interact with the surface of the device during a DF extraction needs to be considered further in relation to the type of stylus and the size of its tip. The stylus employed within this study was a passive universal stylus with a large tip. The tip was 7.5 mm in diameter, expanding to 9 mm when fully depressed, and, as a consequence, the interaction with the fingerprint in both press and swipe was between those widths depending on the pressure applied. A smaller, ballpoint pen-tipped active pen may well cause significantly less damage as a consequence of the smaller surface area touching the device. The active pen offers a wider range of options with respect to usability such as input buttons and touch sensitivity, which may alter the manner in with a DF extraction can occur, thereby resulting in an even greater reduction in damage to any latent prints present on the device. However, in this instance, two examples of active pens were tested on the iPad devices and neither pen interacted with the device in such a way as to allow an extraction. An examiner would, therefore, need to ensure that the stylus employed was able to interact with and operate the device being examined, or identify and utilise an active pen which was universally suitable.

With regards to the utilisation of any finger-based extraction method (bare finger, cotton touch screen glove, latex glove), consideration is needed in respect to the sensitivity of the device screen and the force needed to interact with it during the data extraction. For example, the pressure that was required to interact with the device screen whilst wearing a pair of touch screen cotton gloves was considerable and resulted in greater damage. Bare fingered touches produced the second lowest level of damage but, given the likelihood of the need to take into account DNA-based evidence, this method of DF extraction may be unsuitable.

5.1 Future Work

This work has offered a preliminary analysis of the DF examination impact on latent screen fingerprints. As a result of analysis, the following areas are offered as considerations for future work.

The effect of ageing of fingerprints on the outcome of an examination: As devices may be examined both immediately due to triage procedures and in some cases subject to backlogs of multiple months in length, latent prints with a range of ages will be encountered. The composition of a latent print is affected over time, principally by moisture loss (Farrugia *et al*, 2015), but also through changes to the sebaceous material present (Archer *et al*., 2005). As powders adhere to the fatty deposits of sebaceous sweat in older prints, a longitudinal study is required to assess the vulnerability of latent marks to damage during the interactions of a DF practitioner during data extraction of a device.

Pressure: Pressure is also likely to have a role in the damage of latent prints. Work is needed to establish a threshold at which the minimal pressure can be applied in order to obtain a response from a device screen. An assessment is also required in order to establish the level of pressure needed which results in damage to a print.

Mark Types: In this work, assumptions have been that latent prints are plain impressions (full fingerprints). However, when a user interacts with their device, a range of latent prints may be generated from various surface areas, including the very tip of the finger. The impact of a DF extraction upon a range of different types of user generated marks, particular the very tip of the finger, should be examined.

Impact of Aluminum powder on modern devices: This work has operated on the assumption that aluminium powder can be potentially destructive to mobile devices following acknowledgments made in literature (Girard, 2017) and best practice guidelines (CAST, 2014). Further testing is required to examine the impact of fingerprint powder types on the function of mobile handsets in order to assess the risks posed by this form of fingerprint recovery.

6 References

Androulidakis, I.I., 2012. *Mobile phone security and forensics: A practical approach*. Springer.

Apple, 2017. Apple awards Corning first advanced manufacturing fund investment. Available at: https://www.apple.com/uk/newsroom/2017/05/12Apple-Awards-Corning-First-Advanced-Manufacturing-Fund-Investment/ (Accessed 01 February 2018)

Association of Chief Police Officers (2007) 'Good Practice Guide for Computer-Based Electronic Evidence' Available at: https://www.7safe.com/docs/default-source/default-document-library/acpo_guidelines_computer_evidence_v4_web.pdf (Accessed 22 January 2018)

Ballou, S. ed., 2010. *Electronic crime scene investigation: A guide for first responders*. Diane Publishing.

BBC News (2014a) 'Fingerprints give police new clues for solving crime' Available at: http://www.bbc.co.uk/news/science-environment-26668838 (Accessed 22 January 2018)

BBC News (2014b) 'Mobile phones carry owners' bacterial 'fingerprint'' Available at: http://www.bbc.co.uk/news/health-27985815 (Accessed 22 January 2018)

BBC News (2017) 'Hatton Garden pair burgled Mayfair jewellers, court told' Available at: http://www.bbc.co.uk/news/uk-england-london-39119346 (Accessed 22 January 2018)

BBC News (2018a) 'Nottingham station fire: Police recover 'items of interest'' Available at: http://www.bbc.co.uk/news/uk-england-nottinghamshire-42735593 (Accessed 22 January 2018)

BBC News (2018b) 'All current rape cases to be 'urgently' reviewed over disclosure fears'. Available at http://www.bbc.co.uk/news/uk-42841346 (Accessed 10 April 2018)

BBC News (2018c) 'Drug dealer jailed after £230,000 'dirty money' swoop' Available at: http://www.bbc.co.uk/news/uk-scotland-glasgow-west-42718378 (Accessed 22 January 2018)

Brezinski, D. and Killalea, T., 2002. *Guidelines for evidence collection and archiving* (No. RFC 3227).

Campbell, A., 2011. The fingerprint inquiry report. *Edinburgh, Scotland: APS Group Scotland*, *790*.

Casey, E., 2011. *Digital evidence and computer crime: Forensic science, computers, and the internet*. Academic press.

Centre for Applied Science and Technology (CAST), 2014. Fingerprint Visualisation Manual. 1st Edition. ISBN - 978-1-78246-270-5

College of Policing (2016) 'Bail report Pre-charge bail – an exploratory study' Available at: http://www.college.police.uk/News/College-news/Documents/Bail_report_document_439E0816_2.pdf (Accessed 12th July 2017)

Corning, 2018. *Products with Gorilla*. Available at: http://www.corning.com/gorillaglass/worldwide/en/products-with-gorilla.html (Access 01 February 2018)

Curran, K., Robinson, A., Peacocke, S., Cassidy, S. (2010) Mobile Phone Forensic Analysis, International Journal of Digital Crime and Forensics, Vol. 2, No. 2, pp:, April-May 2010, ISSN: 1941-6210, IGI Pub

European Network of Forensic Science Institutes (2015) 'Best Practice Manual for the Forensic Examination of Digital technology' Available at: http://enfsi.eu/wp-content/uploads/2016/09/1._forensic_examination_of_digital_technology_0.pdf (Accessed 22 January 2018)

European Network of Forensic Science Institutes (2015b) 'Best Practice Manual for Fingerprint Examination' Available at: http://enfsi.eu/wp-content/uploads/2016/09/6._fingerprint_examination_0.pdf (Accessed 22 January 2018)

Farrugia, K.J., Fraser, J., Friel, L., Adams, D., Attard-Montalto, N. and Deacon, P., 2015. A comparison between atmospheric/humidity and vacuum cyanoacrylate fuming of latent fingermarks. *Forensic science international*, *257*, pp.54-70.

Fisher, B.A.J. and Fisher D.R., 2012. Techniques of Crime Scene Investigation 8th Ed p.121 CRC Press, Boca Raton.

Girard, J. E. (2017) Criminalistics, *Jones & Bartlett Learning*

Home Office Scientific Development Branch, 2005. Fingerprint Development Handbook. 2nd Edition.

Horsman, G., Laing, C. and Vickers, P., 2014. A case-based reasoning method for locating evidence during digital forensic device triage. Decision Support Systems, 61, pp.69-78.

Jones, N., Stoilovic, M., Lennard, C., and Roux, C., 2001. Vacuum metal deposition: developing latent fingerprints on polyethylene substrates after the deposition of excess gold. Forensic Science International. 123 (1): 5-12.

Murphy, C.A., 2009. Developing process for mobile device forensics. *SANS Digital Forensics and Incident Response*.

National Crime Agency (n.d.) 'Cyber crime: Preventing young people from getting involved' http://www.nationalcrimeagency.gov.uk/crime-threats/cyber-crime/cyber-crime-preventing-young-people-from-getting-involved (Accessed 22 January 2018)

Parliamentary Office of Science and Technology (2016) 'Digital Forensics and Crime' POSTNOTE 520, March 2016, Available at: file:///C:/Users/u0032268/Downloads/POST-PN-0520%20(1).pdf (Accessed 22 January 2018)

Scanlon, M., 2016, August. Battling the digital forensic backlog through data deduplication. In *Innovative Computing Technology (INTECH), 2016 Sixth International Conference on*(pp. 10-14). IEEE.

Scanlon, M., Du, X. and Lillis, D., 2017. EviPlant: An efficient digital forensic challenge creation, manipulation and distribution solution. *Digital Investigation*, *20*, pp.S29-S36.

Statista (2018a) 'Number of mobile phone users worldwide from 2013 to 2019 (in billions)' Available at: https://www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/
(Accessed 22 January 2018)

Statista (2018b) 'Smartphone ownership penetration in the United Kingdom (UK) in 2012-2017, by age' Available at: https://www.statista.com/statistics/271851/smartphone-owners-in-the-united-kingdom-uk-by-age/ (Accessed 22 January 2018)

Statista (2018c) 'Number of digital video viewers in the United States from 2012 to 2021 (in millions)' Available at: https://www.statista.com/statistics/271611/digital-video-viewers-in-the-united-states/ (Accessed 22 January 2018)

Statista (2018d) 'Number of monthly active WhatsApp users worldwide from April 2013 to July 2017 (in millions)' AVailable at: https://www.statista.com/statistics/260819/number-of-monthly-active-whatsapp-users/ (Accessed 22 January 2018)

Statista (2018e) 'Number of monthly active Twitter users worldwide from 1st quarter 2010 to 3rd quarter 2017 (in millions)' Available at: https://www.statista.com/statistics/282087/number-of-monthly-active-twitter-users/
(Accessed 22 January 2018)

Statista (2018f) 'Number of monthly active WhatsApp users worldwide from April 2013 to July 2017 (in millions)' Available at: https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ (Accessed 22 January 2018)

Statista (2018g) 'Unit sales of the Apple iPhone worldwide from 2007 to 2017 (in millions)' Available at: https://www.statista.com/statistics/276306/global-apple-iphone-sales-since-fiscal-year-2007/ (Accessed 22 January 2018)

SWGDE (2013) 'SWGDE Best Practices for Mobile Phone Forensics' Available at: https://www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices%20for%20Mobile%20Phone%20Forensics (Accessed 02 February 2018)

SWGFAST, 2013. 'Document #10. Standards for examining friction ridge impressions and resulting conclusions (latent/tenprint). Available at: http://clpex.com/swgfast/Documents.html (Accessed 02 February 2018)

Quick, D. and Choo, K.K.R., 2014. Impacts of increasing volume of digital forensic data: A survey and future research challenges. *Digital Investigation*, *11*(4), pp.273-294.