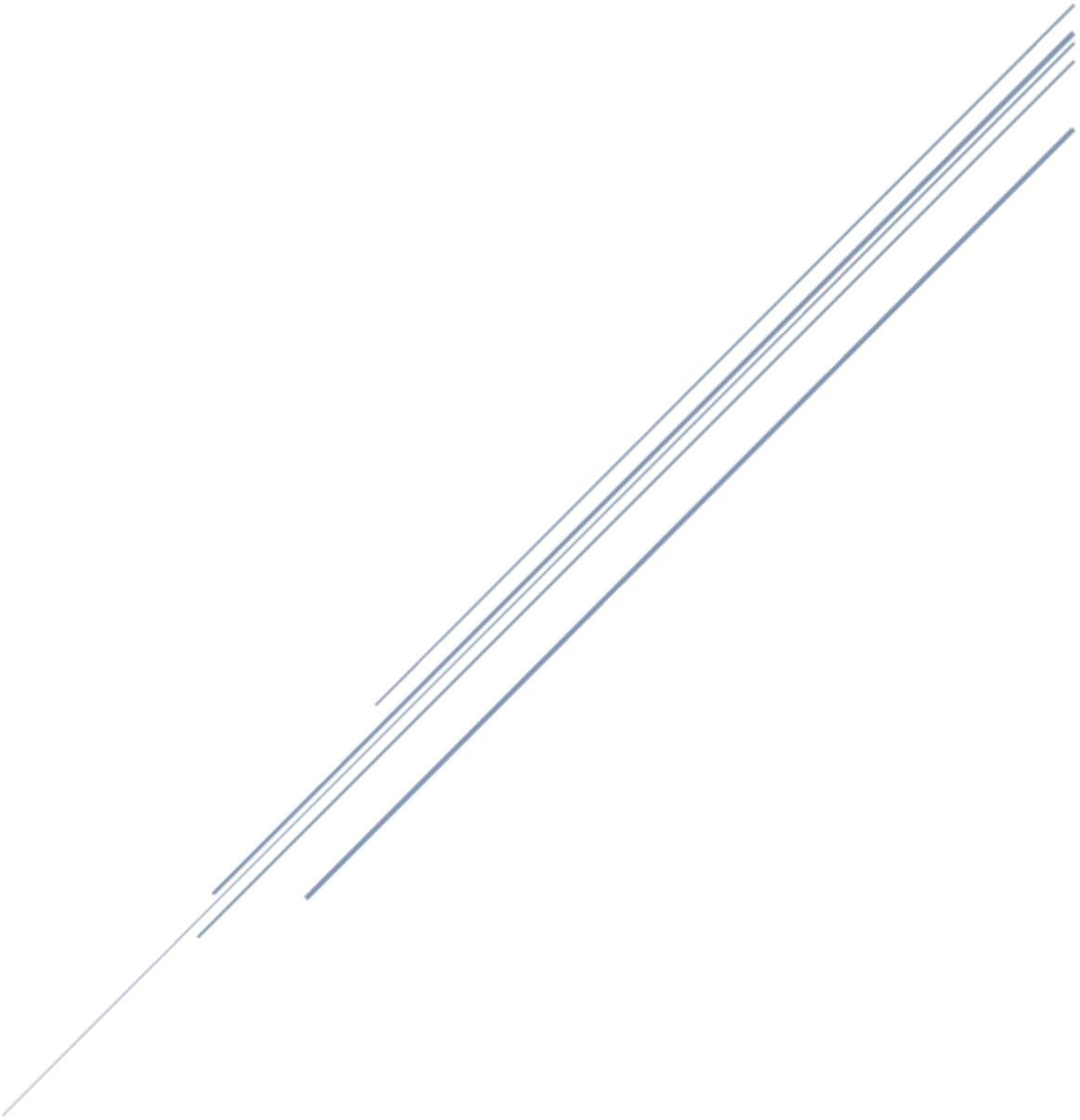
How Mobile Device Security is Challenging Law Enforcement

By Jonah McElfatrick



CMP416 Digital Forensics 2

BSc (Hons) Ethical Hacking – 4th Year

Law enforcement face a variety of different challenges every day dealing with case evidence, from obtaining the evidence to preserving the integrity of the evidence. In mobile forensics, law enforcement can face further challenges when trying to gain access to information on mobile devices seized during an investigation. With these challenges in mind, consideration must be taken into areas such as the security features implemented on mobile devices, how law enforcement is to carry out forensic investigations and access the data on mobile devices with these security measures in place while also maintaining the data's integrity in a forensically sound manner. There are laws in place to protect user's information and privacy on a mobile device. When law enforcement carries out a forensic investigation, these laws must be considered and examined in detail to determine how law enforcement can gain access to the information on a device while still staying within the bounds of the law. There are a variety of ways that law enforcement can attempt to gain access to data in a mobile device, some of these are very simple and some very complex.

With over 3.5 billion smartphones currently around the world (Turner, 2018), there are two main ecosystems that exist in the mobile market, Apple iOS and Google's Android. Both companies behind these operating systems have the same goal, to provide a stable, secure operating system for their consumers. These two operating systems have multiple security features implemented into the software and hardware of the devices. Both systems implement similar security features including biometrics such as fingerprint scanners and facial recognition, or more basic features such as pin codes and passwords. Although they may accomplish the same outcome, the way in which these security methods are implemented can differ. Where Apple uses capacitive sensors to read the fingerprint of the user, Android uses a mixture of different sensors for different devices, these include capacitive sensors, ultrasonic sensors and optical sensors. Both the ultrasonic and optical sensors can be placed below the screen in the case of some Android devices. This is not always noticeable at first glance of the device and requires an up to date knowledge of device hardware to know what features are implemented into the devices. As Android is an open source operating system, this allows for manufacturers of devices to configure their own hardware and software to tailor the operating system to their own needs. Examples of these are Sony's Xperia, Samsung Experience and Huawei EMUI. Due to this option, some manufacturers have added some of their own security features, this includes Iris scanners, pattern locking and other security features. All these features can be used for both unlocking the physical device and unlocking the apps installed on it. Some of these security features can also be used in unison. For example, on an Android device, the user can setup their fingerprints but must also have a backup in case of a hardware failure or the sensor being unable to read the fingerprint due to dirt or moisture. This allows for a combination such as the fingerprint scanner and a pin code to be used at the same time. This allows the user to use either of these methods to unlock the device. All these features can be used in different configurations depending on the device manufacturer. The user then has the choice of which of the features to use to lock their device. With all these security features in place, it can make unlocking the device very difficult for those who do not have the correct passkey.

When a device is seized for the use in a criminal investigation, obtaining access to the data on the device is one of the main difficulties that a forensic investigator comes across. The security features present on mobile devices present difficulty for law enforcement when trying to gain access to the device. The most straightforward way to unlock the device is for the owner of the passkey to unlock it. Although it may be straightforward in theory, the owner of the passkey does not have to provide law enforcement with the passkey due to the possibility of self-incrimination or due to privacy concerns. If the suspect is unwilling to provide the passkey to the device, law enforcement cannot force the owner to unlock the device. Law enforcement must get approval from a judge to make the owner unlock the device. In the UK, the Regulation of Investigatory Powers Act 2000 allows for

public bodies such as the police to demand the owner of the passkey to share it with them. According to section 49 of the Regulation of Investigatory Powers Act 2000 (Participation, 5 February 2019*):"If any person with the appropriate permission under Schedule 2 believes, on reasonable grounds that the imposition of a disclosure requirement in respect of the protected information is necessary on grounds falling within subsection (3)"*, where section 3 reads *"A disclosure requirement in respect of any protected information is necessary on grounds falling within this subsection if it is necessary for the purpose of preventing or detecting crime"*. To simplify, this allows for law enforcement to request the passkey to be shared with them to allow access to the information on a device if they feel that the information on the device is relevant to an ongoing or proposed crime. If the owner of the device still refuses to hand over the passkey without proof that they do not have possession of the key then according to section 53, they can then be sentenced to jail time. This can be seen as follows: *"A person to whom a section 49 notice has been given is guilty of an offence if he knowingly fails, in accordance with the notice, to make the disclosure required by virtue of the giving of the notice."*, *"A person guilty of an offence under this section shall be liable on conviction on indictment, to imprisonment for a term not exceeding the appropriate maximum term or to a fine, or to both"*. *"the appropriate maximum term' means in a national security case or a child indecency case, five years; and in any other case, two years."*. As can be seen above, in the event that the owner of the passkey refuses to hand the passkey over to law enforcement, after being compelled to by a judge, the owner of the passkey can be sentenced to jail time for a maximum sentence of 5 years if the case is related to national security or child indecency, and in all other cases the maximum sentence is 2 years. In some cases, this is enough to compel the owner of the passkey to hand it over to law enforcement, in other cases this is not.

There are cases that, even when compelled to by a judge, the owner of the passkey refuses to hand it over to law enforcement. This means the forensic investigators must attempt other ways of gaining access to the information stored on the device. A paper produced in 2009 details the challenges that law enforcement face in the acquisition phase of the investigation (Raghav and Saxena, 2009). It conveys the issue of a pin or password protected mobile device being a big issue that law enforcement face when trying to acquire information from the seized device as it can take a long time to bypass. If law enforcement were to attempt to try and crack a password set on a device, there are multiple aspects to consider. Not only are there concerns on the user's rights to privacy, but passwords can vary in length and complexity, as both increases so does the length of time it takes to crack. According to Core Security, a password using both upper- and lower-case letters, numbers and symbols only requires to be 7 characters long to exponentially increase in the time taken to crack (*The Exponential Nature of Password Cracking Costs | Core Security Blog*, no date). Using a hashing algorithm on top of a sophisticated password decreases the chances of the password being cracked again. The complexity and storage of the password is not the only issue law enforcement face if they were to attempt to brute-force their way into a device. Some devices have a time delay between entry attempts, this time increases after each failed attempt. This can drastically increase the time taken to try and brute force the device by guessing the passcode. Modern devices also allow for settings that would only allow for a limited number of logins. This only allows for a certain number of attempts to be made to unlock the device before wiping the data on the device or preventing the device being unlocked from that method. This could be detrimental to an investigation as any data on the device could have been the evidence needed in court to prove innocence or provide a conviction.

Other ways in which law enforcement can interrogate a device to gain access to the data stored on it, which tend to be quite successful and completed in a much smaller time frame, can include jailbreaking or rooting the device, or using 3rd party devices and software. Law enforcement in the United States have been using Jailbreaking techniques to be able to find evidence in criminal cases.

Jailbreaking is a term referring to Apple devices, whereas rooting a device is in reference to Android devices as every device is exploited differently. Exploiting the device involves removing software restrictions and gaining root access to the operating system on a mobile device. This allows users to install applications, other operating systems and gain access to features and functions that are otherwise restricted or hidden from the user. By Jailbreaking or rooting a device, law enforcement can bypass some security features and access the data that is stored on the device. Business Insider reported "Police routinely obtain warrants to search suspects' phones — just like searching a suspects' home — especially in high-profile investigations. But the new documents show that police regularly crack into phones for low-level cases like vandalism and shoplifting" (Holmes, 21 October 2020). If it is possible to Jailbreak or root a device, this indicates the data that can be obtained from the exploitation of the device and the wide variety of applications that the Jailbreaking/rooting method has, allowing access to all forms of data that can prove to be valuable in a criminal case.

Data can also be retrieved without the need for jailbreaking or rooting a device. Using 3rd party tools and software is another method of obtaining data. It was shown that not all iPhone devices need to be Jailbroken to be able to gather data from them. The use of Linux based tools allowed for data such as bookmarked webpages, recently visited webpages, last backup time and more data that could be used in an investigation to be gathered (Priyank Parmer, July-August 2018). As there are different tools available, there will be instances where some tools work better on certain mobile devices rather than others. This can be due to many attributes, including the differences in operating system architecture and underlying languages or the data storage methods used. A 2010 paper discusses the architecture of what makes an Android device and an iPhone device, the Android operating system having the Linux kernel underlying it and the iPhone operating system, iOS, being derived from the desktop MAC OS (Yates, 2010). Digital forensic tools can be classed under 5 different categories: computer, memory, network, database and mobile forensics (Wazid *et al.*, 2013). Although there are no certified approved mobile forensic tools, forensic tools instead need to demonstrate their integrity and independence from any single state or system. XRY is a software application designed by MSAB (Micro Systemation AB) for use on a windows operating system. It allows for data extraction from a vast variety of different devices in a forensically sound manner. XRY was designed and created to meet the following principles: "*Principle 1 No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court. Principle 2 In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions. Principle 3 An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result. Principle 4 The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to"* (MSAB, no date). This allows XRY to be used in any form of forensic investigation without the software holding any form of bias towards any one side. This ensures that the integrity of any found results cannot be questioned and can be used in a non-bias system such as a court of law. Although these tools are there to help law enforcement, these tools do not work in every instance. There can be times where new devices will appear on the market that are proprietary or use a different underlying structure that could cause issues with some of these tools.

If law enforcement manages to gain access to the data stored on the device, the challenge does not end. Methods such as app manipulation or concealment can cause further issues for law enforcement. These methods are known as Antiforensics and attempt to obscure and secure the data in the device further by disguising the data as another application or by hiding the applications existence to the user of the device (Chernyshev *et al.*, 2017). These methods are aimed to make analysing the data on the

device increasingly difficult to prevent law enforcement from being able to gather the evidence required for a conviction. It is also possible for data on the device to be encrypted even after gaining access to the device, a proprietary encryption algorithm, which is chosen by the owner, could be used to cause further issues in being able to read the data (Lutes and Mislan, 2020). There are applications that have been developed that are completely legal and serve to increase security and privacy on a device. These applications can be downloaded from the Google Play Store or Apple's App Store and can be used to hide or secure data further. An example of these applications is: Calculator – Photo Vault & Video Vault hide photos. This application allows for photos and videos to be hidden behind a supposed 'Calculator' application (*Calculator - Photo Vault & Video Vault hide photos – Apps on Google Play*, no date). This can cause further issues with law enforcement as these files will be hidden in different directories than what are commonly used to store this form of data.

Another possible way for entry into a mobile device is through the manufacturer. Although it is possible, some companies are not willing to help law enforcement unlock devices in an investigation as it would damage their image of their products being secure and the information on their devices being private. On 2nd December 2015, Syed Rizwan Farook and his partner Tashfeen Malik carried out a mass shooting at a Public Health Training event in San Bernardino. On the day of the attack, 14 people were confirmed dead and 17 others were seriously injured, later rising to 22 seriously injured ('SAN BERNARDINO SHOOTING: 22nd injured victim steps forward, FBI says', 2015). Law enforcement arrested the suspects and seized Syed Rizwan Farook iPhone device. After an initial attempt to unlock the device, the FBI requested Apple to assist in unlocking the device. Apple refused to help unlock the device as it would implicate creating a backdoor into their products and would shake their customers' trust with their own products (*Apple Opposes Judge's Order To Help FBI Unlock San Bernardino Shooter's Phone*, 17 February 2016). Although law enforcement required Apple to unlock the device, Apple were unwilling to do so and this in turn meant the investigation took a considerable amount of time longer than it would have if Apple were willing to help. This is a challenge for law enforcement as they can't use the 'easy' way in to be able to unlock the device.

If data is accessed from a mobile device and used in court, the next step is to allow both jurors and judges to understand the evidence gathered. This is not always as simple as it seems. As jurors are randomly chosen, they can come from a variety of different backgrounds, including some without a technological understanding. Most judges also do not have a technological based background to allow them to understand what some of the gathered data is and how it was obtained. A knowledge-based study carried out alongside court judges to analyse the acceptance and understanding of digital forensic evidence revealed that judges understand the importance of digital evidence but usually receive it in the forms of printed emails or files. It was also noted that judges believe that digital evidence gathered needs to be authenticated as they believe that digital evidence can easily be altered. To understand the evidence themselves, judges themselves ask for further training in the acquisition and analysis of digital evidence as to no longer rely on other parties explaining to them what the data they are looking at means (Kessler, 2011).

In 2020, there are many challenges that face law enforcement in mobile forensics. The vast amount of security features on devices, relevant privacy laws, bypassing security features, handling uncooperative suspects and companies, data manipulation or obscurification and allowing others to understand the evidence gathered. All these challenges can make gathering evidence very difficult for forensic investigators. To help with these challenges, there are some possible solutions, there are laws in place to help with investigations and suspect compliance if there is enough cause for suspicion for a judge to compel the suspect to comply. There has also been software and hardware developed in order to aid forensic investigators in the process of obtaining data from a mobile device. As technology advances so do the security features being implemented and the laws surrounding the use and

exploration of these. Moving forward, it will continue to be a challenge for law enforcement to gather evidence from mobile devices, to what extent will be unknown, but the ways in which data is accessed and analysed will develop alongside the challenges to come.

Word Count: 3096

References

Turner, A. (2018) '1 Billion More Phones Than People In The World! BankMyCell', *BankMyCell*, 10 July. Available at: https://www.bankmycell.com/blog/how-many-phones-are-in-the-world (Accessed: 2 November 2020).

Participation, E. (5 February 2019) *Regulation of Investigatory Powers Act 2000*. Statute Law Database. Available at: https://www.legislation.gov.uk/ukpga/2000/23/section/49 (Accessed: 31 October 2020).

Raghav, S. and Saxena, A. K. (2009) 'Mobile forensics: Guidelines and challenges in data preservation and acquisition', in *2009 IEEE Student Conference on Research and Development (SCOReD)*. *2009 IEEE Student Conference on Research and Development (SCOReD)*, pp. 5–8. doi: 10.1109/SCORED.2009.5443431.

The Exponential Nature of Password Cracking Costs | Core Security Blog (no date). Available at: https://www.coresecurity.com/blog/the-exponential-nature-of-password-cracking-costs (Accessed: 2 November 2020).

Holmes, A. (21 October 2020) *Police in all 50 states are using secret tools to break into locked phones — and they're using them for cases as low-level as shoplifting, records show*, *Business Insider*. Available at: https://www.businessinsider.com/police-tools-crack-locked-smartphones-2020-10 (Accessed: 7 November 2020).

Priyank Parmer, Dr Ravi Sheth. (July-August 2018) "Logical acquisition of iPhone without Jail Breaking", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN: 2395-602X, Print ISSN: 2395-6011, 4 Issue 9, pp. 01-05, doi: 10.32628/IJSRST184815

Yates, M. (2010) 'Practical investigations of digital forensics tools for mobile devices', in *2010 Information Security Curriculum Development Conference*. New York, NY, USA: Association for Computing Machinery (InfoSecCD '10), pp. 156–162. doi: 10.1145/1940941.1940972.

Wazid, M. *et al.* (2013) 'Hacktivism trends, digital forensic tools and challenges: A survey', in *2013 IEEE Conference on Information Communication Technologies*. *2013 IEEE Conference on Information Communication Technologies*, pp. 138–144. doi: 10.1109/CICT.2013.6558078.

MSAB (no date) *Are there any "court-approved" mobile forensic tools?* www.msab.com Available at: https://www.msab.com/wp-admin/admin-ajax.php?juwpfisadmin=false&action=wpfd&task=file.download&wpfd_category_id=13596&wpfd_file_id=65561&token=ca7bb7c801659f3a9370bdfe326a8d02&preview=1 (Accessed: 14/11/2020)

Chernyshev, M. *et al.* (2017) 'Mobile Forensics: Advances, Challenges, and Research Opportunities', *IEEE Security Privacy*, 15(6), pp. 42–51. doi: 10.1109/MSP.2017.4251107.

Lutes, K. and Mislan, R. (2020) 'Challenges in Mobile Phone Forensics'. Available at: https://www.researchgate.net/profile/Rick_Mislan/publication/264884578_Challenges_in_Mobile_Phone_Forensics/links/543920e70cf204cab1d8d265.pdf (Accessed: 13 November 2020)

Calculator - Photo Vault & Video Vault hide photos – Apps on Google Play (no date). Available at: https://play.google.com/store/apps/details?id=com.hld.anzenbokusucal&hl=en_GB&gl=US (Accessed: 19 November 2020).

'SAN BERNARDINO SHOOTING: 22nd injured victim steps forward, FBI says' (2015) *Press Enterprise*, 9 December. Available at: https://www.pe.com/2015/12/09/san-bernardino-shooting-22nd-injured-victim-steps-forward-fbi-says/ (Accessed: 13 November 2020).

Apple Opposes Judge's Order To Help FBI Unlock San Bernardino Shooter's Phone (no date) *NPR.org*. Available at: https://www.npr.org/sections/thetwo-way/2016/02/17/467035863/judge-orders-apple-to-help-investigators-unlock-california-shooters-phone (Accessed: 13 November 2020).

Kessler, G. (2011) 'Judges' Awareness, Understanding, and Application of Digital Evidence', *Journal of Digital Forensics, Security and Law*. doi: 10.15394/jdfsl.2011.1088.

Police powers to search your phone and social media accounts (no date) *Conspiracy Solicitor*. Available at: https://www.conspiracysolicitor.co.uk/site/our-services/police-powers-phone-social-media/ (Accessed: 6 November 2020).

majo (no date) 'XRY - Extract', *MSAB*. Available at: https://www.msab.com/products/xry/ (Accessed: 6 November 2020).

Is jailbreaking legal and safe? (no date). Available at: https://us.norton.com/internetsecurity-mobile-is-jailbreaking-legal-and-safe.html (Accessed: 8 November 2020).

'How Does Jailbreaking Or Rooting Affect My Mobile Device Security?' (2012) *McAfee Blogs*, 13 June. Available at: /blogs/consumer/identity-protection/how-does-jailbreaking-or-rooting-affect-my-mobile-device-security/ (Accessed: 8 November 2020).

Zapotosky, M. (2016) 'FBI has accessed San Bernardino shooter's phone without Apple's help', *Washington Post*, 28 March. Available at: https://www.washingtonpost.com/world/national-security/fbi-has-accessed-san-bernardino-shooters-phone-without-apples-help/2016/03/28/e593a0e2-f52b-11e5-9804-537defcc3cf6_story.html (Accessed: 12 November 2020).