# Digital Forensics 2: Mobile Forensics Challenges in Investigating Android Devices and their Security Features

*Thomas MacKinnon*
*School of Design and Informatics*
*Abertay University*
*DUNDEE, DD1 1HG, UK*
*Word Count: 3068*

Throughout the last twenty years we have witnessed the exponential growth of the mobile phone industry, as they rapidly evolved from a simple communication method to an essential tool for all aspects of your life. 2007 saw the introduction of the Apple iPhone, which revolutionised the phone market with the features it possessed and became the standard that manufacturers aimed for. However, Apple decided to keep their operating system exclusive to the iPhone, leading to the meteoric success of the open source Android OS, which now runs on an estimated 95% of the three billion active smart phones (Wielen, 2018). The nature of mobile phone use has led to new possibilities for Digital Forensic Investigators, as know there is potential for text messages, phone logs, device location, images and much more to be utilised in a court case. Smart Phones will continue to evolve, gaining new features and properties, meaning that there will be even more potential data to help convict criminals in the future, surely this emerging technology is a godsend to Forensic Investigators? Unfortunately this is not the case. Mobile forensics has proved to be much more challenging than traditional PC forensics, leading to investigators only using the easiest accessible data to aid investigation when dealing with mobile devices. Tools like write blockers that come standard on PC forensics are not as simple on mobile phones, as they tend to change the state of the device making the evidence unusable. There is also a much wider variety of phones and operating systems, meaning an investigator could have zero experience with a suspect device. The Android OS possess many security features that not only block criminals, but also Law Enforcement, leaving Mobile device forensics as a very risky but rewarding practise.

This essay aims to reveal the challenges that Forensic Investigators face when dealing with Android devices, and specifically on how their security features effect gathering of evidence. Topics range from Android features like biometric security and authentication all the way to laws affecting investigators and the issues with mass manufacturing of devices in order to show the difficulties faced in Mobile Digital Forensics.

Herrera (2020) highlights a key security feature of the Android Operating system, being it's locked bootloader until a pin code has been entered. If a device is seized and powers off very little to even zero data can be recovered without the device owners compliance, and a forceful unlock will wipe the entire system (Hoffman, 2017). Android offers a variety of code unlocks for phones, being a pin number, a password or even a drawn pattern. Some of these options are much more appealing to Forensic Investigators, a four digit pin is a lot easier to crack then a long password with many different characters. A peer reviewed study from 2017 revealed pattern passwords to be the weakest form of security by far, as over 60% of the participants were able to replicate the pattern from one demonstration (Aviv et al. 2017). Dealing with Android devices becomes a greater challenge depending on what security features the owner has enabled, as the unlock authentication blocks the

rest of the phones content. For Law Enforcement this is a big issue, getting the pin can be near impossible, or will simply take too much time for the proper court order to be obtained.

Digital Forensic Investigators based in the United Kingdom face problems caused by the law when seizing device's with pin or password protection. If the owner does not comply with the investigators then they have to acquire a court order under section 49 of the Regulation of Investigatory Powers Act (RIPA). This takes a significant time to acquire so many Law enforcers use manipulation and threats, claiming that the owner is committing an offence by not providing access (Ajaz, 2020). Even after the court order has been acquired the suspect can simply play dumb, claiming they have forgotten the pin, in this circumstance the suspect can serve anywhere from two to five years in prison depending on the severity of the crime (Saunders Law, 2018).

The United States of America offer a similar challenge to investigators through the Fourth and Fifth Amendment to the Constitution. The Fourth Amendment prevents law enforcers from unreasonable seizure of a device (Interactive Constitution, 2020), whilst the Fifth Amendment protects the owner from self-incrimination through searching the device (Zerman, 2019). Like in the UK, a court ordered warrant has to be acquired before the owner is legally forced to give up their pin, however many warrants come with limitations which in turn limit investigators. Mobile phones running Android always have some form of password to unlock the device contents, and still do even with the current trend of biometric security, this challenge looks like it will be a permanent problem to investigators.

Biometric Security has been a core feature of Android for the last five years, starting with the introduction of "Face Unlock" with Android 4.0 Ice Cream Sandwich and Fingerprint scanning features with Android 6.0 Marshmallow. Each feature gave users a new way to unlock their devices and some applications, such as mobile banking, used fingerprint scanning as their primary security. To law enforcement this features was a tricky grey area in ethics and policing, as neither the USA or the UK have specific laws in place preventing an officer from forcing an unlock through these methods. In 2019 Judge Kandis Westmore set a precedent ruling by stating that "all logins are equal", protecting the suspects from forced biometric unlocks under the Fifth Amendment (Osborne, 2019). This ruling significantly limits investigators ability to unlock mobile phones for data acquisition without the use specialised tools. Android's Trusted Face unlock was not always effective though, as of last year all devices running Android 10 or below had the feature removed (Khoury, 2019). This was due to a major security flaw, trusted face would unlock the device from a simple picture of the owner. For an investigator this flaw was a gold mine, a mugshot of the suspect would allow all access to the device without the any of the normal issues associated, the removal of this bug further increase the difficulty of mobile forensics.

Kovalchik & Maro (2018) conducted an interesting experiment into bypassing fingerprint scanners on various devices, one being a Samsung Galaxy S8 running Android. The pair managed to retrieve the fingerprint directly from the phone's protective glass and used a 3D printer to create a fake gelatine thumb. The artificial fingerprint was able to unlock every device tested, with the Samsung Galaxy S8 unlocking having a success rate of 60% throughout the multiple attempts. Garcia-Peral et al. (2018) conducted further research into this area of security by testing different materials ability to fake a fingerprint. Their testing shows that Kovalchik & Maro's recreation through gelatine is actually quite ineffective, and was the worst out of the materials tested, with an average unlock rate of *1.33%*. The best material found was white glue with graphite powder sprayed on, which was able to unlock each phone tested. These results do not discredit Kovalchik & Maro's work, as their paper took the form of an extended Abstract, where they focused on one specific issue aiming to be concise with their findings. Their results were effective in their own right, and experimentation with other materials was completely outside the scope of the paper. Garcia-Peral et al. wrote a

traditional research paper, with many different variables for testing, meaning their paper would always overshadow Kovalchik & Maro's results.

This process has seen some practical application, in 2016 Anil Jain of Michigan State University was asked by the police force for help in unlocking a dead man's phone to try and uncover who his murdered was (Planet Biometrics, 2016). Anil was provided with fingerprints from a previous arrest of the victim, and used it to create an artificial thumb print with conductive paper, which was able to unlock the device.

This breakthrough is obviously amazing for Digital Forensic Investigators, but this technique does have significant drawbacks. Anil Jain and his team took three weeks to bypass the fingerprint scanner, Android now has features that requires pin or passcode unlocks after a certain time has passed or if too many failed biometric unlock attempts have been made (Samsung, 2020). If these settings are active then the artificial fingerprint is completely useless, wasting time and resources of the investigators.

The whole process of replicating a fingerprint brings up an ethical concern, the victim could not consent to this practise, and could be breaking the Fifth Amendment. Bryan Choi, a security and law researcher, clarifies this by stating "The Fifth Amendment protects against self-incrimination. Here, the fingerprints are of the deceased victim, not the murder suspect. Obviously, the victim is not at risk of incrimination" (Whyte, 2016). So with this statement it's clear that Forensic teams (at least based in the USA) can use fake fingerprints to unlock a device if the owner is not the suspect of the case. Unfortunately there is no cases in the UK where this technique has been used, and so there is no precedent on the legality of it.

Biometric bypassing only works if the phone remains on, after a reboot the user's pin is needed to unlock the device, making it imperative to keep all suspect devices charged. Forensic teams will carry multiple battery banks with many different wires in order to keep any devices found powered on. However there is always the risk of not having the right wire for the device, many off brand or cheap devices come with a non-standard charging cable which the forensic team does not have. Bennet (2012) states the importance of retrieving any wires or accessories suspected to be used with the device have to be seized in order to minimize the risk of a device losing charge and potentially valuable data. Reiber (2015, Chapter 2, paragraph 23) adds to this by stating that investigators should have an in depth knowledge of how the device communicates with the forensic software through any method (WiFi, Bluetooth, Physical Wire, etc), as there is always the risk of tainting the evidence.

Remote Wiping has been feature of Android devices for years, allowing users to wipe their phone's content in cases of theft or loss of the device, and has been a nightmare for Digital Forensics teams ever since its debut. A case from 2014 saw six seized devices being remotely wiped whilst under the custody of the Dorset Police force (Wakefield, 2014). Most wireless signals have the power to wipe the device, removing any potentially valuable data that could be stored within, so it is of utmost of importance to remove the phone from the network. Faraday cages (and Faraday bags) are utilised by forensics teams to counteract remote wiping, as they prevent connections to any WiFi, Bluetooth or mobile networks to the device. Bennet (2012) states that connection blocking equipment is not always available to police, as bags/cages are reliable but not full guarantee of safety, as some could be a cheaper alternative. Police have also advised clients to place any suspect devices into a microwave, as they help to shield the device from signals. This advice is counter intuitive, as recommending potential suspects to place devices into an appliance with the power to destroy them is completely illogical. Furthermore this recommendation gives suspects plausible deniability for the destruction

of a device, as they can simply say that it was accidentally microwaved rather than a suspicious last minute wipe to destroy evidence. Airplane mode is also used to disable any connections, but does come with the risk of losing the integrity of the data, as it alters the state of the device and is only accessible once the phone has been unlocked (Packt, 2016).

Unlike traditional forensic conducted on Personal Computers, Mobile forensics does not have the extensive documentation and unity that is standard. Manufacturers tend to use the standard Android operating system, but add slight variations that cause great differences between devices of competing brands. Comparing Market shares really emphasises the difference between fields, Windows has a 78% share as of 2020, whilst macOs has 17%, with the remaining 5% shared amongst Linux and other operating systems (Statista, 2020). Mobile Phone Market share is much more varied, Samsung and Huawei both lead the market with a 20% share each, whilst Apple follows behind with a 16% share (Counterpoint, 2020). The remaining 44% contains a variety of Android based Operating Systems, mostly coming out of China with little documentation or existing history. It may seem unfair to compare PC Operating systems to different phone brands, as there are many brands of PCs just like mobile phones. The core distinction to make is that PC manufactures ship their product with a standard OS, whilst mobile manufacturers add variations to the OS thus separating it from its competitors. Aneja et al. (2016, pp. 606) emphasises this difference further by showing the industry standard of yearly phone releases, each containing new hardware and upgrades to the device, often with bugs/exploits being patched on both hardware and software. The sheer variety and constant changes to Mobile devices means Investigators are always behind on the current tech, and any experience with a device could be made useless with a major change.

This also raises the issue with Digital Forensics tools used for Mobile devices, how can a tool keep up with the growing rate of new phones? Well they can't. Investigators have found themselves in a tricky spot where it is not known if their tool will work on the device, and if it will alter data on the device making it forensically invalid. These tools are a significant drain on Law Enforcement budget, XRY is a forensic tool kit used in extraction of data from mobile devices, the starting cost for the kit is $7,990 with a license fee of $2,995 a year (SC Media, 2015). If this tool proves ineffective at investigating a suspect device in a high class case it leave Law Enforcement no option but to purchase another tool or just use low hanging evidence retrieved. As mentioned earlier this is an growing problem as production of new devices increases, tools cannot keep up with the flow of new tech and so Forensic Investigators are left with no way to properly investigate every device seized.

Even with an effective tool Police are still overwhelmed by their backlog of devices, with a total of 12,122 waiting to be examined (ITV, 2020). Time is a growing problem, Investigators tend to avoid deep searches onto suspect devices simply due to the lack of time available. Often the only information gathered for court is the "low hanging fruit" pieces of data that do not require significant time to find and decode. Lee Reiber (2015, Chapter 2, paragraph 38) highlights this problem with an effective metaphor, stating that this form of investigation is "like reading the first and last chapters of a book and then trying to write a review". It is easy to say this, however Law Enforcement have to provide evidence in a timely manner, and cannot risk the forensic integrity of the data, so "low hanging fruit" will continue to be used rather than deep dives into every device. Even traditional methods such as imaging simply can't be performed on Mobile devices without altering the contents.

Android devices produced in China have proven to be a growing threat to Forensic Investigations. Huawei, Vivo, Oneplus are the main players in the Chinese phone market, however the real problem comes from phones without a brand. Unbranded Chinese devices are often produced to a lesser standard than high end phones, as the manufacturers care more about mass producing at the cheapest price. Performing investigations on foreign devices is not easy, as the investigators likely

have no previous experience with the device and have no accessible documentation on how it works. These devices also cause significant issues in investigations due to their lack of IMEI(International Mobile Equipment Identity) number, which prevents the device from being traced. Signal towers can identify devices through the IMEI number thus aiding forensic teams in locating the device (Moore, 2005), so most Chinese phones are therefore untraceable for Law enforcement.

This flaw in design makes unbranded Chinese phones extremely appealing to criminals, having an untraceable device that's hard to crack is perfect for evading law enforcement. India, a long time enemy of China, has banned all Chinese devices from entering the country in order to counteract this problem (Bennet, 2012, pp. 163). The United States of America has followed suit by banning all Huawei devices from the country, due to concerns that the phone's manufacturer were using the devices to spy on US citizens and report back to the Chinese government (Hoyle, 2020). This trend of blocking foreign devices does not look like it will be going anytime soon, as the Trump Administration is pushing their Allies to follow the ban and will likely be banning more Android devices produced in China.

Clearly the art of Mobile Digital Forensics is nowhere near the level that PC forensics is at, investigating a phone is significantly harder for Law Enforcement, requiring more time, skill and resources. Investigators never really know what they are getting into when examining a suspect device, it could a common phone or an unbranded device with no documentation and irregular file systems. Simply accessing the device can be a strenuous task, requiring court orders or owner permission even before any data can be collected. Android OS has been designed to protect their user's device from theft and unlawful access, which will also always negatively affect investigations into these devices. This is a permanent problem for Investigators, as even the manufacturing standards of phones are against them, producing new devices every year leaves Law Enforcement always playing catch up. With such challenges it obvious why Investigators go for "Low Hanging Fruit" evidence, it minimizes the great risk of losing forensic integrity without dealing with all the hassle of mobile forensics, this will always leave potential evidence uncovered. The smartphone revolution has led to many new methods of for Digital Forensics, but also comes with immense challenges that contently plague Investigators. These issues are not going away any time soon, Investigators will simply have to live with the complex problems Android devices cause in Digital Forensics.

# REFERENCES


Ajaz, A. 2019. POWERS OF THE POLICE: WHEN TO PROVIDE YOUR MOBILE PHONE PIN OR PASSWORD. [online] abv Solicitors. Available at: https://www.abvsolicitors.co.uk/articles/ powers-of-the-police-when-to-provide-your-mobile-phone-pin-or-password/ [Accessed 11 November 2020]

Aneja, L. Khanna, A.K. Roy, N.R. 2016. Android phone forensic: Tools and techniques. *2016 International Conference on Computing, Communication and Automation (ICCCA)*. pp. 605-611.

Aviv, A.J. Davin, J.T. Kuber, R. Wolf, F. 2017. Towards Baselines for Shoulder Surfing on Mobile Authentication. *ACSAC 2017: Proceedings of the 33rd Annual Computer Security Applications Conference*. pp. 486-498.

Bennet, D. 2012. The Challenges Facing Computer Forensics Investigators in Obtaining Information from Mobile Devices for Use in Criminal Investigations. *Information Security Journal: A Global Perspective*. Volume 21, Issue 3, pp. 159-168.

Counterpoint. 2020. Global Smartphone Market Share: By Quarter. [online] Counterpoint. Available at: https://www.counterpointresearch.com/global-smartphone-share/ [Accessed 18 November 2020]

Garcia-Peral, A. Goicoechea-Telleria, I. Husseis, A. Sanchez-Reillo, R. 2018. Presentation Attack Detection Evaluation on Mobile Devices: Simplest Approach for Capturing and Lifting a Latent Fingerprint. *2018 International Carnahan Conference on Security Technology (ICCST)*. pp. 1-5.

Herrera, L.H. 2020. Challenges of acquiring mobile devices while minimizing the loss of usable forensics data. *2020 8th International Symposium on Digital Forensics and Security (ISDFS)*.

Hoyle, A. 2020. Huawei ban timeline: Qualcomm reportedly gets OK to sell 4G chips to Chinese company. [online] Cnet. Available at: https://www.cnet.com/news/ huawei-ban-full-timeline-us-sanctions-china-trump-administation-qualcomm/ [Accessed 18 November 2020]

Interactive Constitution. 2020. Fourth Amendment: Search and Seizure. [online] Interactive Constitution. Available at: https://constitutioncenter.org/interactive-constitution/amendment/amendment-iv [Accessed 12 November 2020]

ITV. 2020. Thousands of digital devices awaiting analysis by police investigators. [online] ITV news. Available at: https://www.itv.com/news/2020-04-22/ thousands-of-digital-devices-awaiting-analysis-by-police-investigators [Accessed 18 November 2020]

Khoury, R.E. 2019. Trusted Face smart unlock method has been removed from Android devices. [online] Android Police. Available at:

https://www.androidpolice.com/2019/09/04/
trusted-face-smart-unlock-method-has-been-removed-from-android-devices/ [Accessed 12 November 2020]

Kovalchik, M. & Maro, E. 2018. Bypass Biometric Lock Systems With Gelatin Artificial Fingerprint. *Proceedings of the 11th International Conference on Security of Information and Networks (SIN '18).* pp. 23-24.

Lumb, D. 2016. Police get dead man's finger 3D-printed to unlock his phone. [online] Engadget. Available at:
https://www.engadget.com/
2016-07-21-police-get-dead-man-s-finger-3d-printed-to-unlock-his-phone.html [Accessed 14 November 2020]

Moore, T. 2004. The economics of digital forensics. [online] ResearchGate. Available at:
https://www.researchgate.net/profile/Tyler_Moore2/publication/
216757779_The_economics_of_digital_forensics/links/549b030d0cf2b80371371814.pdf [Accessed 18 November 2020]

Osborne, C. 2019. Police can't force you to unlock your phone by iris, face or finger. [online] ZD net. Available at:
https:
//www.zdnet.com/article/police-cant-force-us-citizens-to-unlock-their-phone-by-face-or-finger/ [Accessed 12 November 2020]

Packt. 2016. Digital and Mobile Forensics. [online] Packt. Available at:
https://hub.packtpub.com/digital-and-mobile-forensics/ [Accessed 18 November 2020]

Reiber, L. 2015. *Mobile Forensic Investigations: A Guide to Evidence Collection, Analysis, and Presentation.* First Edition. McGraw Hill Education, New York.

Samsung. 2020. Samsung phone requires additional security for biometric Lock screen.[online] Samsung. Available at: https://www.samsung.com/us/support/troubleshooting/TSG01001281/ [Accessed 18 November 2020]

Saunders Law. 2018. Prosecuted for your password. [online] Saunders Law. Available at:
https://www.saunders.co.uk/news/prosecuted-for-your-password/ [Accessed 12 November 2020]

SC Media. 2015. MSAB XRY Office. [online] SC Magazine. Available at:
https://www.scmagazine.com/review/msab-xry-office/ [Accessed 18 November 2020]

Statista. 2020. Desktop PC operating system market share worldwide, from January 2013 to July 2020. [online] Statista. Available at:
https://www.statista.com/statistics/218089/global-market-share-of-windows-7/ [Accessed 18 November 2020]

Tayeb, H.F. & Varol, C. 2019. Android Mobile Device Forensics: A Review. *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*. pp.18.

Wakefield, J. 2014. Devices being remotely wiped in police custody. [online] BBC news. Available at: https://www.bbc.co.uk/news/technology-29464889 [Accessed 18 November 2020]

Whyte, M. 2016. Police asked this 3D printing lab to recreate a dead man's fingers to unlock his phone. [online] In The Loop. Available at: https://www.in-the-loop.net.au/police-asked-3d-printing-lab-recreate-dead-mans-fingers-unlock-phone/ [Accessed 15 November 2020]

Wielen, B.V.D. 2018. *Insights into the 2.3 Billion Android Smartphones in Use Around the World.* [online] newzoo. Available at: https://newzoo.com/insights/articles/insights-into-the-2-3-billion-android-smartphones-in-use-around-the-world/ [Accessed 20 November 2020]

Zerman, E. 2019. Can police force you to unlock your phone?. [online] Android Authority. Available at: https://www.androidauthority.com/police-unlock-phone-rules-rights-998683/ [Accessed 12 November 2020]