CMP416 Unit 1 By Christopher Di-Nozzi 1800317

As their popularity has grown, mobile devices have begun to play a pivotal role in criminal investigations. Carried by most every day, they contain vast amounts of information about their owner, acting like virtual journals. Even over the last five years, the number of smart phone users has close to doubled, and this increase shows no signs of slowing down, as shown in Figure 1.

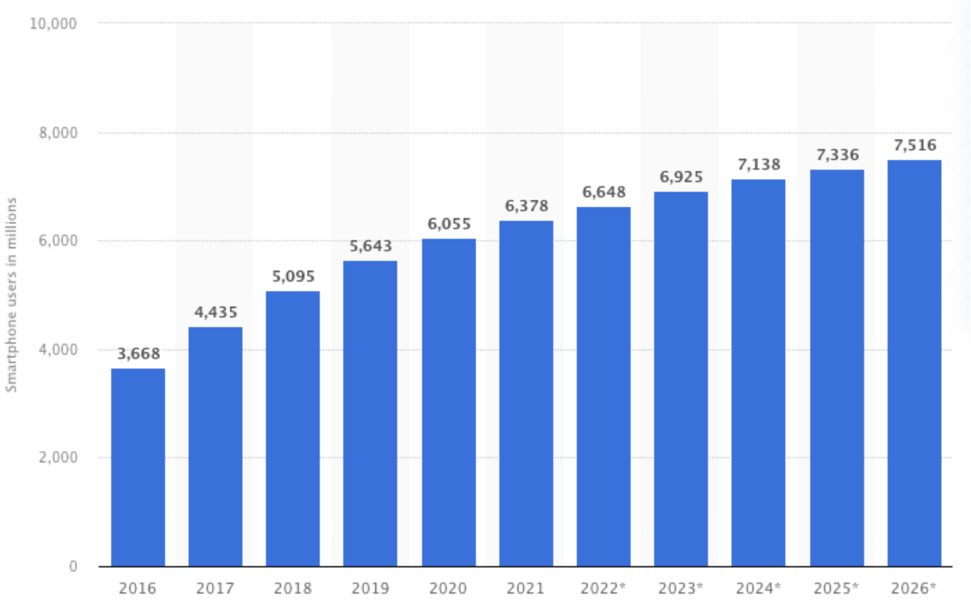


Figure 1: Number of smartphone users from 2016 to 2021 and predicted to 2026, (Statista, 2021).

The first notable case of data from a mobile phone playing a key role in a court case was in 2008 as part of the murder of Oscar Grant at Fruitvale Station in Oakland, California. Video was recorded of the event using a mobile phone that was later used as evidence in court. This led to the conviction of BART police Officer Johannes Mehserle, (Bulwa & Swan, 2018). Since then, mobile phones have continued to play a pivotal role in the court room, not just because of what they capture on tape but because of the information they store inside.

However, using mobile devices as evidence in court poses many more challenges than traditional digital forensics on personal computers. The aim of this report is to discuss a handful of the most prominent issued faced by law enforcement performing mobile forensics and the challenges they cause. This paper will mainly focus on the issues posed by the iPhone Operating System (iOS) run exclusively by Apple iPhones including its locked down nature, powerful encryption, security features and file system. It will also touch of the impact that the lack of consistency within mobile device operating systems poses to creating effective tools to perform forensics on mobile devices.

Having the second largest market share of mobile devices iOS devices are commonplace within criminal investigations and provide their own unique challenges for law enforcement conducting digital forensics investigations against them. iOS has run on every Apple iPhone since the first iPhone released in 2007. The OS has evolved drastically since its first introduction over a decade ago, however, some key tenements of the system have remained. The most problematic of these being that iOS is very closed off, especially when compared to Android, a Linux based mobile operating system. This focus on privacy has only increased in the last couple of years with the introductory of Apple's iPhone privacy campaign first starting in 2019 with the slogan "Privacy. That's iPhone.", (Wuerthele, 2019). This strong stance on privacy is good for consumers but is a massive obstacle for law enforcement attempting to recover evidence from iOS devices. The issues of security and privacy within iOS device forensics have been explored in great depth by Dave Bullock, Aliyu Aliyu, Leandros Maglaras, and Mohamed Amine Ferrag, (Bullock, et al., 2020). This review looked at the existing challenges faced by law enforcement conducting digital forensics against iOS devices and categorised them into three types: technical, legal, and resources.

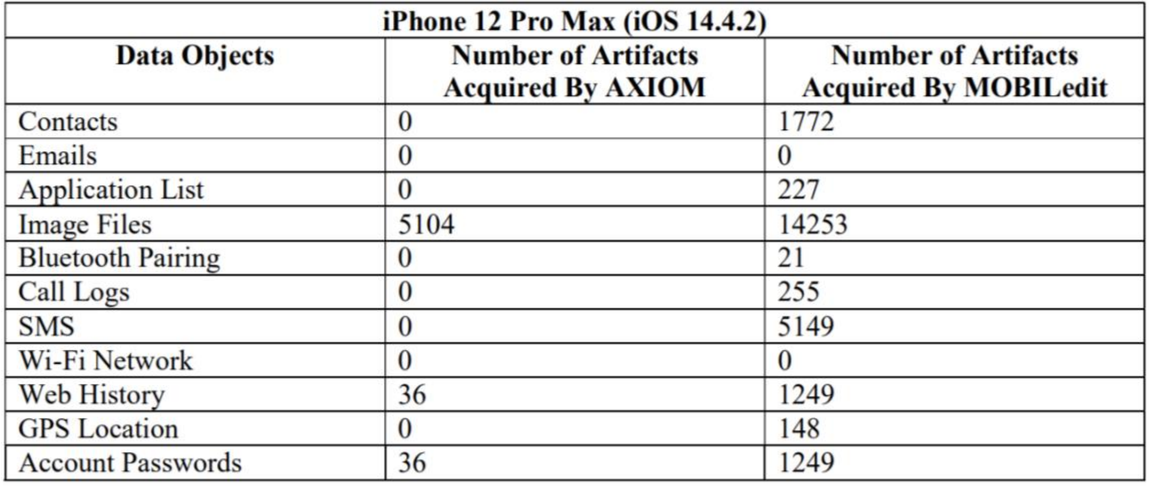
The technical challenges in this paper examined file extraction, security features, and constant security updates. Due to the nature and scope of the report, it did not go into as much detail about the technicalities and effectiveness of certain data extraction tools or techniques in the same way that other papers like (Shakir, et al., 2021) did, however, it provides a simple but high quality overview of the technical challenges posed by iOS. The researchers present the idea that an alternative way to extract data from a device is from backups made by the device and the backup applications that facilitate them. The research referenced by Bullock et al. was published in 2018 by researchers from Taiwan, (Huang, et al., 2018). It showed, through a handful of experiments with different iOS cloud providers (Google Drive, Dropbox, and OneDrive), that a large amount of data could be recovered from these services via caches, logs, and file thumbnails. While this is a less traditional technique, this approach towards cloud backups could server law enforcement well as it provides an additional area in which to find evidence. Although the research conducted by Huang et al. was published in 2018, making it quite recent, it could benefit from being reconducted due to how quickly the iOS changes.

However, the obvious challenge of first accessing these backups does exist. Bullock et al. further discussed the security features built into iOS that prevent this data being accessed. Being introduced in iOS 2, iOS devices are locked down using a combination of encryption and digital signing. Encryption is one of the biggest challenges faced by law enforcement. Charles Edge and Rich Trouton explain iOS encryption in good detail in their book "Apple Device Management", (Edge & Trouton, 2020). The most recent iOS devices have a Secure Enclave coprocessor and a dedicated AES-256 cryptography engine used to encrypt the hardware that can only be decrypted using the fingerprint sensor (Touch ID) or facial recognition (Face ID). This secure enclave sits between the system memory and the data storage, runs its own OS, and is not directly accessible by the OS itself or any applications that run on it. The Secure Enclave holds all the private keys, which are unique to each device, and handles encryption and decryption for all applications. This hardware encryption is combined with a filesystem encryption named Data Protection which creates a new AES-256 private key for every file on the device which is then stored with the other file private keys. The AES-256 standard is essentially uncrackable with the computing power that currently exists. The only hope is using side channel attacks. Alexander S. La Cour and peers have conducted successful research into side channel attacks against iOS devices via their wireless charging feature. This cutting edge technique allowed the researchers to identify webpages loaded by the device with an 87% accuracy against an iPhone 11, however, this technique is yet to be used in an attempt to gain encryption keys, (La Cour, et al., 2021). Encryption is automatically enabled on the device when a pass code is set. These passcodes can range from 4 digits to long alphanumeric strings. Attempting to guess these passcodes is potentially a viable option, however, a feature can be enabled to wipe the device after 10 incorrect guesses, rendering it useless as evidence. Even if that feature is not enabled, after a threshold, each incorrect guess causes the device to lock itself for longer and longer periods of time. As mentioned prior, iOS devices can also be unlocked using bio metrics. This has played to the advantage of law enforcement in the past. A notable case of this was in 2018 when Grant Michalski has his home in Ohio searched by the FBI with a warrant that allowed them to force him to unlock his iPhone X using Face ID, (Brewster, 2018). This made accessing the data on his phone trivial and was a big step forward for law enforcement. However, this approach to biometrics is not universal. A similar request was made in 2019 to Californian Judge Kandis Westmore to force suspects to unlock their devices using Face ID or Touch ID, with the logic being that a suspect giving a copy of their fingerprint, or a sample of their DNA is already the standard expectation when dealing with suspects. However, Westmore ruled that biometrics should be classified as testimonials in the same way that passwords and PIN numbers are, and must be spoken by the suspect, thus protecting them under the Fifth Amendment, (Wakely, 2019). The debate over biometrics is an ongoing challenge for law enforcement. Forcing suspects to unlock devices using biometrics could make the issue of locked devices history but it is yet to be seen which line of the debate the justice system will fall on. Furthermore, even if the majority rule on the side of biometrics being unprotected, iOS devices still will not become open books. (Bullock, et al., 2020) further discusses how the devices password or passcode can be required even if biometrics are usually used to unlock the device. If the device has just been powered on or has not been unlocked in more than 48 hours, if the password has not been used in over 156 hours and facial recognition has not been used in 4 hours, if the device receives an unlock command, or after 5 unsuccessful biometrics attempts. Therefore, while biometrics could be a loophole to have suspects unlock devices, this is a scenario Apple have already prepared for and could possibly cause them to tighten their security even further. The final technical issue discussed by (Bullock, et al., 2020) is that of constant device updates that make changes to the device. Bullock et al. do not go into this issue in as much detail as (Shimmi, et al., 2020) regarding SQLite database structures, however, it does touch on how quick Apple are to patch security vulnerabilities, especially vulnerabilities that allow custom code to be side loaded. This can lead to the device being “jailbroken”, comparable rooting an Android device, allowing custom code to be run. This can be very advantageous to law enforcement since it can allow them to gain deeper access into the device, allowing bit for bit copies of the device to be made. However, if law enforcement themselves jailbreak the device, the integrity of the data on the device could be called into question since the process of jailbreaking makes fundamental changes to the device.

(Bullock, et al., 2020) also discuss the legal issues that Apple pose to law enforcement. Apple have never been willing to work with law enforcement to assist with accessing user data. This is great news for users who value privacy but also a compelling selling point for criminals looking for a device that will be a challenge to law enforcement. Apple demonstrated their strict privacy stance famously in 2015 when asked to assist with unlocking a device in connection to Syed Rizwan Farook and the San Bernardino mass shooting. The FBI did not want to risk wiping the phone by attempting to brute force it and therefore reached out to Apple for assistance, only to be refused any help. Apple was backed up in this stance by other big tech companies including Google, Facebook, and Amazon, (Hack, 2016). Whether or not Apple should help law enforcement access their customers device is out of the scope of this report, however, Apple’s attitude, along with many other big tech organisations, towards law enforcement continues to be a hurdle, especially as more security features are implemented into these devices.

The research conducted by Bullock et al. provides a thorough overview of the issues faced by law enforcement tackling iOS. Being published in 2020, it is still satisfactorily accurate with its analysis of the different issues using a variety of up-to-date sources.
Another aspect of iOS that continues to be a challenge is its file systems. This issue was explored in depth in a paper by Samiha S. Shimmi, Gokila Dorai, Umit Karabiyik and Sudhir Aggarwal, (Shimmi, et al., 2020). The IOS filesystem uses SQLite databases to store large amounts of data about the device and the applications installed onto it. When forensics examinations are being performed on IOS devices, this data is often obtained via backups of the device and then examined using automated tools to extract useful information from the back up. These tools rely on the structure of the SQLite databases staying the same, however, these databases often change with IOS and application updates. This lack of consistency in structure leads to tools becoming obsolete rapidly. This poses an obvious challenge for law enforcement since any bespoke tooling created for IOS devices can very quickly become outdated by an update. When tooling becomes obsolete there is an inevitable downtime before tools can be updated to work on the new database structure. Shimmi et al. proposed a tool to help tackle this issue. This tool was designed to analyse the SQLite databases within iOS backups and compare them to identify differences. A tool like this would greatly assist in updating tooling to work with new versions of iOS and thus assist law enforcement in extract useful data from iOS backups. While it is a useful tool, it does not fully automate the process, requiring analysis to be done by someone with the knowledge to update tooling. By developing this tool further and implementing it with notable iOS forensics tools this research would be dramatically more useful.

The lack of effective, quality tooling to is another big issue facing law enforcement when conducting mobile digital forensics. Due to the dominance of Windows in traditional digital forensics, there is a large variety of reliable tools that exists to extract data from, and analyse information stored on these systems. In comparison, mobile forensics lacks this maturity in tooling due to the huge variety of devices and operating systems. While there does exists reputable tools for mobile forensics, like Elcomsoft's iOS forensic toolkit or the XRY toolkit, they are expensive and licensing more than one of these tools for multiple analysts quickly adds up. The opensource alternatives, while often free and more flexible, are often out of date and unreliable. This challenge is made even harder by the variety of mobile devices and OSs, particularly for Android devices which can run a variety of slightly tweaked OSs on differing hardware. A study was conducted by Htar Htar Lwin, Wai Phyo Aung, and Kyaw Kyaw Lin that compared a handful of data acquisition tools for Android devices to evaluate their efficiency at extracting data, (Lwin, et al., 2020). The three tools, Android Debug Bridge backup, Magnet Acquire, and Belkasoft Acquisition tool were used to extract data from two different devices running two different versions of Android, 6.0.1 and 7.1.1. The two devices were rooted, and the three tools were used against the device. The researchers performed hash calculations to ensure the integrity of the data and the acquired data was analysed using Autopsy and Belkasoft Evidence Center. The results showed that all three tools extracted different amounts of data about different artefacts on the devices. The research concluded that multiple tools had to be used to accurately acquire data from an Android device due to each tool missing different pieces of data from the devices. The reason this poses a challenge to law enforcement is that it causes them to be dependent on using multiple tools to get as much data as possible, rather than just a single, reliable tool. Running more tools against a device increased the chance of integrity issues or causing damage to the device. This study could be improved upon further by using a wider variety of data acquisition tools against the devices and comparing them against similar tools for iOS devices to analyse the different challenges faced by each. A study of this nature was conducted by Amer Shakir, Muhammad Hammad, and Muhammad Kamran as part of a master thesis. This research compared two tools, Magnet AXIOM and MOBILedit, on their ability to extract data from iOS and Android devices, using two devices running different versions of Android (5.1.1 and 8.0.0), and two devices running different versions of iOS (13.5.1 and 14.4.2). All four devices had been used daily which populated them with data reflective of regular use. All four devices had both tools run against them after being put into airplane mode to protect the devices integrity. The results found by Shakir et al. (2021) were consistent with the overall results of Lwin et al. with both tools uncovering different data that the other missed. Additionally, Shakir et al. demonstrated the difficulty of extracting data from iOS devices. While MOBILedit managed to extract a notable amount of data from both iOS devices, AXIOM extracted a fraction of the same information, failing to extract data in many of the categories. Part of the results can be seen in Figure 2.



iPhone 12 Pro Max (iOS 14.4.2)		
Data Objects	**Number of Artifacts Acquired By AXIOM**	**Number of Artifacts Acquired By MOBILedit**
Contacts	0	1772
Emails	0	0
Application List	0	227
Image Files	5104	14253
Bluetooth Pairing	0	21
Call Logs	0	255
SMS	0	5149
Wi-Fi Network	0	0
Web History	36	1249
GPS Location	0	148
Account Passwords	36	1249

Figure 2: Results from the report by (Shakir, et al., 2021) showing the number of files extracted by two different tools run against an iPhone 12 Pro Max running iOS 14.4.2.

This study could have been improved by incorporating a wider variety of tools for both Android and iOS devices to compare more than just two. This could have demonstrated better where other tools fall short, or if there is another tool that outperforms the rest. Both these studies demonstrate how a lack of effective tooling can cause challenges for law enforcement when carrying out mobile forensics. The necessity to use multiple tools to extract as much information as possible not only increases time and cost but calls into question whether all the data has been extracted from the device. Furthermore, the difference in tools ability to extract data from Android devices compared to iOS devices demonstrates the difference the OS of the device can make.

This report has examined a number of academic papers to present and discuss a few of the challenges faced by law enforcement during mobile digital forensics. In particular, the challenges brought about by iOS were examined. This included file extraction and found that while traditional file extract from an iOS device proved difficult, lots of interesting data could be extracted from cloud back up files installed on the device. This brought in the challenge of encryption. With Apples strong stance on privacy and fortified security system, this is a huge continually challenge for law enforcement, with most useful techniques and tricks being quickly nullified by Apple. While there has been some success for law enforcement using warrants to force suspects to unlock their devices using Face ID and Touch ID, it is still debated whether this practice should be legal, or if these biometrics should be treated the same way as passwords and PIN numbers. Finally, iOS posed an issue around their constant updates and changes. Not only is this a factor that prevents any side loading techniques working in the long term, it also constantly changes the SQLite database structure used to store most of the data on the device. This causes tools to become obsolete with each update, but a solution to help update these was proposed. The issue of tooling was further discussed. It was found that the existing tools for mobile forensics are widely inconsistent with the amount and types of data they retrieve, particularly on Android devices. The tools used against iOS were even more inconsistent, with one tool retrieving only a fraction of the data of the other. This could lead to important evidence being left on the device if not extracted properly or force law enforcement to purchase and use a multitude of different tools to give them the best chance of retrieving all the data.

Bibliography

Brewster, T., 2018. *Feds Force Suspect To Unlock An Apple iPhone X With Their Face.* [Online]
Available at: https://www.forbes.com/sites/thomasbrewster/2018/09/30/feds-force-suspect-to-unlock-apple-iphone-x-with-their-face/?sh=1ec4661e1259
[Accessed 14 Nov 2021].

Bullock, D., Aliyu, A., Maglaras, L. & Ferrag, M. A., 2020. Security and privacy challenges in the field of iOS device forensics. *Electronics and Electrical Engineering,* Volume 4, pp. 249-258.

Bulwa, D. & Swan, R., 2018. *10 years since Oscar Grant's death: What happened at Fruitvale Station?.* [Online]
Available at: https://www.sfchronicle.com/bayarea/article/10-years-since-Oscar-Grant-s-death-What-13489585.php
[Accessed 1 Nov 2021].

Edge, C. & Trouton, R., 2020. Endpoint Encryption. In: A. Bakir, ed. *Apple Device Management.* Berkeley(CA): Apress, pp. 343-349.

Hack, M., 2016. The implications of Apple's battle with the FBI. *Network Security,* 2016(7), pp. 8-10.

Huang, C.-T.et al., 2018. Mobile Forensics for Cloud Storage Service on iOS Systems. *IEICE*, pp. 178-182.

La Cour, A. S., Afridi, K. K. & G., S. E., 2021. Wireless Charging Power Side-Channel Attacks. *arXiv,* pp. 1-13.

Lwin, H. H., Aung, W. P. & Lin, K. K., 2020. Comparative Analysis of Android Mobile Forensics Tools. *IEEE Conference on Computer Applications,* pp. 1-6.

Shakir, A., Hammad, M. & Kamran, M., 2021. *Comparative Analysis & Study of Android/iOS Mobile Forensics Tools,* Halmstad: Halmstad University.

Shimmi, S. S., Dorai, G., Karabiyik, U. & Aggarwal, S., 2020. Analysis of iOS SQLite Schema Evolution for Updating Forensic Data Extraction Tools. *International Symposium on Digital Forensics and Security* , Volume 8, pp. 1-7.

Wakely, M., 2019. *California Judge Makes Major Decision in Biometric Privacy Rights.* [Online]
Available at: https://www.biggerlawfirm.com/california-judge-makes-major-decision-in-biometric-privacy-rights/
[Accessed 14 Nov 2021].

Wuerthele, M., 2019. *'Privacy. That's iPhone' ad campaign launches, highlights Apple's stance on user protection.* [Online]
Available at: https://appleinsider.com/articles/19/03/14/privacy-thats-iphone-ad-campaign-launches-highlights-apples-stance-on-user-protection
[Accessed 13 Nov 2021].