Discussing How Anti-Forensics Techniques Present Continuous Challenges to Forensic Investigators and the Law

Finlay Reid – 1904629

CMP416: Digital forensics 2

Mobile devices, most notably mobile phones have seen a 2.7 billion increase in users over the past 5 years according to Statista(O'Dea, 2021). With the release of the first modern smartphone in the late 1990s, this evolution of mobile technology helped propel the device into outnumbering its counterpart, the desktop computer(Petrov, 2021). The role mobile phones play in a user's day to day life has also shifted, becoming significantly more of a personal diary than a device primarily used for communication. Data related to a individuals most intimate experiences with critical information such as banking accounts, social media info, and location data remain stored within this portable machine. Due to the nature of data stored on the device, users and manufactures became increasingly concerned with the lack of security and the risk malicious users posed to the contents inside mobile devices. While the mobile revolution raged on and mobile phones became ubiquitous globally, a new field of forensics emerged, known as mobile forensics. And this development, brought about the antonym of mobile forensics, Anti mobile forensics.

Anti-forensics is defined as "Techniques that attempt to compromise the availability or usefulness of digital evidence" in the Handbook of Research on Computational Forensics (Li, 2010). The techniques employed by malicious users attempting to derail mobile forensic investigations include hiding data, data obfuscation, data forgery, and secure wiping. This presents a host of challenges for mobile forensic analysts, for instance failing to secure key evidence from a mobile phone, in a case where this information is pivotal. Asking the question of "What are the challenges faced by law enforcement in terms of mobile forensics?" and what is the potential in anti-forensics techniques challenging mobile forensics analysts. The aim of the essay is to thoroughly discuss the issues law enforcement encounter in mobile forensics due to anti forensics measures, while critically analysing and appraising relevant papers related to anti forensics.

The following critical essay discusses the topic of anti-forensics and the challenges these techniques create for mobile forensic analysts. Critiquing the basic techniques of mobile anti-forensics such as physically destroying the hardware to more complex methods in cold boot attacks and sudden death measures. Furthermore, describing how suspects look to undermine the regulations set by bodies within the field of mobile forensics and the inherent differences between desktop forensics. In the later stages of the paper commercially available anti forensics applications are explored, examining the effectiveness of these programs using industry leading forensics tools. The real-world effects of anti-mobile forensics are then considered, with a discussion relating to the consequences of anti-forensics on organizations. A case study is detailed, discussed, then analysed to further expand on the element of a real-world example linking back to the consequences of anti-forensic techniques on law enforcement.

The simplest form of anti-forensics requires minimal expertise and involves physically destroying the data in the mobile phone. Destroying the data located on the devices hard drive can be achieved through the use of any blunt force instrument. Criminals can accomplish the same outcome through more finesse, utilising strong magnets to demagnetize the media or acid to dissolve the device. Primitive techniques such as these are rarely employed due to loss of hardware and expense this

puts on the criminal. A cleaner approach is preferred, enabling for a chance of data recovery after the device has been investigated.

One example of an anti-forensic technique employed by criminals is known to mobile forensic analysts as sudden death. An application is installed on the hosts device, running in the background the program monitors the phones internal logs. If the mobile phone detects the device has been connected to a forensic tool, the phone will initiate a shutdown protocol erasing all data located on the phones internal hard drive. A limitation of this anti-forensics' method relates to the human element of a mobile forensics investigation, analysts will presumably discover that the process of data recovery has failed, prompting for an analyst to use a tool such as XRY. This industry leading forensics tool enables investigators to circumvent the phones operating system gaining access to any deleted or hidden data. A strongly associated anti forensics technique involves the criminal completely overwriting the data located on the device, for instance preforming the technique correctly ensures the odds of data recovery are minimal. The technique has been defined as artifact wiping and can be implemented through numerous methods. One of these procedures entails the user creating a modified recovery image, subsequently moving all their critical files over to external storage. Succeeding the transfer of files, the devices memory is overwritten, and the data is copied back to its original location. Limitations of this artefact wiping technique include the prospect of the wipe failing to remove all the data on the device. Furthermore, the wiping process may leave evidence on the device alerting the forensic analyst.

Criminals attempting to disrupt a mobile forensics investigation have the option to exploit the processes and tools used by mobile forensics analysts rather than the definite hardware. Central bodies such as ACPO and NIST regulate the field of mobile forensics through regularly updated guidelines. Understanding this information anti forensic tools have been developed with the intention of committing analysts to a decision between abiding by the rules set from relevant bodies or violating them to gain critical evidence (Distefano, Me and Pace, 2010). An instance of this involves concealing data by means of a program that permits users to set a single password protected folder. If the analyst attempts to access the data, it will be deemed to have been modified therefore breaking rule one of the ACPO guidelines "That no action is taken that should change data held on a digital device including a computer or mobile phone that may subsequently be relied upon as evidence in court" (An Explanation of ACPO Guidelines for Digital Based Evidence, 2021). The paper has its limitations however as it fails to mention to the reader how the program is activated and how the data is returned if the password is incorrect a set number of times. The results from the experiment sufficiently details how long the device takes to conceal the specified data. At 10 seconds depending on the quantity of data, suggesting that the hiding process is action sensitive when connected to a forensic tool. As there are no details included pertaining to the process of data restoration it can be presumed that the data is manually restored by the user after the analysts have returned the mobile device(Distefano, Me and Pace, 2010). This method of anti-forensics is evidence of the growing intellect of criminals attempting to disrupt forensics investigations, further increasing the challenge mobile forensics analysts encounter.

Due to complex nature of a mobile phones design a thoroughly different form of analysation is required when compared with their counterpart the desktop computer. With the field of mobile forensics being relatively new dating back to the late 1990s, early 2000s and a mobile device's integrated design. The combination of these two variables makes numerous methods of data collection employed for personnel computers redundant. As forensic analysts are required to disassemble the phone and remove the surface mounted memory chips, which is a delicate and

highly risky procedure to complete a component analysis. Furthermore, there is no direct way in which to access the mobile devices internal storage. Even so removable storage including sim cards and memory cards can in fact be removed then examined. As anti-mobile forensics is still a new discipline with emerging difficulties, there is no standard classification related to the field. However, in the following paper four broad categories are suggested for anti-forensic methods including destroying evidence, hiding evidence, eliminating evidence sources, and counterfeiting evidence(anti-forensics consensus, 2006). The paper was originally intended for standard anti forensics involving desktop computers, but the categories can be applied to any forensic field including mobile forensics. The limitations of these definitions are in lack of technical language and the definitions fail to cover all the anti-forensics techniques due to date of the conference. As the discipline is constantly evolving new methods of anti-forensics are being discovered and definitions must be updated to incorporate these new techniques. A more fleshed out, technical and up to date classification is included in the paper (Karlsson, K.J. and Glisson, W.B., 2014). Categories are defined as data hiding, artifact wiping, trail obfuscation and attacks against processes/tools. These categories represent todays anti forensics methods to a higher degree, greater than the classifications described in the senior paper(anti-forensics consensus, 2006).

Mobile forensic analysts rely heavily on the basic interfaces utilized by mobile devices to analyse, which is endorsed by both the Association of Chief Police Officers (ACPO) and American National Institute of Standards and Technology (ACPO,2021) (Ayers, R., Brothers, S. and Jansen, W., 2013). Due to the heavy reliance on basic operating system functions and the simple process of installation when downloading 3rd party applications, there has been several apps developed with anti-forensic functionality. Research has been undertaken and found successful, in modifying the android operating system to deceive forensics tools using falsified data (Karlsson, K.J. and Glisson, W.B., 2014). In the aforementioned paper mobile forensic tools such as XRY and Celebrite are successfully fooled through a modified version of the android operating known as Cyanogen. The anti-forensic techniques utilized in conjunction with the operating system allow for the mobile device to prevent the installation of forensic tools, while enabling the device to create falsified data. Furthermore, the operating system creates large delays when attempting to extract data and can completely prevent the data extraction process altogether. The technique described in this paper is more effective than the methods described previously, due to this method modifying the actual operating system of the device and its ability to obstruct forensic apparatus through fabricated data. Rather than a simple removal of condemning data.

Whether on android, IOS or another mobile operating system there is numerous anti forensic tools available at the commercial level and these have been analysed in papers fulfilled by mobile security professionals. The following paper conducted an experiment analysing anti-forensic tools accessible for smartphones on two devices the HTC Desire HD and iPhone 3G, both using their standard operating systems, Android and IOS (Sporea, Aziz and McIntyre, 2021). In order to analyse the applications appropriately two anti-forensic tools were employed, the Paraben Device Seizure and Oxygen Forensic Suite, two highly respective pieces of technology. An evaluation report done by the Criminal Justice Electronic Crime Technology Center on the Paraben Device Seizure confirmed the effectiveness of this mobile forensic tool. Describing how the forensic apparatus is effective in its main goal of extracting data from mobile devices and how the tool presents data in a readable format (Paraben device seizure, 2021). Additional addons are available to analysts inducing the opportunity to export to PC and data recovery, all this for over 4000 devices. The Oxygen Forensic Suite is equally formidable in data acquisition, offering a service which can acquire data from over 19500 mobile phones and undertake in depth data analysis.

The experiment conducted involved testing applications related to different anti-forensics techniques such as file wiping, encryption, stenography and spoofing. For instance, an application named file shredder was utilized on android, while on IOS the application 'iShredder' was examined. Both tools fall under the file wiping category and attain their goal of data removal through having selected files overwritten with random data, essentially destroying the files. The results from the file wiping section of the experiment, display that both the high-end forensic tools failed to identify any data wiping activity on the mobile device. In the encryption section of the experiment the results were similar, using the LUKS Manager which offers encryption to virtual folders on Android devices. A virtual volume was created through the application and data was stored; the forensic tools however did detect the volume but were unable to successfully read the data within the encrypted volume. In the next two sections of the investigation, Steganography and Spoofing, the results followed the same pattern. Results of the experiment demonstrate the availability of commercial applications that are free and require minimal technical knowledge to operate, that can fool high end forensic tools. Furthermore, these applications are shown to be extremely effective when combined. This paper thoroughly demonstrates the risks posed by anti-forensic techniques within the field of mobile forensics. Due to the sheer availability of anti-forensics applications and the wide range of techniques that disrupt even the industry leading tools of mobile forensics investigations. A limitation of the paper and its contained knowledge is related to the date of publication, as the software used in the experiment is out of date. Including the operating system versions, applications and forensic tool implementations. Anti-forensics measures have progressed further since the publication of this paper not just mobile device software. Another instance of the papers limitation is the failure to test another operating system such as the windows phones OS.

An oversight in the research of anti-mobile forensics involves the risks these techniques pose to organizations through their employees and how the usage of mobile phones in the workplace could be used to thwart a mobile forensic investigation. The paper examines these issues to a certain extent and more, by first describing the anti-forensic technique data hiding using cryptography (Omoloa, K. and Abadeb, E., 2019). Expanding on this, the paper suggests that criminals who utilize a complex password when encrypting the data through a full disk encryption, can force analysts to abandon the brute force attacks. This statement is correct due to length of the decryption process therefore enabling the suspect to delay the investigation achieving the goal through the use of anti-forensic measures. An area in which the paper fails to discuss is in relation to the weaknesses of a full disk encryption, primarily with a cold boot attack. The security measures of this encryption method can be fully bypassed using the attack, at its simplest the technique operates by cold booting a machine then attempting to dump the data within memory, stealing the encryption keys.

A mobile devices memory is thought as a secure place for critical data due to the inbuilt security mechanisms within the device, both at the software and hardware level. As these mechanisms are highly respected, important data is stored within memory and the cold boot attack can bypass these security implementations. By exploiting a weakness in the DRAM chips, a memory image at runtime is recovered, enabling for sensitive data to be obtained. The following paper completes a thorough investigation into how the cold boot attack functions (Zheng, J, et al., 2017). Examining the exploitable weaknesses found within a Dynamic memory chip and detailing the approach to be taken to protects AES keys from being acquired by forensics tools. The process of protecting AES keys from being obtained through the cold boot attack involves first storing the AES keys in a block of the kernel image. When the encryption process is executed the AES keys are stored into special memory space rather than the common. Modifying the AES encryption algorithm to have the structure pointer mapped to the special memory enables the keys and data, protection from external forensic tools. The authors of the paper suggest their method works on different models of

phones and versions of android through “experimental verification”. However, they fail to include this process relying on the readers confidence which is a major limitation of the paper. Another drawback is the overall readability and grammar of the paper, many sentences do not make sense and punctuation is poor. However, this can be forgiven due to the authors first language being presumably Mandarin.

A real-world case study is examined to further understand the effects anti forensics has on mobile forensic investigations. To protect everyone involved relevant names and locations have been modified to ensure complete anonymity. The legal case occurred in the Sultanate of Oman and involved a user which will be known as Jim. A complaint was issued to an organization from the user concerned over his mobile device being hacked as his contacts had been receiving text messages through WhatsApp on an iPhone running the iOS 5.0.1 operating system. This text message application has over 2 billion active users and is used by criminals worldwide due its inherent anti-forensic capabilities (Dean, 2021). As text messages sent using WhatsApp are encrypted and stored locally making the process of extracting data from WhatsApp extremely complex.

The report provided by Jim’s ISP confirmed that there were records of the contacts receiving the messages but no evidence of them being sent. The paper makes the argument that based on the ISP report it is possible to conclude that Jim is innocent (*Al-Hadadi, M. and AlShidhani, A., 2013)*. However, it can be argued that this evidence is insufficient, due to the possibility of the user obfuscating the process of sending data, even though this is unlikely. Furthermore, a message application such as WhatsApp does not necessarily require an internet connection to function, it can send and receive data over Wi-Fi networks. In the practical element of the paper these statements are backed up, through an experiment involving the same model and operating system as the user. Two leading industry tools Oxygen Forensic Suite and the UFED physical Analyzer Cellebrite were used to extract data and from the evidence acquired two scenarios were thought to have occurred. Scenario one involved the removal of the sim card prompting the WhatsApp message to have been sent over Wi-Fi, scenario two involved Jim disposing of the device failing to delete WhatsApp then having a new user send WhatsApp messages to Jim’s contacts over a Wi-Fi network. The first scenario seems more likely from the evidence as the device is never mentioned to have been sold or disposed and most users will wipe their device if they do. Furthermore, it is common that smartphones will have passcodes protecting the device or some form of biometric identification.

This critical essay presents the key risks posed by anti-forensics to mobile forensic analysts. Arguing that the current tools used within the field of mobile forensics are susceptible to basic anti-forensic applications which require little technical knowledge to operate. Furthermore, the growing sophistication of anti-forensic measures are worrying for analysts due to the delay these techniques can cause to investigations. Due to the immature nature of anti-mobile forensics, there is not enough research available to equip analysts with the appropriate tools to combat the issues this field presents. The guidelines set by mobile forensic bodies fail to consider a lot of these techniques, hampering analysts in investigations, these rules require an update taking anti-forensic methods into account. As the rate of crimes involving anti forensics continues to rise and more criminals utilise these methods there needs to be a better understanding of anti-forensics. Creation of guidelines or a methodology concerning the approach to anti forensics would enable analysts to further understand anti-forensics, its techniques and mitigations.

Sources from different areas have been considered including case studies, academic papers/journals and specialists from the field of mobile forensics. To thoroughly demonstrate the challenges mobile forensic analysts face due to anti forensic techniques and their consequences. The paper has thoroughly answered the topic question of “What are some of the key challenges facing law

enforcement in the field of mobile forensics?” clearly and critically analysed papers relevant to anti-forensics within the field of mobile forensics. In conclusion anti-forensics significantly disrupts and delays mobile forensic investigations, continually challenging the investigators and law enforcement with effective anti-forensics techniques.

References

ACPO.7safe.com. 2021. [online] Available at: <https://www.7safe.com/docs/default-source/default-document-library/acpo_guidelines_computer_evidence_v4_web.pdf> [Accessed 15 November 2021].

Al-Hadadi, M. and AlShidhani, A., 2013. Smartphone forensics analysis: A case study. International Journal of Computer and Electrical Engineering, 5(6), p.576.

Athena Forensics. 2021. *An Explanation of ACPO Guidelines for Digital Based Evidence*. [online] Available at: <https://athenaforensics.co.uk/acpo-guidelines-for-computer-forensics/> [Accessed 22 November 2021].

Ayers, R., Brothers, S. and Jansen, W., 2013. Guidelines on mobile device forensics (draft). *NIST Special Publication*, *800*, p.101.

Dean, B., 2021. *WhatsApp 2021 User Statistics: How Many People Use WhatsApp?*. [online] Backlinko. Available at: <https://backlinko.com/whatsapp-users> [Accessed 20 November 2021].

Distefano, A., Me, G. and Pace, F., 2010. Android anti-forensics through a local paradigm. *digital investigation*, *7*, pp.S83-S94.

Karlsson, K.J. and Glisson, W.B., 2014, January. Android anti-forensics: Modifying cyanogenmod. In *2014 47th Hawaii International Conference on System Sciences* (pp. 4828-4837). IEEE.

Li, C.T. ed., 2009. *Handbook of Research on Computational Forensics, Digital Crime, and Investigation: Methods and Solutions: Methods and Solutions*. IGI Global.

O'Dea, S., 2021. *Smartphone users 2026 | Statista*. [online] Statista. Available at: <https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/> [Accessed 22 November 2021].

Ojp.gov. 2021. *Paraben device seizure*. [online] Available at: <https://www.ojp.gov/pdffiles1/nij/nlectc/239588.pdf> [Accessed 17 November 2021].

Omoloa, K. and Abadeb, E., 2019. Smartphone as an Agent of Anti-forensics: A Case of Workplace Environment in Kenya. *International Journal of Computer (IJC)*, *34*(1), pp.106-119.

Petrov, C., 2021. *51 Mobile Vs Desktop Usage Stats You Should Know in 2021*. [online] TechJury. Available at: <https://techjury.net/blog/mobile-vs-desktop-usage/> [Accessed 22 November 2021].

Sporea, I., Aziz, B. and McIntyre, Z., 2021. [online] Citeseerx.ist.psu.edu. Available at: <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.735.3154&rep=rep1&type=pdf> [Accessed 16 November 2021].

Zheng, J., Tan, Y.A., Zhang, X., Liang, C., Zhang, C. and Zheng, J., 2017, July. An anti-forensics method against memory acquiring for Android devices. In *2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)* (Vol. 1, pp. 214-218). IEEE.