What are some of the key challenges facing law enforcement in the field of mobile forensics?

As of 2021, smartphones are used by roughly 6 billion worldwide with a very large percentage of those in Europe and North America (statista, 2021). In fact, the share of Americans that own a smartphone is now 85%, up from 35% in 2011 (Pew Research Center, 2021). Smartphones have created benefits and drawbacks to investigations. The benefits are that there is more evidence that can be obtained to convict an individual of a crime such as browser activity, and travel activity. However, the downsides are that it can be a complicated and time-consuming process to get evidence. As a result, in recent years the need for forensic analysts has grown to combat this mobile crime surge. However, even though mobile forensic investigators have made great strides to convict criminals in recent years, criminals have come up with new methods to either slow down the forensic analysts or to destroy evidence. This new field is called 'Anti-Forensics' and SANS Institute (2015) discovered that only 1 in 4 digital forensics professionals had the training to combat these techniques. To answer the essay question, this essay aims to investigate common anti-forensic techniques used in IOS and Android devices and their impact on mobile forensic investigators. To address the aim, the essay will consist of the following paragraphs. The essay will begin by discussing the details behind anti-forensics and the differences between traditional and modern anti-forensics. Using relevant academic sources, the essay will then discuss common anti-forensic techniques, and how they impact a forensic investigation. The essay will conclude with a summary of the points discussed above, and how they have addressed the essay question.

Anti-forensics is a complex field of study so there is no definition agreed on by all parties. However, various sources have attempted to define anti-forensics. Gul & Kugu, (2017) described anti-forensics as an attempt at limiting the identification, collation, collection, and validation of sensitive data at a crime scene. On the other hand, Chhabra & Jain (2014) explained anti forensics as countermeasures taken to evade and frustrate forensic investigators. To get an even greater understanding, Peron & Legary, (2005) broke down anti-forensics into four separate categories: the destruction of data, hiding of data, data creation prevention, and the alteration of sensitive data. Overall, these papers are professionally written, and provide a good insight into the intricacies of anti-forensics, but they also show that anti-forensics is still an unexplored topic due to the lack of a definition. Furthermore, the paper by Peron & Legary, (2005) is older than Gul & Kugu, (2017) so the information on anti-forensic techniques might be out of date. This means more research needs to be conducted on the methods criminals use when disrupting a mobile forensic investigation

There are several methods techniques that a criminal can use when they want to disrupt the process of a mobile forensic investigation and each method has its strengths and weaknesses. In order to simplify things even further, anti-forensics can be split into two main techniques. Gul & Kugu, (2017) describes these two techniques as modern and traditional anti-forensics. These two techniques include all the methods of anti-forensics listed above but it is important to understand the differences because it can be the difference between a criminal being convicted or being acquitted of a crime. The oldest techniques are known as traditional mobile anti-forensics. According to Wundram et al.,

(2013) some traditional techniques are file wiping and overwriting of data, steganography, encryption, and physical destruction of device components. In recent years, however, modern mobile anti-forensic techniques have become more widely used by criminals. In contrast to traditional techniques, modern anti-forensic techniques aim to minimise footprints, obfuscate trails, complicate/ slow down a forensic investigation, exploit bugs in forensic tools, and make data paths incomprehensible (Gul & Kugu, 2017). It can be said that both approaches are relatively easy to implement if a criminal is experienced. Conlan et al (2016) explains that there is a thriving market online that sells tools, methodologies, and anti-forensic packages, which criminals can use to their advantage. However, it can also be argued that modern mobile anti-forensics is more effective because forensic analysts/companies are on strict budgets and constant time constraints. Therefore, any impact on these factors can severely affect law enforcement when it comes to a forensic investigation. Kumar, et al., (2021) also backs this point up by explaining that traditional forms of anti-forensics can still be effective but may be becoming obsolete as law enforcement are inventing effective ways to extract data even if a criminal thinks, they have wiped their files or destroyed the evidence. The conclusions by Kumar, et al. (2021) are also trustworthy because it is from an academic conference and a practical experiment on a mobile device was included in their research. Gul & Kugu (2017)'s findings can also be considered credible because it is a conference paper which means it has been peer-reviewed by many experts.

Destruction of a mobile phone or its components is an effective method of anti-forensics that can be utilised to make the contents of the phone unreadable to law enforcement. Mobile components are very delicate so any damage or shock could cause an electrical short circuit in the motherboard and make the device shut down forever (Kumar, et al., 2021). Furthermore, even if the device isn't fully destroyed it can still be very difficult for forensic analysts to retrieve information using techniques such as chip-off. This is because the chip pins are delicate and if they are already damaged or get damaged during the chip-off process, data extraction will be difficult or impossible (NIST, 2020). However, studies by Kumar et al (2021) and NIST (2021) have also shown that it can be possible to retrieve information from a damaged mobile device, which casts doubts over the effectiveness of device destruction as a form of anti-forensics in 2021. Kumar et al (2021) described a criminal case in which five suspects were accused of smuggling gold illegally. Four suspects surrendered their phones, but one suspect threw their phone at a wall to destroy all the evidence. The phone was shattered into different pieces and damaged by short circuits. The forensic investigators were unable to retrieve information with the chip-off technique as the device was already damaged and the chip was encrypted (Kumar, et al., 2021). However, in short, forensic analysts managed to reassemble the structure of the phone using forensic repair toolkits and replace components of the motherboard with working parts. Once the repaired mobile device was powered on a comprehensive amount of evidence was obtained such as call logs, contacts, WhatsApp chats and SMS messages. Therefore, this experiment by Kumar, et al (2021) shows that the destruction of mobile devices may not be an effective method of anti-forensics in the modern world. This point is further backed up by experiments conducted by NIST in which they extracted information from a damaged phone using a derivation of the chip-off technique. Instead of taking the phone chip off the board the traditional way, the NIST team ground down the opposite side of the board on a lathe until the chip pins were exposed. This method prevents the components from getting

more damaged and avoids unnecessary data loss (NIST, 2020). However, it is important to mention that the forensic process in both experiments took a long time and was very expensive because specialist personnel and equipment such as microscopes were required for the investigation. This reinforces the previous point, that any time/ cost delays can severely impact law enforcement in a forensic investigation. Furthermore, it can be said that the investigation done by Kumar et al (2021) was only a success because the majority of the motherboard was intact. If the motherboard was fully destroyed it is unlikely that the forensic analysts would be able to find evidence to convict the suspects. Overall, this shows that traditional anti-forensics is still effective at challenging law enforcement in the modern world, but investigators are catching up with cybercriminals as innovative techniques are being utilised. Although, the mobile destruction isn't the only anti-forensic technique.

Gul & Kugu (2017) said steganography is an effective and traditional anti-forensics technique. Stanescu et al (2010) described steganography as a science that focuses on the hiding of messages using specialised techniques in such a way that only the sender and the intended receiver will be able to decipher it (Stanescu, et al., 2010). This paper focuses on experiments using several steganography techniques and algorithms to see if they can secure the transfer of data between modern mobile devices with modern image and video processing capabilities. Steganography is effective as criminals can hide messages throughout a mobile device. Stanescu et al (2010) found that data can be hidden inside bitmap images and black and white images can be hidden inside SMS messages. In comparison, Sporea et al (2012) says that data can also be hidden inside document files or executable files. This has advantages for criminals as they can securely exchange hidden information using a built-in mobile phone feature. However, criminals are limited by the byte size capacity of SMS and the fact that images can only be in black and white format (Stanescu, et al., 2010). Steganography can be achieved using simple algorithms that use the LSB method, the YUV method, or the KLT method (Stanescu, et al., 2010). According to Stanescu et al (2010), algorithms based on the LSB method usually hide the most significant bits of the secret message image pixels within the least significant bits of the carrier image pixels. It is also important to note that the images are always in RGB format and the number of bits may vary (Stanescu, et al., 2010). Algorithms using the YUV method of steganography are the most researched among the three. This method is largely based on the LSB method but prior to applying the LSB algorithm, the images are converted from RGB to the YUV format. The LSB algorithm is then used on the image before converting the image back to RGB format (Stanescu, et al., 2010). The results of the testing showed that steganography can be effectively implemented on modern devices, which can potentially hinder law enforcement. However, as this is a traditional method of anti-forensics, there are limitations. A major disadvantage of steganography is the large overhead to hide very little amounts of information. There will be very little space to embed the hidden data if the data is already compressed (bartleby, n.d.). Steganography is also limited by the fact that forensics investigators will be able to see unencrypted data if the use of steganography is detected. This is because steganography is not supposed to keep hidden data from being known, it's about keeping its existence from being known by forensic analysts (Artz, 2001). Overall, this shows steganography is still a valid method of anti-forensics when dealing with small amounts of data or sending hidden information to

other sources. However, criminals shouldn't fully rely on steganography and instead use it in conjunction with techniques like encryption.

Encryption is an effective form of anti-forensics used by criminals worldwide. This form of anti-forensics is proving to be a major problem for forensic analysts because the sophistication of encryption algorithms used by mobile operating systems is increasing every year. In the past, it was easier for forensic analysts to extract evidence as encryption techniques were only applied at the application level or to protect sensitive user data. However, in recent years software companies have started to implement encryption at a system level with hard codded passwords that are not accessible to anyone (Fukami, et al., 2021). These system-level encryption schemes are called Full Disk Encryption (FDE) and File-Based Encryption (FBE). FDE was introduced with the iPhone 3GS and devices supporting Android 4.4 and it allows users to encrypt the entire User Data partition at the Flash Block level. FBE on the other hand encrypts files in the user data flash partition with different keys. FBE can also be regarded as the more contemporary method of encryption as FDE was discontinued with the release of Android 9 leaving FBE as standard in Android and IOS devices (Fukami, et al., 2021). There are several advantages to using FBE over FDE. Fukami, et al (2021) provides some advantages such as allowing individual files to be decrypted independently. Apple also states that if a file is in the Complete Protection class, the decryption key will get deleted from the mobile device's memory if the device is locked. This renders all data in this protection class inaccessible to everyone until a correct passcode or Touch ID is used. In short, essential OS files can remain decrypted while user files aren't (Apple, 2021). FDE on the other hand must always keep the encryption key in memory to access OS files so the system can keep running. This makes FDE less challenging to law enforcement when the device is powered on since there is only one key to recover from memory, unlike FBE which has multiple keys (Apple, 2021). These features have vastly improved the usefulness of mobile encryption as a form of anti-forensics as criminals can now take advantage of the OS without having to install third-party applications (Fukami, et al., 2021). Official documentation from Android states that mobile devices running its operating system are encrypted using 256 Advanced Encryption Standard (AES 256) (Android, n.d.) This means forensic analysts will find it very hard to extract information from a suspect's phone because AES 256 uses a 256-bit key length for encryption which has approximately 1.1 x 1077 possible combinations. To back this up further, even if law enforcement teams had a powerful supercomputer it would still take 3.31 x 1056 years for them to crack the key (KryptAl, n.d; Bernstein & Cobb, n.d). Although this would still be futile because Android and IOS devices have brute force protection. This means the devices will lock or even wipe their data after a set number of failed password attempts (Fukami, et al., 2021). Overall, modern mobile devices are encrypted using a strong encryption key, which is very hard for forensic analysts to extract information during an investigation. However, Teufl et al, (2014) and Fukami et al., (2021) both state that forensic analysts can still manage to get into a mobile device. The papers explain that forensic analysts can use zero-day attacks, malware, and vulnerability exploits as a last resort if there is no other way to get in. These methods are a last resort as they can potentially compromise the data stored on the mobile device. In the 2016 San Bernardino case, the FBI had to use a zero-day attack to break into a terrorist's iPhone because they found it impossible to break into the device. This was due to IOS's complex encryption scheme, which was explained earlier, and brute-force

protection, which the FBI couldn't risk due to the reasons stated above. In the end, the zero-day attack allowed the FBI to extract evidence to convict the terrorist. However, the investigation caused a dispute between Apple and the FBI and sparked legal debates about the US Government's access to encrypted devices (Fukami, et al., 2021). This real-world example demonstrates the advantages of mobile encryption as a method of anti-forensics and how it severely impacts law enforcement, but it also highlights the fact that law enforcement can still extract evidence to convict a criminal. Overall, the papers by Fukami et al (2012) and Teufl et al (2014) provide useful information about encryption such as the differences between FDE and FBE, and how they impact investigations. The inclusion of a real forensic investigation in Fukami et al (2012) helps to reinforce the effects these encryption techniques have on law enforcement. Unfortunately, they don't go into much detail about which mobile operating system is more likely to be exploited by law enforcement. In the USA, IOS holds 57.46% of the smartphone market share compared to 42.22% for Android (statcounter, 2021). Therefore, it is likely that IOS is more at risk to law enforcement since Apple has the highest market share. Furthermore, it is unlikely that American law enforcement has exploits for every brand of android device. In summary, encryption is a relevant form of anti-forensics that is still challenging to law enforcement worldwide. However, criminals shouldn't fully rely on encryption as their sole means of anti-forensics as encrypted mobile devices can still be exploited by law enforcement like the FBI. The techniques discussed are all traditional methods of anti-forensics and although they are still effective against law enforcement, experts in the field say they are slowly being replaced by more modern methods of anti-forensics.

Trail obfuscation or counterfeiting is an example of a modern mobile anti-forensic technique (Chhabra & Jain, 2014). Trail obfuscation is a technique that criminals use to mislead, divert, complicate, disorientate, and distract a forensic investigation (Panhalkar, n.d.). According to Hosgor (2020) and Majed et al (2020), methods of trial obfuscation include log manipulation, IP address spoofing, P2P networking, Proxy servers, and timestamp modification. Trail obfuscation is a challenge for law enforcement because many forensic tools fail to detect the trial obfuscation being used. This is evident in the paper Grover (2013) where they researched automated data collection and reporting on a mobile device for forensic investigations. For the experiment, they tested a prototype data collection app called 'DroidWatch' on an android device and ran several data collection experiments on it. Upon completion, the research team found that the tool was susceptible to anti-forensic techniques such as counterfeiting because no checks are performed to differentiate fake data entries from real ones. Furthermore, adding large amounts of fake data can result in a DOS attack and crash the app (Grover, 2013). Overall, this shows that trail obfuscation is an effective method of anti-forensics as it can drastically slow down an investigation and affect the credibility of the evidence. However, the paper explains that the weaknesses of forensic tools are known to analysts so the effectiveness of this technique may decline in the future. This paper can still be considered reliable as it has a well-structured methodology and the advantages and disadvantages of the tool 'DroidWatch' were well analysed and evaluated. However, the results in the paper may be different to a developed tool since they conducted the experiments on a prototype.

In conclusion, it can be said that anti-forensics techniques are very effective at challenging law enforcement in the field of mobile forensics, but only if they are carried out correctly and used in conjunction with other anti-forensic techniques. Anti-forensic techniques such as the destruction of mobile phones is effective at removing incriminating evidence. However, sources have shown that it can still be possible to extract evidence from destroyed devices using creative techniques. This is why it is important to use multiple techniques like encryption, steganography, and trail obfuscation. Encryption is effective due to the implementation of strong encryption keys like AES 256, which prevents law enforcement using brute force attacks. However, as was seen in the 2016 case, encryption cannot be fully trusted because mobile devices are still vulnerable to malware and exploits. Steganography and Trail Obfuscation are both similar in that they attempt to prevent the existence of evidence from being known by law enforcement. The differences being that steganography hides evidence within images, while trail obfuscation tries to minimise footprints or mislead law enforcement by creating counterfeit evidence elsewhere. Nevertheless, they both suffer from similar limitation, that being law enforcement are learning what evidence to search for, where to search for it, and what evidence is counterfeit. In summary, anti-forensics is effective when multiple techniques are implemented. This is because delaying and increasing the costs of an investigation by making it harder for forensic analysts to find evidence is the most effective method at challenging law enforcement in the field of mobile forensics.

References

Android, n.d. *Full-Disk Encryption.* [Online]
Available at: https://source.android.com/security/encryption/full-disk
[Accessed 11 November 2021].

Apple, 2021. *Data Protection classes.* [Online]
Available at: https://support.apple.com/en-gb/guide/security/secb010e978a/web
[Accessed 20 11 2021].

Artz, D., 2001. DigitalSteganography:Hiding Data within Data. *IEEE Internet Computing,* 5(3), pp. 75-80.

bartleby, n.d. *Disadvantages And Disadvantages Of Steganography And Information Hiding.* [Online]
Available at: https://www.bartleby.com/essay/Disadvantages-And-Disadvantages-Of-Steganography-And-Information-PJHJ4NMBNR
[Accessed 23 November 2021].

Bernstein , C. & Cobb, M., n.d. *Advanced Encryption Standard (AES).* [Online]
Available at: https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard
[Accessed 11 November 2021].

Chhabra, G. & Jain, A., 2014. Anti-Forensics Techniques: An Analytical Review. *Seventh international conference on Contemporqy Computing,* pp. 412-418.

Conlan, K., Baggili, I. & Breitinger, F., 2016. Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy. *Proceedings of the 16th Annual USA Digital Forensics Research Conference,* 07 August.

Fukami, A., Stoykova, R. & Geradts, Z., 2021. A new model for forensic data extraction from encrypted mobiledevices. *Forensic Science International: Digital Investigation,* Volume 38, pp. 1-10.

Grover, J., 2013. Android forensics: Automated data collection and reportingfrom a mobile device. *The Proceedings of the Thirteenth Annual DFRWS Conference,* Volume 10.

Gul, E. & Kugu, E., 2017. A survey on anti-forensics techniques. *International Artificial Intelligence and Data Processing Symposium,* 16 September.pp. 1-6.

Hosgor, E. C., 2020. Detection and Mitigation of Anti-Forensics. *International Journal of Computer Science and Information Security (IJCSIS),* Volume 18, pp. 46-52.

Jang, D.-i., Ahn, G.-J., Hwang, H. & Kim, K., 2016. Understanding Anti-forensic Techniques with Timestamp Manipulation. *IEEE 17th International Conference on Information Reuse and Integration,* pp. 609-614.

KryptAl, n.d. *How Safe is AES Encryption? | Advanced Encrption Standard.* [Online]
Available at: https://www.kryptall.com/index.php/2015-09-24-06-28-54/how-safe-is-safe-is-aes-encryption-safe
[Accessed 11 November 2021].

Kumar, A., Ghode, B. & Maniar, K., 2021. Forensic Analysis of Broken and Damaged Mobile Phone - A Crime Case Study. *International Journal of Scientific Research in Computer Science Engineering and Information Technology,* 7(3), pp. 481- 487.

Majed, H., Noura, H. & Chebab, A., 2020. Overview of Digital Forensics and Anti-Forensics. *8th International Symposium on Digital Forensics and Security (ISDFS),* pp. 1-5.

NIST, 2020. *NIST Tests Forensic Methods for Getting Data From Damaged Mobile Phones.* [Online]
Available at: https://www.nist.gov/news-events/news/2020/01/nist-tests-forensic-methods-getting-data-damaged-mobile-phones
[Accessed 09 November 2021].

Panhalkar, T., n.d. *Anti-Forensics Techniques: Trail Obfuscation, Artifact Wiping, Encryption, Encrypted Network Protocols and Program Packers.* [Online]
Available at: https://info-savvy.com/anti-forensics-techniques-trail-obfuscation-artifact-wiping-encryption-encrypted-network-protocols-and-program-packers/
[Accessed 17 11 2021].

Perklin, M., 2013. *Anti-Forensics and Anti-Anti-Forensics.* Las Vegas, DEFCONConference.

Peron, C. S. & Legary, M., 2005. Digital anti-forensics: emerging trends in. *E-Crime Comput. Evid,* pp. 1-11.

Pew Research Center, 2021. *Mobile Fact Sheet.* [Online]
Available at: https://www.pewresearch.org/internet/fact-sheet/mobile/
[Accessed 05 November 2021].

SANS Institute, 2015. *Rise of anti-forensics techniques requires response from digital investigators.* [Online]
Available at: https://www.sans.org/press/announcements/rise-of-anti-forensics-techniques-requires-response-from-digital-investigators/
[Accessed 05 October 2021].

Sporea, I., Aziz, B. & McIntyre, Z., 2012. On the Availability of Anti-Forensic Tools for Smartphones.

Stanescu, D., Stangaciu, V. & Stratulat, M., 2010. Steganography on new generation of mobile. *International Joint Conference on Computational Cybernetics and Technical Informatics,* pp. 343-347.

statcounter, 2021. *Mobile Operating System Market Share United States Of America.* [Online]
Available at: https://gs.statcounter.com/os-market-share/mobile/united-states-of-america
[Accessed 13 November 2021].

statista, 2021. *Number of smartphone users from 2016 to 2021.* [Online]
Available at: https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/
[Accessed 05 October 2021].

Teufl, P. et al., 2014. Android Encryption Systems. *2014 International Conference on Privacy and Security in Mobile Systems (PRISMS).*

Vanderburg, E., 2009. *MAC times in computer forensics.* [Online]
Available at: https://www.tcdi.com/mac-times-in-computer-forensics/
[Accessed 18 November 2021].

Wundram, M., Freiling, F. & Moch, C., 2013. Anti-Forensics: The Next Step in Digital Forensics Tool Testing. *Seventh International Conference on IT Security Incident Management and IT Forensics,* pp. 83-97.