Journal of Forensic Sciences And Criminal Investigation
ISSN: 2476-1311

Juniper Publishers key to the Researchers

Opinion
Volume 15 Issue 4 - February 2022
DOI: 10.19080/JFSCI.2022.15.555917

J Forensic Sci & Criminal Inves

Mobile Forensics – The End of a Golden Age?

Dirk Pawlaszczyk*

Department of Applied Computer and Biosciences, University of Applied Sciences, Mittweida, Germany

Submission: February 10, 2022; **Published:** February 28, 2022

***Corresponding author:** Dirk Pawlaszczyk, Department of Applied Computer and Biosciences, University of Applied Sciences, Mittweida, Germany

Abstract

Mobile forensics today is an essential part of nearly every criminal investigation. This contribution tries to shed light on the question, to which extent mobile forensics has reached its zenith. Moreover, is it turned out whether we are heading for a crisis in the future? In this context, a literature survey is presented that attempts to identify the most crucial current challenges in this field.

Keywords: Mobile Forensics; Challenges; Opportunities; Future; Digital Forensics; Holy Grail; Specialized Training; Criminal Investigation; Acquisition; Practitioners Struggle

Abbreviations: EU: European Union; PET: Privacy-Enhanced Technologies; LEA: Law Enforcement Agencies; MDFT: Mobile Device Forensic Tool; CASE: Cyber-investigation Analysis Standard Expression

Introduction

In 2020, French police infiltrated the EncroChat network, resulting in hundreds of arrests in different European countries, including Germany, the Netherlands, and the UK. The dismantling of this network was hailed as a great success for digital forensics [1]. However, even this apparent success cannot hide the fact that we are in danger of losing the race against criminals, especially in the field of mobile forensics. At the same time, we need to be more concerned about the quality standards in investigating the evidence. The term "mobile forensics" refers to the seizure, acquisition and analyze evidence stored on mobile devices for use in court. This area has become increasingly important in recent years. This situation is not surprising when people continuously use mobile phones to share information, files, and images. According to the Eurostat portal, more than 80% of persons aged 16 to 74 in the European Union (EU) used the internet in 2016 via mobile or smartphone [2]. 6.4 billion smartphone users worldwide trust their phones to carry information regarding all aspects of their everyday lives. Criminals use the same communication channels to coordinate their illegal activities. Digital forensics today is an integral part of nearly every criminal investigation. 85% of Crime Investigations include electronic evidence [3]. So, examining a suspect's daily companion takes on particular importance for law enforcement agencies (LEAs). In an article from 2010, the authors proclaim to be the "golden age of computer forensics" and that it will end [4]. Today, more than ten years later, one must ask whether this statement is still valid?

A Stocktaking

The picture is very mixed if we look at mobile forensics today. Practitioners struggle with an increasing number of variants in cell phones. Beyond this, the introduction of new privacy-enhanced technologies (PET) such as passcodes, biometric access, secure boot, and full hardware-based encryption has improved data security in recent years [5]. Technologies like Secure Enclave on iOS or Trust Zone on Android enable mobile devices to stand up to attack attempts far beyond what most desktop computers could achieve.

At the same time, messenger apps like WhatsApp, Signal or Telegram are much more concerned with ensuring customer data privacy and burying them deep within the protected area of the cell phone in encrypted databases. In the following years, multi-level encryption becomes the standard and no longer the exception. However, for the LEAs, this makes it increasingly challenging to acquire evidence. Today, relevant data on a mobile phone is only accessible via specialized digital forensics software. Have we missed something? It seems to be a natural development. Data and identity theft pose a significant threat. The whistleblower affair around Eduard Snowden in 2014 has led people to become more sensitive to information security. Accordingly, phone vendors pay more attention to the customers' desire for security and privacy. Therefore, the path taken is logical and makes it more difficult for criminals to obtain their victims' data. Unfortunately, this

also makes the work of the investigating authorities increasingly challenging.

In the meantime, at least for the latest generation of mobile phones, it is more and more the case that only highly specialized laboratories can unlock and forensically acquire evidence from encrypted devices. To date, this work has been done by LEAs using a mobile device forensic tool (MDFT). In the meantime, some vendors are already taking a different approach. Cracking the latest cell phone models offers paid data extraction services, which they perform in their labs [6,7]. So, investigators must give away potential evidence. This development is problematic for several reasons. Many companies do digital analysis and digital forensics for the security authorities. However, these are private providers. Acquisition of personal data in a criminal case is an original statutory work since it impacts fundamental civil rights. In a preliminary investigation, the officer signs that the evidence has been handled with care [8,9]. Or was it possible that the incriminated pictures and chat messages were replaced to preserve evidence? If a mobile phone is confiscated, only a small group of governmental institutions should do that. This principle must be duly observed and followed even in the future.

The holy grail of forensic investigation, to keep judicially relevant digital data in its original form, no data may be changed in the investigations process, has long been history [10]. The widespread use of technologies like device encryption implies that at least law enforcement agencies can bypass these security mechanisms more invasive. Today, one possible way to access the data stored on a cell phone is often to remove and dump the soldered memory chips via chip off. In other cases, a special boot loader must be installed before creating a forensic "sound" copy. A third option used by many MDFTs is to jailbreak the mobile phone, whereby apps on the phone are downgraded or replaced. However, all three of these procedures destroy either evidence or change the data stored. Since this becomes the rule and not the exception, one should be aware of this. Another serious challenge is the validity and truthfulness of the mobile evidence. Judges and prosecutors are still all too easily lulled into blindly trusting digital evidence without questioning it. Even forensic experts sometimes succumb to this problem and adopt a particular forensic tool's results without questioning them. There is an unwritten rule to check the results with at least a second tool. However, this is not bindingly defined anywhere. The amount of data generated by examining a single phone run into tens of thousands of files. We are increasingly coming up against a quality problem. We are increasingly coming up against a quality problem, not least because phone acquisition has now become a daily exercise. In addition to the problems already discussed, other challenges remain, which have been named more than ten years before in Garfinkel's contribution [5]:

i. **Tools and Interoperability:** The comparability and easy exchangeability of electronic evidence are only partially implemented. We can still observe a lock-in effect with most forensic tools. Even today, most applications are monolithic. Approaches like Cyber-investigation Analysis Standard Expression (CASE) [11] are significant in the right direction. However, it will still take a few years until most important forensics' vendors support this.

ii. **Standards:** Mobile forensics, even today, lacks standardization. There is no standard way or procedure to extract information from cell phones. However, there has also been movement in this area in the meantime. A current example is the FORMOBILE project, which attempts to map the entire chain of custody in a uniform process, starting with the first-responder teams at the crime scene and ending with presenting the evidence in court [12].

iii. **Training:** Give practitioners the necessary training to effectively use forensic software tools and follow a standardized procedure. Training is a serious problem facing organizations that deliver forensic services [21]. There is a lack of complex, realistic training data, which means that most classes are taught with simplistic artificial data. This in turn influences the quality of education.

iv. **Consideration of academic research:** Meanwhile, academic results are increasingly being considered in forensic products. Thus, there is the possibility for users to extend the existing product via Python scripts. The increasing popularity of open-source software and GitHub repositories is also evidence of a shift in thinking in this area.

We have further examined and evaluated publications from different research groups on challenges in mobile forensics in recent years [17-30]. A total of 14 papers in this field were compared in this survey. The aim was to find out which challenges the respective contributions address. Within our survey, eight top categories could be identified (Figure 1). Without exception, every publication surveyed names circumvent encryption and the latest cutting-edge security features as one of the most significant challenges today and in future [14,17,18, 20,22]. Legal & Privacy issues are also considered by most authors to be significant and are among the second most mentioned [7,18,14,24,26]. The topic of visualization also plays an important role. As an additional category, we were able to identify the topic of, let us say, Process Automation & Intelligence. Most authors further address big data as an increasingly pressing problem field [19,29]. A solution, in turn, is addressed with artificial intelligence and machine learning techniques [28-30].

The complexity and constant changes in mobile forensics require specialized training of practitioners with data sets that are as state of the art and realistic as possible [13,21]. Even today, the generation of training data is almost exclusively done manually. Solutions and approaches are urgently sought here. The lack of standards and the need of common interchange formats

How to cite this article: Dirk Pawlaszczyk. Mobile Forensics – The End of a Golden Age?. J Forensic Sci & Criminal Inves. 2022; 15(4): 555917. DOI: 10.19080/JFSCI.2022.15.555917

is also identified as a problem by many authors [21,23,24]. Another focus in current and future work is seen the tampering and reverse engineering in mobile phone hardware as well as apps [26,27,30]. For Android OS, more than 2.6 million apps are currently available in the Appstore [31]. An investigator is thus confronted almost daily with a new, hitherto unknown app for which existing forensic tools do not yet offer any support. The challenges in the hardware sector are no less difficult, considering the very short development cycles for mobile phones.

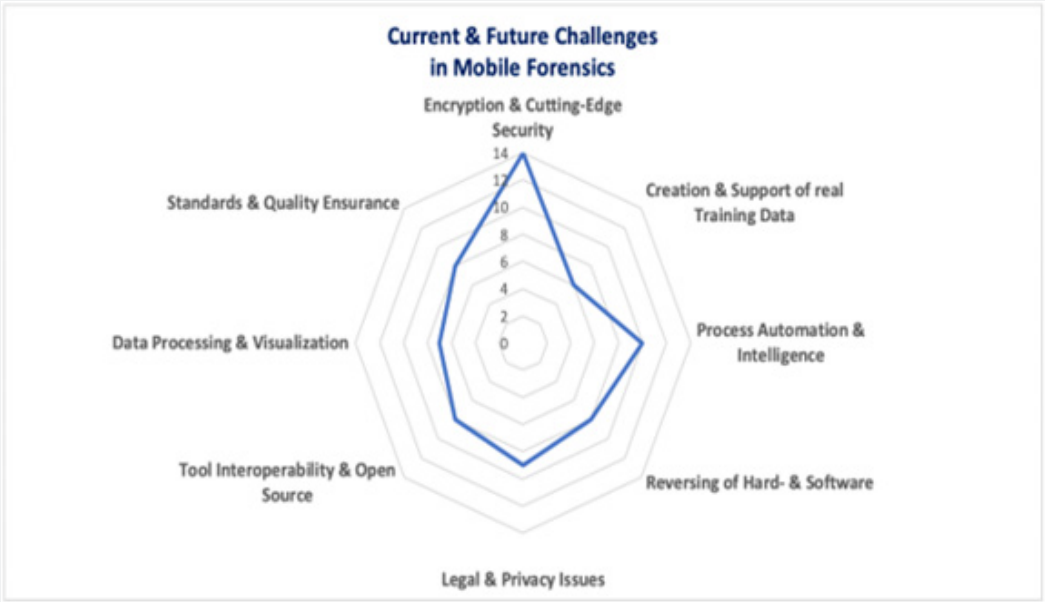

Figure 1: Current and Future Challenges in Mobile Forensics.

Conclusion

We can observe significant technical changes and new hurdles in mobile devices forensics within the last decade. In addition to old problem fields that have existed for a long time, new problem areas have emerged in recent years. Are we witnessing the end of a golden era? In some respects, that does seem to be true. It is becoming increasingly difficult to access data on mobile devices. While technology is invincible, both require time and frequently luck to circumvent. Even today, LEAs have ways to access, decode, and use the data as safe, trustworthy, and reliable evidence. We must make sure that the relevant fundamental rights are appropriately considered even in the future. Are we heading for a crisis? That is not what it looks like now. However, in mobile forensics, we are back on the ground. We are no longer in the land of milk and honey where evidence flies to us, and we do not have to invest anything in it. A new humility is in order, and a change in thinking. In the future, is become increasingly difficult to preserve evidence. However, it is not impossible. The question in the future will be whether it is always appropriate.

Acknowledgements

The project in part has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 832800.

References

1. Richards J Encro Chat Hack: Why It Happened and What It Means for the Encro Chat User.
2. Eurostat (2016) Almost 8 out of 10 internet users in the EU surfed via a mobile or smart phone in 2016. Eurostat newsrelease,
3. European Commission (2021) Press remarks by Vice-President Schinas on EU Strategies to tackle Organised Crime and fight Trafficking in Human Beings. Interview.
4. Garfinkel SL (2010) Digital forensics research: The next 10 years, Digital Investigation 7: S64-S73.
5. Zinkus M, Tushar JM, Green M (2021) Data Security on Mobile Devices: Current State of the Art, Open Problems, and Proposed Solutions.
6. Cellebrite Inc. Cellebrite Advanced Services.
7. Koepke L, Weil E, Janardan U, Dada T, Yu H (2020) Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones.
8. (2012) Association of Chief Police Officers (United Kingdom): Good Practice Guide for Computer-Based Electronic Evidence.
9. (2014) National Institute of Standards and Technologies: Special Publication (NIST SP) - 800-101 Rev Report Number 800-101 Rev 1, NIST Pub p. 87.
10. Horsman G (2020) ACPO principles for digital evidence: Time for an update? Forensic Science International Reports 2.
11. Casey E, Nelson A, Hyde J (2019) Standardization of file recovery classification and authentication. Digital Investigation 31.

How to cite this article: Dirk Pawlaszczyk. Mobile Forensics – The End of a Golden Age?. J Forensic Sci & Criminal Inves. 2022; 15(4): 555917.
DOI: 10.19080/JFSCI.2022.15.555917

12. Karl Grün, Annette Altenpohl (2020) Report on existing practices and standards. In: From mobile phones to court – A complete Forensic investigation chain targeting Mobile devices (Formobile).
13. Caviglione L, Wendzel S, Mazurczyk W (2017) The Future of Digital Forensics: Challenges and the Road Ahead. IEEE Security & Privacy 15(6): 12-17.
14. Department of Homeland Security, Study on Mobile Device Security.
15. Karie NM, Venter HS (2015) Taxonomy of Challenges for Digital Forensics. Journal of Forensic Sciences 60(4): 885-893.
16. Katalov V. The Art of iPhone Acquisition.
17. Chernyshev M, Zeadally S, Baig Z, Woodward A (2017) Mobile Forensics: Advances, Challenges, and Research Opportunities. IEEE Security & Privacy 15(6): 42-51.
18. Bennett D (2012) The Challenges Facing Computer Forensics Investigators in Obtaining Information from Mobile Devices for Use in Criminal Investigations. Information Security Journal 21(3): 159-168.
19. Umale M, Deshmukh AB, Tambhakhe MD (2014) Mobile phone forensics challenges and tools classification A review. International Journal on Recent and Innovation Trends in Computing and Communication 2(3): 622-626.
20. Jonesm GM, Winster SG (2017) Forensics analysis on smart phones using mobile forensics tools. International Journal of Computational Intelligence Research 13(8): 1859-1869.
21. Humphries G, Nordvik R, Manifavas H, P. Cobley, M. Sorell (2021) Law enforcement educational challenges for mobile forensics. Forensic Science International Digital Investigation 38.
22. Yadav D, Mishra M, Prakash S (2013) Mobile Forensics Challenges and Admissibility of Electronic Evidence in India. 2013 5th International Conference and Computational Intelligence and Communication Networks pp: 237-242.
23. Alatawi H, Alenazi K, Alshehri S, Alshamakhi S, Mustafa M, Aljaedi A (2020) Mobile Forensics: A Review. 2020 International Conference on Computing and Information Technology p: 1-6.
24. Brunty J (2016) Mobile device forensics: threats, challenges, and future trends, Digital Forensics Syngress p: 69-84.
25. Fernando V (2021) Cyber Forensics Tools: A Review on Mechanism and Emerging Challenges, 2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS) p: 1-7.
26. Herrera LA (2020) Challenges of acquiring mobile devices while minimizing the loss of usable forensics data. 2020 8th International Symposium on Digital Forensics and Security (ISDFS) p: 1-5.
27. Lwin HH, Aung WP, Lin KK (2020) Comparative Analysis of Android Mobile Forensics Tools. 2020 IEEE Conference on Computer Applications (ICCA) p: 1-6.
28. Montasari R, Hill R (2019) Next-Generation Digital Forensics: Challenges and Future Paradigms. 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3) p: 205- 212.
29. Zareen MS, Waqar MS, Aslam B (2013) Digital forensics: Latest challenges and response. 2013 2nd National Conference on Information Assurance (NCIA) p: 21-29.
30. Mohammmed SS, Sridevi R (2020) A Survey on Digital Forensics Phases, Tools and Challenges. Proceedings of the Third International Conference on Computational Intelligence and Informatics 1090.
31. Statista.com Number of available apps in the Google Play Store.

DOI: 10.19080/JFSCI.2022.15.555917

How to cite this article: Dirk Pawlaszczyk. Mobile Forensics – The End of a Golden Age?. J Forensic Sci & Criminal Inves. 2022; 15(4): 555917. DOI: 10.19080/JFSCI.2022.15.555917