Documents

Almuqren, A.[a] , Alsuwaelim, H.[a] , Hafizur Rahman, M.M.[a] , Ibrahim, A.A.[b]

A Systematic Literature Review on Digital Forensic Investigation on Android Devices
(2024) *Procedia Computer Science*, 235, pp. 1332-1352.

DOI: 10.1016/j.procs.2024.04.126

[a] Department of Computer Networks and Communications, King Faisal University, Saudi Arabia, Saudi Arabia
[b] Department of Computer Science, KICT, International Islamic University, Malaysia IIUM, Kuala Lumpur, Malaysia

Abstract
Mobile forensics, particularly in the Android ecosystem, is a rapidly evolving field that demands continuous advancements to address the growing complexity and diversity of mobile devices. This article emphasizes the importance of developing techniques for digitally analyzing Android smartphones, which dominate the smartphone market. The primary objective of this research is to contribute to the development of effective forensic investigation strategies tailored specifically for Android mobile devices, providing insights into the tools and methods used for this purpose. The objective of this study is to improve the precision and effectiveness of forensic examinations pertaining to Android mobile phones. It discusses the fundamental functionality of mobile devices as a source of digital evidence and provides an overview of tools and methodologies for collecting and analyzing such evidence. The importance of comprehending the hardware and software architecture of Android handsets in order to choose the right forensic tools is also highlighted in the article. Furthermore, it proposes future enhancements for Andriller, a popular digital forensic tool, to improve its effectiveness in Android forensic investigations. These enhancements include advancements in data extraction techniques, compatibility with new Android versions, support for additional data types, integration with advanced analysis methods, and addressing identified limitations. Additionally, the paper stresses the need for robust methodologies for conducting cloud forensics on Android devices, particularly in the context of data stored in cloud storage services. The proposed work aims to enhance the capabilities of Andriller and improve the efficiency of digital forensic investigations on Android devices.

Author Keywords
Andriller; Forensic; Mobile Device Forensics; Mobile devices; Mobile Forensic

Index Keywords
Computer forensics, Digital devices, Digital storage, Electronic crime countermeasures, Smartphones; Andriller, Android smartphone, Forensic, Forensic investigation, Forensic tools, Mobile forensics, Primary objective, Smart phones, Systematic literature review, Tools and methods; Android (operating system)

Funding details
Deanship of Scientific Research, King Saud University
King Faisal UniversityKFUGRANT_ _

Authors\u2019 Contributions: All authors equally contributed. Funding: This paper was funded by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia under the [GRANT_ _]. Availability of Data and Materials: Not applicable. Acknowledgments: The authors extend their appreciation to the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia [GRANT _ _]. The authors would like to thank the anonymous reviewers for their insightful scholastic comments and suggestions, which

References

- Sunde, N., Horsman, G.
  Forensic Science International: Digital Investigation
  (2021) *Forensic Science International*, 36, p. 301074.
- Goel, A., Tyagi, A., Agarwal, A.
  Smartphone forensic investigation process model
  (2023) *Computer Science Journals (CSC Journals)*,
- Kohn, M.D., Eloff, M.M., Eloff, J.H.P.
  Integrated digital forensic process model
  (2013) *Computers & Security*, 38, pp. 103-115.

- Varol, C., Tayeb, H.F.
  Android Mobile Device Forensics: A Review
  (2023) *Cloudfront.net*,

- Parikh, T.S., Lazowska, E.D.
  Designing an architecture for delivering mobile information services to the rural developing world
  (2006) *Proceedings of the 15th International Conference on World Wide Web*,

- Bang, J., Lee, Y., Lee, Y.-T., Park, W.
  AR/VR based smart policing for fast response to crimes in safe city
  (2019) *2019 IEEE International Symposium on Mixed and Augmented Reality Adjunct (ISMAR-Adjunct)*, pp. 470-475.

- Casey, E., Turnbull, B.
  Digital Evidence on Mobile Devices
  (2023) *Elsevier.com*,

- Casadei, F., Savoldi, A., Gubian, P.
  (2023) *Forensics and SIM Cards: An Overview. Utica.edu*,

- Novak, M., Grier, J., Gonzales, D.
  (2023) *New Approaches to Digital Evidence Acquisition and Analysis. Ojp.gov*,

- Pribadi, B., Rosdiana, S., Arifin, S.
  Digital forensics on facebook messenger application in an android smartphone based on NIST SP 800-101 R1 to reveal digital crime cases
  (2023) *Procedia Computer Science*, 216, pp. 161-167.

- Da Naing, A.T., Guan, J.S.B., Win, Y.S., Pan, J.
  A review on the effectiveness of dimensional reduction with Computational Forensics: An application on malware analysis
  (2023) *ArXiv [Cs.CR]*,

- Silalahi, S., Ahmad, T., Studiawan, H.
  Transformer-based named entity recognition on drone flight logs to support forensic investigation
  (2023) *IEEE Access: Practical Innovations, Open Solutions*, 11, pp. 3257-3274.

- Saranya, S., Usha, G.
  Forensic analysis of online social network data in crime scene investigation
  (2022) *Artificial Intelligence and Blockchain in Digital Forensics*, pp. 183-209.
  1st Edition, River Publishers

- Zhang, Y., Li, Y., Li, Z.
  Aye: A trusted forensic method for firmware tampering attacks
  (2023) *Symmetry*, 15 (1), p. 145.

- Shin, Y., Kim, S., Jo, W., Shon, T.
  Digital forensic case studies for in-vehicle infotainment systems using Android Auto and Apple CarPlay
  (2022) *Sensors (Basel, Switzerland)*, 22 (19), p. 7196.

- Mirza, M.M., Ozer, A., Karabiyik, U.
  Mobile cyber forensic investigations of Web3 wallets on Android and iOS
  (2022) *Applied Sciences (Basel, Switzerland)*, 12 (21), p. 11180.

- Kim, H., Shin, Y., Kim, S., Jo, W., Kim, M., Shon, T.
  Digital forensic analysis to improve user privacy on Android
  (2022) *Sensors (Basel, Switzerland)*, 22 (11), p. 3971.

- Hutchinson, S., Mirza, M.M., West, N., Karabiyik, U., Rogers, M.K., Mukherjee, T., Aggarwal, S., Pettus-Davis, C.
  Investigating wearable fitness applications: Data privacy and digital forensics analysis on Android
  (2022) *Applied Sciences (Basel, Switzerland)*, 12 (19), p. 9747.

- Salimi, N.F., Abd Warif, N.B., Ismail, N.S.N.
  Comparative analysis of logical acquisition using Wondershare Dr. Fone, MOBILedit Forensic, and FonePaw on android phones / Nuraimi Farhana Salimi, Nor Bakiah Abd Warif and Nor-Syahidatul N Ismail
  (2022) *Malaysian Journal of Computing (MJoC)*, 7 (2), pp. 1162-1177.

- Younis, L.B., Sweda, S., Alzu'Bi, A.
  Forensics analysis of private web browsing using android memory acquisition
  (2021) *2021 12th International Conference on Information and Communication Systems (ICICS)*,

- Ceballos Delgado, A.A., Glisson, W.B., Grispos, G., Choo, K.-K.R.
  FADE: A forensic image generator for android device education
  (2022) *WIREs Forensic Science*, 4 (2).

- Fernando, V.
  Cyber forensics tools: A review on mechanism and emerging challenges
  (2021) *2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, pp. 1-7.

- Bharath Bhushan, H.H., Metilda Florance, S.
  An overview on handling anti forensic issues in android devices using forensic automator tool
  (2022) *2022 IEEE International Conference on Signal Processing, Informatics, Communication and Energy Systems (SPICES)*, 1, pp. 425-430.

- Tayeb, H.F., Varol, C.
  Android Mobile Device Forensics: A Review
  (2019) *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*, pp. 1-7.

- Kim, D., Lee, S.
  Study of identifying and managing the potential evidence for effective Android forensics
  (2020) *Forensic Science International: Digital Investigation*, 33, p. 200897.

- Almehmadi, T., Batarfi, O.
  Impact of android phone rooting on user data integrity in mobile forensics
  (2019) *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*, pp. 1-6.

- Al-Dhaqm, A., Razak, S.A., Ikuesan, R.A., Kebande, V.R., Siddique, K.
  A review of mobile forensic investigation process models
  (2020) *IEEE Access: Practical Innovations, Open Solutions*, 8, pp. 173359-173375.

- Hermawan, T., Suryanto, Y., Alief, F., Roselina, L.
  Android forensic tools analysis for unsend chat on social media
  (2020) *2020 3rd International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, pp. 233-238.

- Mirza, M.M., Salamh, F.E., Karabiyik, U.
  An android case study on technical anti-forensic challenges of WhatsApp application
  (2020) *2020 8th International Symposium on Digital Forensics and Security (ISDFS)*, pp. 1-6.

- Riadi, I., Umar, R., Firdonsyah, A.
  Identification of Digital Evidence on Android's Blackberry Messenger Using NIST Mobile Forensic Method
  (2017) *International Journal of Computer Science and Information Security (IJCSIS)*, 15 (5), pp. 3-8.

- Febriansyah, L.
  (2018) *ANALISIS KETERLIBATAN CYBERTERORISM MENGGUNAKAN METODE ANALITYCAL HIERARCHY PROCESS (AHP)*,
  Master's thesis, Universitas Islam Indonesia

- Alhassan, J.K.
  Comparative evaluation of mobile forensic tools
  (2018) *Proceedings of the International Conference on Information Technology & Systems (ICITS 2018)*, pp. 105-114.
  Springer International Publishing

- Acharya, S., Rawat, U., Bhatnagar, R.
  A comprehensive review of Android security: Threats, vulnerabilities, malware detection, and analysis
  (2022) *Security and Communication Networks*,

- Maria Jones, G., Godfrey Winster, S., Scholar, P.G.
  (2023) *Forensics Analysis on Smart Phones Using Mobile Forensics Tools.*,
  Ripublication.com

- Hoelz, H., Herdl, C., Gerstl, L., Tacke, M., Vill, K., Von Stuelpnagel, C., Rost, I., Borggraefe, I.
  Impact on clinical decision making of next-generation sequencing in pediatric epilepsy in a tertiary epilepsy referral center
  (2020) *Clinical EEG and Neuroscience: Official Journal of the EEG and Clinical Neuroscience Society (ENCS)*, 51 (1), pp. 61-69.

- Mayrhofer, R., Stoep, J.V., Brubaker, C., Kralevich, N.
  The Android platform security model
  (2021) *ACM Transactions on Privacy and Security*, 24 (3), pp. 1-35.

- Fukami, A., Stoykova, R., Geradts, Z.
  A new model for forensic data extraction from encrypted mobile devices
  (2021) *Forensic Science International: Digital Investigation*, 38, p. 301169.

- Kumar Agrawal, A., Sharma, A., Khatri, P.
  (2019) *Android Forensics: Tools and Techniques for Manual Data Extraction*,
  SSRN Electronic Journal

- Jones, G.M., Winster, S.
  (2017) *Forensics Analysis on Smart Phones Using Mobile Forensics Tools*,

- Casey, E.
  (2021) *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*,
  (4th ed.). Academic Press

- (2017) *Electronic Crime Scene Investigation: A Guide for First Responders*,
  National Institute of Justice

- (2016) *NIST Special Publication 800-86: Guide to Integrating Forensic Techniques into Incident Response*,
  National Institute of Standards and Technology

- Casey, E.
  (2018) *Handbook of Digital Forensics of Multimedia Data and Devices*,
  John Wiley & Sons

- (2020) *Special Publication 800-204. Guide to Forensic Analysis of Mobile Devices*,
  National Institute of Standards and Technology (NIST)

- Sharma, A., Singh, J., Kumar, N.
  A review of Android Smartphone Forensic Analysis Tools
  (2021) *International Journal of Advanced Science and Technology*, 30 (2), pp. 3592-3600.

Correspondence Address
Ibrahim A.A.; Department of Computer Science, Malaysia; email: 222400079@student.kfu.edu.sa

Editors: Singh V., Asari V.K., Li K.-C., Crespo R.G.
Sponsors: Department of Science and Technology; Government of India; Ministry of Electronics and Information Technology and SERB
Publisher: Elsevier B.V.

Conference name: 2nd International Conference on Machine Learning and Data Engineering, ICMLDE 2023
Conference date: 23 November 2023 through 24 November 2023
Conference code: 199981

ISSN: 18770509
Language of Original Document: English
Abbreviated Source Title: Procedia Comput. Sci.
2-s2.0-85196357916
Document Type: Conference Paper
Publication Stage: Final
Source: Scopus