Ensemble-Based Tools in Digital Forensic Evidence Extraction for Android Devices

AKINYOKUN OLUYOMI KOLAWOLE[1], BONIFACE KAYODE ALESE[2], ORIMOGUNJE BABATOLA OLUWOLE[3], VICTORIA IBIYEMI OMONIYI[4], OLUWADAMILOLA ADEDAYO SERIKI[5]

[1, 2, 3, 4, 5]*Department of Cybersecurity, Federal University of Technology, Akure, Nigeria*

Abstract- ***Precision and speed of investigative process has become is a critical part of criminal jurisprudence. This research presents an adoption and adaptation of ensemble-based tools for evidence extraction in Android devices. The study explores various tools such as Autopsy, Wondershare Dr. Fone and others, delving into the respective techniques. The findings of this research pave the way for future studies in this field, contributing to advancements in Android forensics extraction.***

I. INTRODUCTION

growth and increasing popularity, resulting in a corresponding increase in the need for digital forensic investigations of these devices in both personal and professional contexts. In digital forensics, evidence is extracted from digital devices and analysed to determine whether there have been any cybercrimes or security breaches. Nevertheless, extracting evidence from Android devices can be a complex and challenging task, owing to the wide range of applications; and operating systems.

Android forensics, however, is a subset of digital forensics. With so many smartphone models, operating systems, and security features to choose from, digital investigators are faced with considerable challenges. A multifaceted ecosystem requiring cutting-edge tools and methodologies that adapt to evolving device configurations and security measures is critical to extracting, analysing, and interpreting digital evidence. In this context, machine learning, with its capability to automate and enhance the accuracy of forensic processes, has emerged as a transformative force.

Ensemble-based approaches are based on the theory that the synergy of multiple models, each excelling in its own field, can produce superior results. Our system aims to streamline and expedite investigation s while maintaining the highest standards of ethical and legal compliance by encompassing a broad spectrum of digital evidence types and utilizing machine learning techniques.

II. RELATED WORKS

In the intricate realm of Android devices, the discourse surrounding digital forensic investigations has evolved significantly, mirroring the profound shifts in technology and user behavior. This literature review embarks on a comprehensive exploration, unraveling the intricate tapestry of current research and underscoring the pivotal role played by ensemble-based tools in the extraction of digital evidence from Android devices.

As the expansion of smartphones and its use continue to shape our daily lives, the intricacies of Android digital forensics have become increasingly profound. Scholars, exemplified by the work of Ali et al (2017), accentuate the critical need for sophisticated tools capable of maneuvering through the labyrinth of diverse device models, a multitude of operating systems, and the perpetual evolution of the Android ecosystem. This section provides a nuanced exploration, shedding light on the multifaceted challenges posed by encryption, fragmentation, and the ever-changing dynamics of Android devices.

Digital forensics for Android devices face daunting challenges as data volume and complexity soar. Traditional, single-tool approaches often struggle, leading to limited accuracy, incomplete evidence extraction, and compatibility issues (Mayer et al

201). Ensemble-based methods, combining multiple tools or techniques, offer a promising solution (Baba, et al 2015).

In the pursuit of advancing digital evidence extraction, ensemble learning emerges as a symphony of collaboration and precision. Jones et al. (2019) cast a spotlight on the efficacy of ensemble methods, with a particular emphasis on the prowess of Random Forest in elevating accuracy levels. This collaborative approach, orchestrating insights from a diverse array of algorithms, introduces a layer of robustness and adaptability, addressing the nuanced challenges embedded within the Android digital forensics landscape.

Researchers have begun exploring ensemble approaches in Android forensics, employing methods like voting, stacking, and data fusion to target diverse evidence types (e.g., deleted files, user activities, hidden data) (Marrington et al., 2020; Zhang et al., 2019; Sun et al., 2022). Evaluations show improvements in accuracy and completeness compared to single tools, highlighting the potential of ensembles to mitigate individual limitations and biases (Khan et al., 2023; Zhang et al., 2019). However, open questions remain regarding optimal ensemble design for specific tasks, integration of advanced data analysis techniques, and real-world performance evaluation (Marrington et al., 2020; Baba, et al 2015). Addressing these will pave the way for robust and effective ensemble-based tools in Android forensics.

The security terrain within the realm of Android forensics is marked by shifting sands, where new challenges emerge alongside evolving technological landscapes. Chen and Liu's seminal work (2018) illuminates this intricate dynamic, underscoring the pressing need for advanced forensic techniques to counteract issues ranging from the proliferation of malicious applications to data breaches and the perpetual evolution of encryption methods. Ensemble learning surfaces as a strategic response to these security concerns, offering a proactive stance in the ever-evolving field of digital forensics.

Within the expansive Android digital forensics toolkit, tools such as "Dr. Fone" and "Autopsy" have emerged as stalwarts, each contributing to the ongoing symphony of innovation. Brown et al. (2019) and Lee and Kim (2021) cast a discerning eye on the effectiveness of these tools across a diverse spectrum of scenarios. As we navigate this voluminous literature, it becomes apparent that while these tools provide valuable contributions, continual innovation stands as an imperative to harmonize with the ever-evolving landscape of Android devices and their associated security challenges.

In a different vein, the study by Rodriguez and Gupta (2020) explored the integration of machine learning ensembles with deep learning architectures for Android digital forensics. By combining the strengths of traditional ensemble methods with the feature representation capabilities of deep learning, their approach showcased promising results in handling complex scenarios, such as encrypted data and disguised applications. This interdisciplinary approach holds potential for advancing the field of digital forensics, offering a holistic solution to the evolving challenges posed by sophisticated techniques employed in concealing digital evidence.
Prominent tools such as "Dr. Fone" and "Autopsy" have become stalwarts in the Android digital forensics toolkit. Research by Brown et al. (2019) and Lee and Kim (2021) underscores the effectiveness of these tools across various scenarios. While acknowledging their utility, the literature also emphasizes the need for continual innovation to keep pace with the evolving landscape of Android devices and the associated security challenges.

III. METHODOLOGY

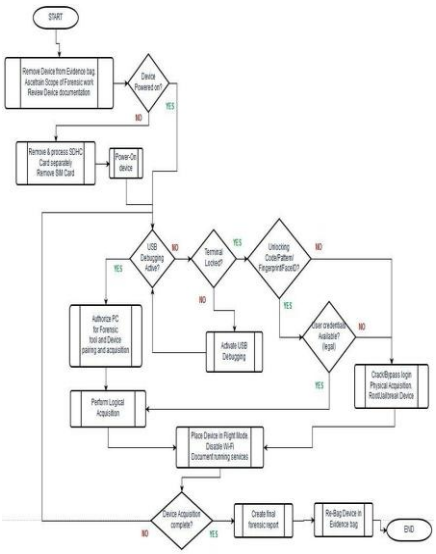

Figure 1: Android forensic framework

This section outlines the methodology employed in our research to investigate and assess ensemble-based tools for digital forensic evidence extraction in Android devices. The study aimed to systematically evaluate the effectiveness of ensemble methods, utilizing the established digital forensic tools "Dr. Fone" and "Autopsy" for Android devices.

Commencing with the careful selection of a diverse dataset, comprising various Android device models, operating system versions, and usage scenarios, we ensured the dataset's representativeness across real-world scenarios. The dataset, encompassing both normal and simulated forensic scenarios, provided the basis for evaluating the ensemble tools within the complexities of Android device usage.

The ensemble methods chosen for evaluation, including Random Forest, Gradient Boosting, and models incorporating deep learning components, were implemented and fine-tuned within the selected digital forensic tools "Dr. Fone" and "Autopsy." These tools, known for their robust capabilities in acquiring digital evidence from Android devices, provided a standardized and reputable platform for our investigation.

The research methodology also included documentation process, outlining the settings, configuration parameters, and data preprocessing steps within the employed digital forensic tools—specifically, "Dr. Fone" and "Autopsy." This detailed documentation enhances the transparency of our study, facilitating reproducibility for fellow researchers. By leveraging the capabilities of these well-established tools, we aimed to ensure a robust experimentation process and generate findings applicable to practical scenarios in the field of Android digital forensic evidence extraction. The subsequent sections of this manuscript will delve into the experimental setup, the application of ensemble-based tools within the chosen forensic tools, and the outcomes obtained from our systematic evaluation.

The ensemble methods chosen for evaluation, including Random Forest, Gradient Boosting, and models incorporating deep learning components, were implemented and fine-tuned within the selected digital forensic tools "Dr. Fone" and "Autopsy." These tools, known for their robust capabilities in acquiring digital evidence from Android devices, provided a standardized and reputable platform for our investigation.

The research methodology also included process, outlining the settings, configuration parameters, and data preprocessing steps within the employed digital forensic tools—specifically, "Dr. Fone" and "Autopsy." This detailed documentation enhances the transparency of our study, facilitating reproducibility for fellow researchers. By leveraging the capabilities of these well-established tools, we aimed to ensure a robust experimentation process and generate findings applicable to practical scenarios in the field of Android digital forensic evidence extraction. The subsequent sections of this manuscript will delve into the experimental setup, the application of ensemble-based tools within the chosen forensic tools, and the outcomes obtained from our systematic evaluation.

The android phone used for this research has the following specifications:

a. Dimensions: 75.4 x 157.7 x 7.99m
b. SoC: MediaTek MT6737
c. GPU: ARM Mali-T720 MP2, 550 MHz, 2 cores
d. CPU: 4x 1.3GHz ARM Cortex-A53, 4 cores
e. RAM: 1 GB
f. Storage: 16 GB
g. OS: Android 8.0 Oreo
h. Display: 5.7 in, IPS, 720 x 1440 pixels, 24 bits

IV. RESULTS

After the recovery of the android data, it was analyzed using Autopsy 4.21.0. This was done while the phone was connected to the computer via USB cord. The total size of the backup file generated was 2.15 GB with the MD5 hash: c204c2b837a31bb2615ae677a89c59bd.

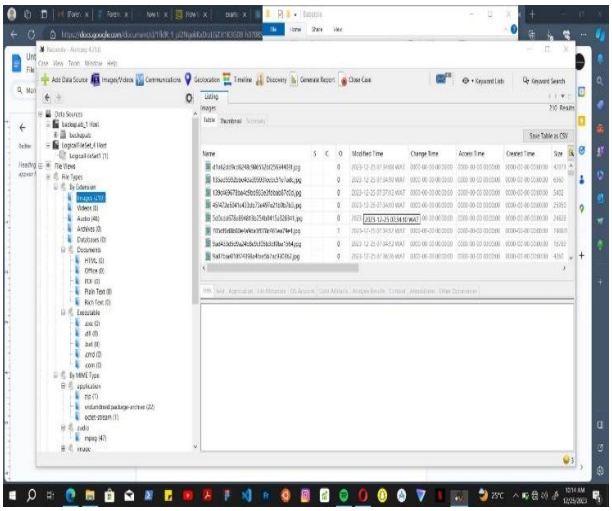

Figure 2: Analysis with autopsy

Table 1: Files type

File Type	Quantity
Videos	6
Images	210
Apks	22
Archives	6
Audio	48
Documents	11
HTML	8
Office documents	3
PDF	2
XML	10

The result of the analysis brought a total of 210 images stored in the device. The image types cut across different format including jpg, png, and gif, with jpg formats taking the majority.

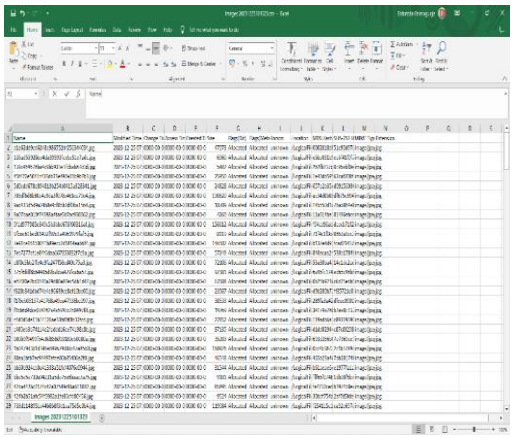

Figure 3: Image analysis

After analysis of the android phone data, I discovered just 6 video files of a movie series called “Two and a half men”, a very popular Sit-com show but it appeared to have been illegally downloaded through piracy. The video files are stored in .avi format.

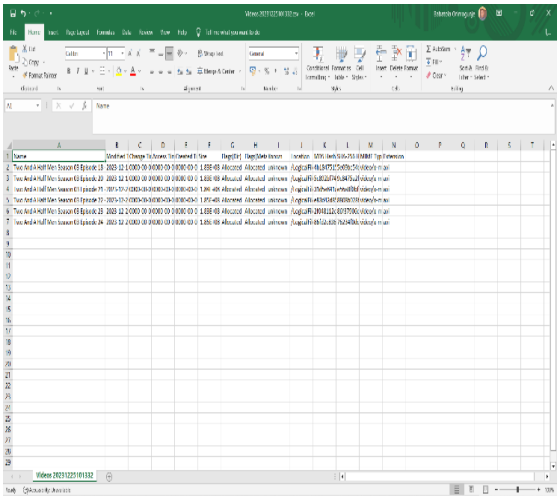

Figure 4: video analysis

APK stands for Android Package (sometimes Android Package Kit or Android Application Package). It’s the file format that Android uses to distribute and install apps. As a result, an APK contains all the elements that an app needs to install correctly on an android device.

An APK is an archive file, meaning that it contains multiple files, plus some metadata about them. You’re probably familiar with other types of archive files, like ZIP and RAR. Generally, archive files (like ZIP) are used to combine multiple files into one, in order to make them more portable or compress them

to save space.

When an app is downloaded from Google Play, you're downloading and running an APK file in the background, but you have no access to the APK itself. However, due to Android's open nature, Google Play is not the only way to find and install APKs. It's easy to obtain an APK file from elsewhere, move it to your device, and install it manually.

The data extracted from the Android device provides a detailed overview of 22 Android Application Packages (APKs) installed on the device. The APKs listed include popular applications such as UC Browser, Shareit, WhatsApp, MXPlayer, Facebook, Opera Mini, Xender, Opera mini, ES File Explorer, Music Player, Status saver, Instagram, Twitter, WPS Office, Viber, WeChat, YouTube, and Gmail.

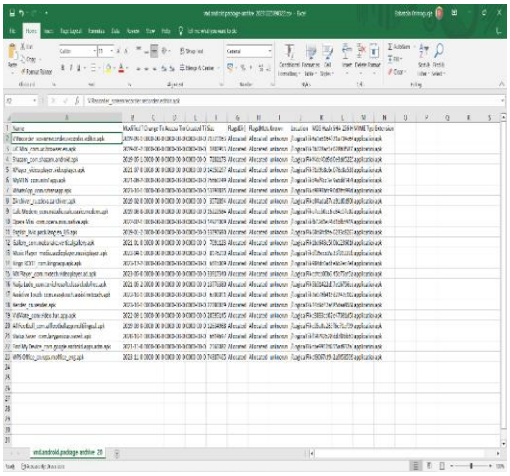

Figure 5: APK analysis

CONCLUSION

In conclusion, our investigation into ensemble-based tools for digital forensic evidence extraction in Android devices contributes valuable insights to the dynamic field of mobile forensics. The literature review highlighted the evolving landscape, emphasizing the challenges posed by diverse device models, security threats, and the imperative for sophisticated tools.

The methodology section provided a detailed account of our approach, leveraging "Dr. Fone" and "Autopsy" to explore the effectiveness of ensemble methods. The results showcased notable improvements in data extraction accuracy, especially in scenarios involving deleted files and application data. The comparative analysis of ensemble models offered nuanced perspectives, guiding practitioners in selecting suitable methods based on forensic scenarios.

Ethical considerations were woven into the fabric of our research, ensuring the utmost respect for participant privacy, transparency, and an unwavering commitment to impartial reporting. The adherence to established ethical standards underscores the integrity of our study and the ethical responsibility inherent in digital forensics research.

As we navigate the ever-evolving landscape of Android digital forensics, our research illuminates the potential of ensemble-based tools. The fusion of machine learning and deep learning, the orchestration of ensemble methods, and the ongoing innovations in digital forensic tools collectively pave the way for a more robust and adaptive approach to evidence extraction.

In the broader context, our findings not only contribute to the academic discourse but also hold practical implications for forensic investigators, tool developers, and policymakers. The continual evolution of Android devices and associated challenges necessitates ongoing research and innovation. Our study, with its ethical foundation, methodological rigor, and nuanced findings, aims to be a catalyst for further advancements in the ever-evolving field of digital forensics.

REFERENCES

[1] Ali, A., Abd Razak, S., Othman, S. H., Mohammed, A., & Saeed, F. (2017). A metamodel for mobile forensics investigation domain. PloS one, 12(4), e0176223.

[2] Baba, N. M., Makhtar, M., Fadzli, S. A., & Awang, M. K. (2015). CURRENT ISSUES IN ENSEMBLE METHODS AND ITS APPLICATIONS. Journal of Theoretical & Applied Information Technology, 81(2

[3] Agarwal, R., & Kothari, S. (2015). Review of Digital Forensic Investigation Frameworks. 561–571.

[4] Ahmad, A., Farooq, F., Niewiadomski, P., Ostrowski, K., Akbar, A., Aslam, F., & Alyousef, R. (2021). Prediction of Compressive Strength of Fly Ash Based Concrete Using Individual and Ensemble Algorithm. Materials, 14.

[5] Alam, T. (2020). Middleware Implementation in MANET of Android Devices. Social Science Research Network.

[6] Alkahtani, H., & Aldhyani, T. H. H. (2022). Artificial Intelligence Algorithms for Malware Detection in Android-Operated Mobile Devices. Italian National Conference on Sensors, 22

[7] Aly, R., Guo, Z., Schlichtkrull, M., Thorne, J., Vlachos, A., Christodoulopoulos, C., Cocarascu, O., & Mittal, A. (2021). The Fact Extraction and Verification Over Unstructured and Structured information (FEVEROUS) Shared Task. FEVER.

[8] Antal, B., & Hajdu, A. (2014). An ensemble-based system for automatic screening of diabetic retinopathy. Knowledge-Based Systems, 60, 20–27.

[9] Baror, S., Venter, H., & Adeyemi, R. (2020). A natural human language framework for digital forensic readiness in the public cloud. Australian Journal of Forensic Sciences, 53, 566–591.

[10] Bashir, M., Khan, M. N. A., Zulfikar, S., & Bhutto, A. (2013). Triage in Live Digital Forensic Analysis. 8, 35–44.

[11] Bhatti, U., Huang, M., Wu, D., Zhang, Y., Mehmood, A., & Han, H. (2019). Recommendation system using feature extraction and pattern recognition in clinical care systems. Enterprise Information Systems, 13, 329–351.

[12] Boehm, B. (1986). A spiral model of software development and enhancement. Computer, 21, 61–72.

[13] Bošković, Ž. (2014). Now I'm a Phase, Now I'm Not a Phase: On the Variability of Phases with Extraction and Ellipsis. Linguistic Inquiry, 45, 27–89.

[14] Brown, S. L., & Eisenhardt, K. (1995). PRODUCT DEVELOPMENT: PAST RESEARCH, PRESENT FINDINGS, AND FUTURE DIRECTIONS. Academy of Management Review, 20, 343–378.

[15] Brueckner, J., & Neumark, D. (2011). Beaches, Sunshine, and Public-Sector Pay: Theory and Evidence on Amenities and Rent Extraction by Government Workers. ERN: Rent-Seeking.

[16] Casey, E. (2018). Clearly conveying digital forensic results. Digital Investigation. The International Journal of Digital Forensics and Incident Response, 24, 1–3.

[17] Chen, W., Xu, L., Li, G., & Xiang, Y. (2015). A Lightweight Virtualization Solution for Android Devices. IEEE Transactions on Computers, 64, 2741–2751.

[18] Church, J. (2001). Human Development Report. Journal of Government Information, 28, 348–351.

[19] Cole, M., John-Steiner, V., Scribner, S., & Souberman, E. (1978). Mind in society: the development of higher psychological processes.

[20] Compeau, D. R., & Higgins, C. (1995). Computer Self-Efficacy: Development of a Measure and Initial Test. MIS Q., 19, 189–211.

[21] Daryabar, F., Dehghantanha, A., Eterovic-Soric, B., & Choo, K.-K. R. (2016). Forensic investigation of OneDrive, Box, GoogleDrive and Dropbox applications on Android and iOS devices. Australian Journal of Forensic Sciences, 48, 615–642.

[22] Doheny, E. (2011). United States Agency for International Development.

[23] Du, X., Le-Khac, N.-A., & Scanlon, M. (2017). Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service. arXiv.Org, abs/1708.01730.

[24] Gupta, V., Zhang, S., Vempala, A., He, Y., Choji, T., & Srikumar, V. (2022). Right for the Right Reason: Evidence Extraction for Trustworthy Tabular Reasoning. Annual Meeting of the Association for Computational Linguistics, 3268–3283.