Zhongguo Kuangye Daxue Xuebao
Journal of China University of Mining and Technology

2023 | Vol 28 | Issue 2 | Page 1-3
Journal Homepage: https://zkdx.ch/
DOI: 10.1654/zkdx.2023.28.2-1

Machine Scientific Reverse Engineering in Quark

Anas Jamwal*
Department of Computer Applications, DAPC College, University of Madrasi, India
*Corresponding author

Abstract
Android forensic reverse engineering is the process of analyzing the internal structure of Android applications and the underlying operating system to extract useful information and detect potential security threats. This involves disassembling the binary code of an Android app, identifying its components and functionalities, and uncovering any hidden or malicious activities. Forensic reverse engineering can be used to investigate a variety of security incidents, including data breaches, malware attacks, and intellectual property theft. It can help identify thesource of a security breach, determine the scope of the damage, and provide insights intothe methods and tools used by attackers .Some of the key techniques used in Android forensic reverse engineering include dynamic analysis, static analysis, and reverse engineering tools such as disassemblesand decompilers. These tools can help extract information from an Android app such as its file system, network traffic, and memory usage. Overall, Android forensic reverse engineering is an important field for enhancing the security of Android-based devices and applications, and for detecting and mitigating potential threats.In the era of smartphones, Android has become one of the most popular mobile operating systems, powering millions of devices worldwide. With the rise of mobile devices, the need for mobile security has become increasingly important. In this context, Android forensic and reverse engineering are important techniques to identify potential security risks in Android applications. Quark is a powerful tool that can be used to analyze the behavior of Android applications and identify potential vulnerabilities. This includes decompiling APK files, monitoring network traffic, and extracting data from Android devices. By using Quark in combination with other forensic tools and techniques, investigators can gain a comprehensive understanding of the behavior of Android applications and identify potential security risks. In this article, we will explore the various aspects of Android forensic and reverse engineering in the context of cybersecurity, with a focus on using Quark to analyze and extract data from Android devices.

Keywords: Cyber security, Quark, Android forensic

1. Introduction
Android forensic reverse engineering in Quark for cybersecurity is a project that aims to explore the various aspects of Android forensic and reverse engineering techniques using the Quark tool. In the era of smartphones, the use of Android mobile devices has become ubiquitous, making mobile security a crucial aspect of cybersecurity(Soe Myint Myatand May Thu Kyaw. 2019). As such, it is important to have an understanding of how to identify potential security risks in Android applications, which is where Android forensic and reverse engineering techniques come in(You and Yim, 2010).The project will cover various topics, including the Android architecture and components, Android application components, Android security model, and the Android debug bridge (ADB). Additionally, the project will explore the different types of reverse engineering techniques that can be used, along with the various Android forensic tools available (Bassey Asuquo Ekanem and Jacob Meye 2021).

The project will also demonstrate how to extract data from Android devices using different techniques, including physical extraction, logical extraction, cloud extraction, and app data extraction. Furthermore, the project will focus on using Quark, a powerful open-source tool, to analyze and extract data from Android devices. Quark can be used for decompiling APK files, monitoring network traffic, and analyzing Android applications' behavior to identify potential security risks. Overall, this project aims to provide a comprehensive understanding of Android forensic and reverse engineering techniques and their importance in mobile security(Wang et al.,2018). The project will also demonstrate how to use Quark to identify potential security risks in Android applications, making it a valuable resource for those interested in cybersecurity and mobile security(RastogiV 2013).

2. Modules
2.1 Materials:

A computer running a Linux operating system. An Android device or emulator-Quark tool-Android SDK and ADB tools-Other forensic tools as necessary (Guo et al.,2020). including physical extraction, logical extraction, cloud extraction, and app data extraction. Furthermore, the project will focus on using Quark, a powerful open-source tool, to analyze and extract data from Android devices. Quark can be used for decompiling APK files, monitoring network traffic, and analyzing Android applications' behavior to identify potential security risks. Overall, this project aims to provide a comprehensive understanding of Android forensic and reverse engineering techniques and their importance in mobile security.

2.2 Understanding Android Architecture and Components:
Researchand study the Android architecture and components. Gain an understanding of how Android applications are built and run. Understand the different components of an Android application, such as activities, services, and broadcast receivers. Analyze how Android applications interact with the operating system and hardware(Dalla Preda and Maggi, 2017).

2.3 Understanding Android Application Components:
Study the different types of Android application components. Learn how these components interact with each other and the Android operating system. Analyze how different components can be used for malicious purposes.

2.4 Understanding Android Security Model:
Research and study the Android security model. Gain an understanding of Android's permission system. Learn about Android's sandboxed environment. Analyze the potential vulnerabilities in Android's security model. Using Android Debug Bridge (ADB):Install Android SDK and ADB tools. Learn how to connect and use ADB with an Android device. Explore the different ADB commands and how they can be used for forensic analysis.

2.5 Understanding Reverse Engineering Techniques:
Study the different types of reverse engineering techniques. Understand how they can be used for analyzing Android applications. Analyze the potential risks andlimitations of each technique.

2.6 Using Forensic Tools:
Explore different forensic tools available for Android devices. Learn how to use them for forensic analysis. Analyze the output of forensic tools and extract relevant data.

2.7 Using Quark:
Install and configure Quark. Use Quark for decompiling APK files and analyzing the behavior of Android applications. Analyze network traffic using Quark. Extract data from Android devices using Quark.

3. Summary and Conclusion

In summary, the Android forensic reverse engineering in Quark for cybersecurity project aims to analyze the security of Android devices using reverse engineering techniques and the Quark tool. The project involves studying the Android architecture and components, understanding Android application components and security models, using ADB and other forensic tools, and applying reverse engineering techniques to identify potential security risks.

The use of Quark tool allows for the decompilation of Android applications, analyzing their behavior, and extracting data from the Android device. The project aims to provide a comprehensive understanding of Android forensic and reverse engineering techniques, and how they can be applied to improve the security of Android devices.In conclusion, the project highlightsthe importance of understanding the security risks associated with Android devices and the need for effective forensic and reverse engineering techniques to identify and mitigate these risks. By applying these techniques and using tools such as Quark, it is possible to improve the security of Android devices and protect users from potential security threats.

References

1. Bassey Asuquo Ekanem and Jacob Meye (2021).Application of Reverse Engineering Technique in Software Forensic Analysis to Detect Infringements. Proceedings of the World Congress on Engineering. GuoJ,D.Liu,R.Zhao,Z.LiWltdroid(2020): repackaging detection approach for android applicationsInternational Conference on Web Information Systems and Applications,Springer, pp.579-591
2. Dalla,M., Preda,F.Maggi(2017). Testing android malware detectors against code obfuscation: a systematization of knowledge and unified methodology. Journal of Computer Virology and Hacking Techniques,13,pp.209-232
3. RastogiV,Y.Chen,X.Jiang(2013). Droidchameleon: evaluating android anti-malware against transformation attacksProceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security, pp.329-334Soe

4. Myint Myat, May Thu Kyaw. (2019). Analysis of Android Applications by Using Reverse Engineering Techniques, International Journal of Innovative Science and Research Technology, 4(3):551-558.
5. Wang, Y., H.Wu,H.Zhang,A.RountevOrlis (2018)obfuscation-resilient library detection for androidIEEE/ACM 5th International Conference on Mobile Software Engineering and Systems (MOBILESoft),IEEE, pp.13-23You, I and K.Yim(2010). Malware obfuscation techniques: a brief surveyInternationalConference on Broadband, Wireless Computing, Communication and Applications,IEEE, pp.297-300.