The number of malicious Android apps is increasing rapidly. Detecting and removing malware apps is insufficient, since they can damage or alter other files or settings, install additional applications, etc. To determine such behaviors, a security analyst can significantly benefit from identifying the family to which an Android malware belongs. Techniques for detecting Android malware, and determining their families, lack the ability to handle certain obfuscations that aim to thwart detection. Moreover, some prior techniques face scalability issues, preventing them from detecting malware in a timely manner.

To address these challenges, I will present a novel machine learning-based Android malware detection and family identification approach, RevealDroid, that operates accurately and efficiently without the need to perform complex program analyses or to extract large sets of features. On a dataset of 51,496 malicious and benign apps, RevealDroid achieves an accuracy of 91%. For 18,065 malicious apps from 68 families, RevealDroid can identify the malware family of an app with an accuracy of 87%.