CSCE 660 Abstract

Marvin Newlin

Log files are a critical component of cyber security, and in the mobile world, specifically with Android, logs are an imperative for keeping phones secure. From a Machine Learning (ML) aspect, log files present an useful application of structured text manipulation and are of particular interest for synthetic generation as seen in Wurzenberger et al [1]. This paper presents a survey of Android logs, both their formats and types, and the tools used to manipulate them. We then explore the process of creating a small Android log dataset by extracting the system logs from an Android phone.

This paper explores the Android Log API, which provides a framework for developers building apps to integrate logging into their apps [2]. We then explore the tools for manipulating Android logs. The built in logging tool is a tool called Logcat [3]. Additional logging tools have been presented such as Data Extraction and Logging Tool for Android (DELTA) [4] and a method for non-redundant logs called NVM [5].

Utilizing the logcat logging tool, we then explore the process of building a small dataset for structured text manipulation. We explore the formats of the system and application logs within the Android framework. The purpose of this is to develop a dataset for synthetic text generation due to the limited availability of Android log datasets.

References

[1] M. Wurzenberger, F. Skopik, G. Settanni, and W. Scherrer, “Complex log file synthesis for rapid sandbox-benchmarking of security- and computer network analysis tools,” *Inf. Syst.*, vol. 60, no. C, pp. 13–33, Aug. 2016.

[2] “Log  |  Android Developers.” [Online]. Available: https://developer.android.com/reference/android/util/Log. [Accessed: 22-Apr-2019].

[3] “Logcat command-line tool  |  Android Developers.” [Online]. Available: https://developer.android.com/studio/command-line/logcat. [Accessed: 22-Apr-2019].

[4] R. Spolaor, E. D. Santo, and M. Conti, “DELTA: Data Extraction and Logging Tool for Android,” *IEEE Trans. Mob. Comput.*, vol. 17, no. 6, pp. 1289–1302, Jun. 2018.

[5] Y. Xu and Z. Hou, “NVM-Assisted Non-redundant Logging for Android Systems,” in *2016 IEEE Trustcom/BigDataSE/ISPA*, 2016, pp. 1427–1433.

Conferences

1. SECURWARE 2019: <https://www.iaria.org/conferences2019/SECURWARE19.html>

2. 2019 International Conference on Cyber Conflict U.S. (CyCon U.S.) [CyCon 2019](http://aci.cvent.com/events/2019-international-conference-on-cyber-conflict-cycon-u-s-/event-summary-6fa2dad0721d43249d40ca05d3a5e94a.aspx)

3. Big Data 2019 <http://www.icmu.org/icmu2019/?submission>

4. DSAA 2019 : The 6th IEEE International Conference on Data Science and Advanced Analytics (DSAA 2019) [DSAA 2019](http://dsaa2019.dsaa.co/).

5. IEEE GLOBECOM 2019 <https://globecom2019.ieee-globecom.org/authors/call-symposium-papers>