C9 An Initial Forensic Analysis of Sailfish OS

Krassimir Tzvetanov, MS, Purdue University, Lafayette, IN ; Umit Karabiyik, PhD, Purdue University, Knoy Hall, Lafayette, IN 47907-2021*

Learning Overview: The goal of this presentation is to address a gap in the forensics analysis of Sailfish OS. This presentation focuses on mapping the digital artifacts pertinent to an investigation, which can be found on the file system of a phone running Sailfish OS 3.2. Currently, there is no other known publicly available research and very few commercially available solutions for the acquisition and analysis of this platform. This is a significant gap, as this Operating System's (OS's) adoption is accelerating in emerging markets on low-cost devices in countries like Russia, China, and India. This presentation documents many of the significant forensics' points of interest, such as call and text, log, phonebook, web browser artifacts, and hardware-specific features.

Impact on the Forensic Science Community: This presentation will impact the forensic science community by providing extensive detail on analyzing mobile phones running Sailfish OS. Sailfish OS is a Linux® kernel-based, embedded-device operation system, mostly deployed on cell phones. Currently, there is no sufficient research in this space. Simultaneously, this operating system is gaining popularity, so it is likely investigators will encounter it in the field.

This system has been rapidly deployed in Russia, India, and China. A clear example of rapid deployment is the mass deployment of eight million hand-held devices planned by the Russian government by the end of 2021. In India, the OS is deployed by some of the major network providers, and in China, Huawei is investigating it as an Android™ replacement, as economic tensions with the United States arise.

This presentation shows the mapping of the digital artifacts, pertinent to an investigation, which can be found on the file system of a phone running Sailfish OS 3.2. It covers call logs, text messages, location services, address books, and other important artifacts. The analysis was conducted based on a comparison of the image of the phone before and after controlled changes were introduced.

Sailfish OS, Cellphone, Artifact Analysis