Read the article "Social Media Forensics" Comments on key findings.

The article: Social Media Forensics tries to emphasize the need to have mobile devices as sources of content for forensic investigation due to their access to social media and instant messaging services. This capability of such devices has facilitated malicious activities, Copyright infringement, cyberstalking, cyberbullying, sexual harassment, and so on, making them critical origins of data during a digital investigation. Hence, to verify this scenario, the researchers carefully examined and analyzed social media (Facebook, Twitter, and Google+) and instant messaging services (Telegram, OpenWapp, and Line) in Peak, a Geeksphone model running Firefox Operating System.

The motive for the research lies in the continually changing misuse of social media and instant messaging services by Cybercriminals to target rapidly growing social media and instant messaging users. The criminals can also utilize these services to deploy malicious codes that allow them to retrieve confidential information. Hence, identifying the individuals or groups behind these activities becomes critical to solves cases such as sexual harassment, threats, bullying, and so on. Unfortunately, this is not an easy task since the difference between mobile devices mandates forensics investigators to develop customized methods and techniques to conduct investigations.

However, according to the researchers, regardless of how complex the investigation can be, social media forensics consists of unique elements. These include the identification of mobile devices’ internal storage, flash memory, and internal volatile memory as valuable sources of digital evidence. As a result, the unique elements were considered when conducting the study.

After analyzing data from various sources, the researchers conclude that most of the valuable forensic information was residing in volatile memory according to the 24 forensic images they acquired from a Firefox Operating System internal phone and volatile memory. Surprisingly, they were also able to recover and trace social media account credentials after they deduced that their forensic tools were able to read data since the memory in the mobile device wasn’t encrypted. On the other hand, they also found that all untraced information in phone images such as profile name on Google+ and user’s phone number for Telegram and Line were traceable in-memory images. Furthermore, by analyzing the same services, both in application and mobile web platforms, the researchers were able to conclude that Firefox Operating System applications behaved the same way as their counterpart websites.

That being said, to comment more on the article, I firmly believe that the researchers’ analysis could pave the way for future forensic investigators to trace and examine residual remnants of forensics value in the Firefox Operating System. That is, the data remnants when application artifacts are uninstalled, as well as leftover information from the application folders and browser history, will have significant value in mobile forensics investigation if it is acquired using a set of strategies to maintain the integrity of the residing data.