Facebook Application Forensics Research Gap Proposal

Ruiyang Liu

In the research, I present the similarities and differences of Facebook's virtual disk file and memory dump forensics under three systems, Linux OS, Android OS and Win7 OS. in each system, several core information were tested, including user information, friend information, instant message content, and posting and comment content. The basic process is that you need to setup three system virtual machines first, and then log in as a Facebook user within the virtual machine, chat with friends, post content, comment on your own posted content and other people's posted content. Finally, use the manual keyword search method to search for useful information in Hex Editor or FTK. However, there are some questions and uncertainties in my research, and they are perfect for my gap research.

Firstly, according to the papers and sources I have referenced, all Facebook forensics use a manual method of setting up keyword searches. This method is very inefficient in the first place. Second, you need to have a lot of known information in order to search. For example, if you want to manually search Facebook chat log information, it is actually more difficult to find forensic evidence if you don't know at all who and what the chat is about. After studying other students' research, I lacked the process of using forensic tools for examine. So the next most critical research direction is to find and use tools or automated code for three different platform memory dumps to further analyze.

Second, according to the summary of my report, there is a big difference in the information that can be obtained from the three systems and it is difficult to draw a direct conclusion as to which system is more or less secure. I would like to explore the root causes for the different evidence of Facebook forensics by the three systems. The "root cause" here refers to the underlying logic of the systems that operate on Facebook to process and store information. In my study, all conclusions come from my searches and observations of search results, which are relatively superficial, so I cannot explain many of the search

results. It would be a great progress for my research if I could explain from the underlying logic why certain user actions are forensic and certain actions are not forensic. At the same time, when obtaining forensic evidence, the same information can usually appear in the memory dump many times. For example, evidence of a chat log may reappear many times in the memory dump. Since I don't understand the internal logic of how operation systems deal with the Facebook operations, I can't explain the phenomenon.

Finally, when using the Hex Editor or FTK imager and other RAM reader tools to view the virtual disk file or memory dump, the readability of the contents of different systems varies greatly. Here the readability specifically refers to the readability of valid information, for example, when using Hex Editor to read the Linux memory dump, the proportion of garbled and "random characters" is greater than that of Android and Win systems. I would like to investigate the reason for this situation. If I can know the cause, I can obviously get more valid forensic evidence. Because in the process of forensics, I can feel that a lot of valid information is hidden in the already garbled memory dump.