Forensics Data Recovery of Skype Communication from Physical Memory

DR. Ahmad Ghafarian

Abstract

Computer forensics is the application of computer science to the investigation and analysis techniques for gathering and preserve evidence from a particular computer in a manner that is admissible to the court of law. Computer forensic techniques can be used for investigating crimes, policy violations, or reconstructing data. The first step in any computer forensics investigation is to decide on potential sources for acquisition of data. Generally, there are two sources of data on a machine namely, hard drive and physical memory (RAM). The data stored on hard drive are permanent in nature and the techniques and tools for this kid of forensics are fairly established. On the other hand, the data on RAM is volatile and its content is lost when the machine is powered down. Because not all data needed exists in hard drive forensics, physical memory forensics have become popular in recent years.

In physical memory forensics, the live memory is captured or dumped as a raw image file and then memory analysis tools is used to examine and analyze the captured image file. Physical memory forensics enable us to retrieve most evidential data related to an incident respond. The goal of this research is forensics investigation of volatile data artifacts related to Skype communication. We will specifically focus on the data related to the possible misuse of Skype communication. We will be looking at logins credentials, audio/video conversations, transferred files, email, and geographical location of the caller. There are three reasons for the focus of the research. The first is, to the best of our knowledge, there are no published results about specifics focus of Skype forensics. The second reason is that Instant messaging technology such as Skype is increasingly becoming popular and computer forensics investigators may benefit from the techniques for retrieval of Skype-related artifacts from the RAM. The third is, the author is very familiar with the underlying architecture of Skype through other previous researches. Our results will provide practitioners with a better picture of the live system. We will determine what kind of data we can retrieve via memory forensics. In addition, the results of this research will arm the practitioners with the tools and methodologies in their investigation of Skype misuse. Finally, this research will engage our undergraduate students in meaningful research.