Abstract

Instant messaging technology is increasingly becoming popular among individuals, businesses, as well as criminals. Technologies such as Skype is widely used due to its secure and cheap services. Traditional static media computer forensics approach is not effective in retrieving traces of instant messaging activity. This research presents the findings from physical memory forensics examination of Skype communication. We examined both client-based Skype as well as web-based Skype to determine whether the forensics data remnants in memory would be different for each case. For each case, we evaluated the forensics artifacts at both the operating system level and the application level. At the operating system level, we examined active processes, terminated processes, hidden processes and open files related to Skype activity. At the application level, we evaluated Skype activity artifacts such as logins credentials, audio and video conversations, transferred files, emails, and geographical location of the caller. In addition, we found some differences in the client-based and web-based Skype data remnants in memory. Overall, we confirm that physical memory forensics is the most effective technique for retrieving forensics artifacts of instant messaging technology.
References

14. Karayiannis, S., and Katos V. Practical Password harvesting from Volatile Memory. Information Security and Incident Response Unit, Democritus University of Thrace (retrieved from research gate), 2012.
15. Skype Forensics: shows geographical location http://resources.infosecinstitute.com/skype-forensics-2/#gre
19. Cai L., Sha J. and Qian W. Study on Forensic Analysis of Physical Memory. 2nd
29. XML editor, retrieved from https://www.liquid-technologies.com

Index Terms

Computer Science

Information Sciences

Keywords

Skype; forensics; instant messaging; artifacts; geographic location; operating systems; IM