Digital Forensic Exploration Framework for Email and Instant Messaging Applications

Authors : T. Manesh, Abdalla A. Alameen, M. Mohemmed Sha, A. Mohamed Mustaq Ahmed

Abstract : Email and instant messaging applications are foremost and extensively used electronic communication methods in this era of information explosion. These applications are generally used for exchange of information using several frontend applications from various service providers by its users. Almost all such communications are now secured using SSL or TLS security over HTTP communication. At the same time, it is also noted that cyber criminals and terrorists have started exchanging information using these methods. Since communication is encrypted end-to-end, tracing significant forensic details and actual content of messages are found to be unattended and severe challenges by available forensic tools. These challenges seriously affect in procuring substantial evidences against such criminals from their working environments. This paper presents a vibrant forensic exploration and architectural framework which not only decrypts any communication or network session but also reconstructs actual message contents of email as well as instant messaging applications. The framework can be effectively used in proxy servers and individual computers and it aims to perform forensic reconstruction followed by analysis of webmail and ICQ messaging applications. This forensic framework exhibits a versatile nature as it is equipped with high speed packet capturing hardware, a well-designed packet manipulating algorithm. It regenerates message contents over regular as well as SSL encrypted SMTP, POP3 and IMAP protocols and catalyzes forensic presentation procedure for prosecution of cyber criminals by producing solid evidences of their actual communication as per court of law of specific countries.

Keywords : forensics, network sessions, packet reconstruction, packet reordering

Conference Title : ICCCISE 2017 : International Conference on Computer, Communication and Information Sciences, and Engineering

Conference Location : Jeddah, Saudi Arabia

Conference Dates : January 30-31, 2017

Open Science Index, Computer and Information Engineering Vol:11, No:01, 2017 publications.waset.org/abstracts/57591.pdf