Example of literature review on forensic examination of skype

Law, Evidence

Introduction

Crimes digital evidence recovery from the storage media is actually a growing time consuming process since the storage media capacity is in a constant growth state. In addition, it is a complex and difficult task for forensic investigator to examine all the locations in storage media. In modern days, it is actually generally accepted that there is continuing technological evolution including networks, computers, and e-commerce among others, which are ever more involved in aspects of human life. Crimes and illegal activities have in addition increased with the technological evolution. Various organizations are in fact suffering from computer crimes and criminals, which perpetrate them and possess a range of motivations. For instance, criminals may have their terrorism goals or may aim to destroy customer confidence and reputation of the organizations. Computer forensic or digital forensic is a new field in the forensic investigations as a result of crimes moving into computing environment.

Skype is one of the technological evolutions that are taking place at an increasing rate. It is essentially communications software, which allows its users to communicate with one another in the real time using video chat, voice over IP, or a more traditional text chat (Abdulezer 2007). Its uniqueness among the other instant messaging applications is due to the fact that it runs over decentralized peer to peer network instead of routing all the communications packets through central server. It is designed to function out of box on the modern networks and additionally does not have problems working behind Newark Address Translation devices or the other firewalls. Due to its decentralized architecture, it makes broad use of encryption that is strong, making casual impersonation or eavesdropping all but impossible.

Skype usage is on an increasing demand. This is because it is believed to bring people together and in particular, it brings businesses people together, helping their businesses to overcome barriers of distance, cost, and technology. It also allows these people to do more everywhere throughout the world. However, Skype usage has various effects on windows registry. Windows registry is actually a hierarchical database, which stores the configuration options and settings on the Microsoft windows operating systems. This registry contains settings for the low level operating system components (Gough 2006). Therefore, the usage of Skype has effects on windows registry. This means that its usage have various security limitations on the windows registry.

Skype control mechanisms and encryption are only in a position to protect the communications when the users in communication are using unmodified, Skype produced software over public network. Thus, when the communications transit the other third party systems, which includes servers, modified software, and phone networks, users may experience decreased security and privacy levels. For that reason, Skype usage affects the windows registry and this is what decreases the security and privacy levels.

Furthermore, since it simplifies the transfer of files through allowing the direct file transfer between its clients, P2P file transfer in it is actually a security challenge for the corporate networks. This occurs through the windows registry where the network security infrastructure of a business is possible to be bypassed when using Skype. It is therefore important for an organization to disable the file transfer via GPO Editor or through changing the XML files if it is required(Max 2006) . In this case, file transfers are only enabled by default. This means that by affecting the windows registry, Skype usage affects the corporate network, which is harmful to the operations of an organization. In addition, Skype usage transfers virus to the windows registry because it lacks support for the centralized anti virus scanning.

Windows Registry essentially holds great deal of information concerning the system like the configuration and settings. Skype usage affects the product information and BIOS information. It affects the BIOS version and release date. Therefore, in this case, under the windows registry, the usage of Skype affects the information concerning the product name and that product manufacturer’s name. In addition, the usage of Skype affects the information concerning the user account, which is stored in the registry. For instance, over usage of Skype may affect the information about the list of the user accounts, and reveal their passwords to other users (Heijkoop 2006).

The other effect of Skype usage is that it may lead to a user’s computer or that of his contact to be compromised or hacked. This hacking takes place in the windows registry. Albeit it takes care to defend or protect the communications from the unwanted disclosure, in some instances it is possible for the users’ computers to be hacked or to be compromised by the unauthorized users. It is thus important for an individual when using Skype to choose Skype passwords that are strong and from time to time change them. In addition, when using it on a public or shared computer to always check the “ remember my password” option.

In the modern world, crime level have risen and become more and more sophisticated. The methods used by anti-crime units have also been sharpened to match the intelligence of the criminals of this new world . Over the years , the use of internet based communication methods has become common and widely accepted globally. Most f these communication tools within the internet have a very high level of confidentiality which is backed by the use of firewalls and passwords to prevent unauthorized people from accessing information. However, with the current crime rates and sophistication of crime, the need to retrieve information or evidence from internet-based communication has become necessary. Most crimes nowadays have gone digital. Criminals are using the available technology to their full advantage (Carrier 2005).

The internet has become a very vital forensic and evidence field for forensic experts. Communication between people carries very vital information pertaining to their intentions and plans. Forensic experts have found the internet to be a primary source of forensic information, which can give insights or clues pertaining to thousands of crime that take place very day. Ina recent survey undertaken by scientists from Berkeley has found that more than 90% of information pertaining to communication and chat do not leave the digital sphere.

Most activities in the digital world leave very definite evidence and traces, which allow investigators to extract very vital forensic information, which can be very resourceful in solving criminal cases at the law court or even preventing the occurrence of crime. Digital forensics has become a very important area of study since it has turned out to be a strong forensic tool.

Most intelligence and forensic systems have equipped themselves with adequate resources and computer applications, which are used to retrieve forensic data from the internet- based communication . There, and are many ways for retrieving both criminal and non-criminal digital evidence and information from the internet based communication (Blackledge 2007). Skype is one of the vital communication avenues provided by the internet. Skype provides high levels of security and decentralization of information. Internet based communication techniques may provide minimal or no forensic evidence if proper or robust forensic approach or tools are not used. Modern forensic technology seeks to retrieve information internet based communication where convectional approaches fail. When retrieving forensic date from Skype, it is important to identify the potential sources of forensic information within the communication avenue. Contacts lists and addresses form one of the sources of data on Skype. The call logs provide first hand information of people who were contacted or called through Skype. Voice recordings and audio files in Skype carry a lot of valuable information, which can be of great use to the forensic experts (Carvey 2007). Email attachments, exchanged pictures, cookies, and chat messages exchanged through Skype carry very imperative information that forensic experts can build evidence from.

Of all, data sources the call logs and History files form the wealthiest source of forensic information. Chat and online communications a re usually accompanied with nicknames of other individuals or parties as well as time stamps. This allows forensic experts to determine who the recipient is . The first step in obtaining forensic information in Skype is to identify the exact name and location of the target file. The search for forensic information is worsened by the fact that most windows do not have fixed data locations on the disks. Deleted files are a good source of forensic evidence. A lot of evidence lies within the recycle bin. It actually raises eyebrows why one would delete chat information.

This could be because of obvious reasons that there is something illegal or unscrupulous with the chat file. Information in the recycle bin and deleted files can be combined with information collected from other sources to build on good evidence. Skype shelves or stores the chat logs within the history databases (Carvey 2012). Within these databases, there are chunks of information pertaining to user chats and conversations within the ‘ chat sync’ folder. Although the format of the chat sync folder is not officially known, there are mechanisms available that can be used to retrieve information and files. The most commonly used application to do this is the Belkasoft Evidence Center 2012. This means that forensic information from Skype can be obtained if at all the chatsync file exists.

There are tremendous steps taken to improve Skype to change its features to allow the application to store video recordings of every video conversation. This improvement will see Skype not only becoming a source of evidence but a witness. In one of the BBC articles dated 26 January 2012, by Chris Summers, a woman was charged of killing her child as the father watched . The forensic experts could not trace it on Skype . However, this video, and the case majorly relied on graphical analysis of voice. The Voice over Internet Protocol (VoIP) was however very critical in gathering enough evidence to prosecute the woman. The development of including video features that can allow future retrieval of videos from Skype would be very beneficial to the forensic scientists . (Carrier 2005) This advancement would be monumental in curbing internet –based communication.

Bibliography

Abdulezer, L., Abdulezer, S., Dammond, H., & Zennström, N. (2007). Skype for dummies. Hoboken, N. J: Wiley Pub.

Gough, M. (2006). Skype me!: From single user to small enterprise and beyond. Rockland, Mass: Syngress.

Max, H., & Ray, T. (2006). Skype: The definitive guide. Indianapolis, Ind: Que.

Heijkoop, H., Boel, J., & Ottenhof (Almere). (2006). Skype. Brussel: Easy Computing.

Barreau, M. (2006). Skype. Paris: CampusPress.

Sheppard, A. (2006). The complete idiot's guide to Skype for PCs. New York: Alpha

Shaw, R. (2006). Hacking Skype. Hoboken, N. J: Wiley.

National Research Council (U. S.). (2004). Forensic analysis: Weighing bullet lead evidence. Washington, D. C: National Academies Press.

Carrier, B. (2005). File system forensic analysis. Boston, Mass: Addison-Wesley.

Blackledge, R. D. (2007). Forensic analysis on the cutting edge: New methods for trace evidence analysis. Hoboken, NJ: J. Wiley & Sons.

Carvey, H. A. (2007). Windows forensic analysis: DVD toolkit. Burlington, MA: Syngress Pub.

İşcan, M. Y., & Helmer, R. P. (2003). Forensic analysis of the skull: Craniofacial analysis, reconstruction, and identification. New York, N. Y: Wiley-Liss.

Carvey, H. A., & Kleiman, D. (2007). Perl scripting for Windows security: Live response, forensic analysis, and monitoring. Burlington, Mass: Syngress Pub.

Carvey, H. A., & Kolde, J. (2012). Windows forensic analysis toolkit: Advanced analysis techniques for Windows 7. Amsterdam: Elsevier/Syngress.

Winter, R. (2012). A simple guide to Skype. Carmel, Ind: Luminis Books.