11/1/2018

Application Forensics

Eric Swisher
Vashaad Fincher
Tracey MacLeavy

Application Forensics

Computer Forensics is “the practice of collecting, analyzing and reporting on digital data in a way that is legally admissible” (Forensic Control). Computer forensics can aid in discovering as well as solving crimes. In this paper, we will investigate the forensics of computer applications. The applications focused on are Dropbox, Gigatribe and Skype.

Dropbox is a complicated application due to the fact that it uses cloud computing. This can pose challenges for investigators. Gigatribe is a file sharing network which encrypts the information being sent. This can also make investigating difficult and consequently most investigators go undercover on the application rather than trying to decrypt information.

Skype as an application saves valuable information about users and their interactions on the application. This information is easily accessible however forensic tools such as IEF can help organize the information as well as retrieve deleted information.

Dropbox Forensics

Dropbox is a desktop client like Microsoft SkyDrive or Google Drive that gives access directly to the computer’s hard drive. The program can share files, be used for backups and auto syncs with the other devices that are linked with the Dropbox account. This is like having the same folders on all your computers and mobile devices all at the same time. Dropbox is free or very low cost.

A few challenges become immediately apparent when dealing with the investigation process of Dropbox. This is a system that has access to multiple machines in multiple locations that is accessible anywhere there is an internet connection. Cloud based computing will inadvertently cause problems by splitting data, replicating it and storing it in multiple areas geographically. Data could be stored in pieces in as many data locations there are available for storage. It may be challenging to explain chain of custody for the forensic investigator who must translate and make the data acceptable for use during court proceedings. It is important to know the legalese for obtaining the data in each area that your information is in because violating their laws could mean the end of your investigation for the result of missing data.

In a traditional investigation the professional would seize the machine and make copy of the files, only using the copy to investigate as to not corrupt the chain of custody or data that is associated with the single machine. With Dropbox and other cloud computing storage applications the evidence has no local based equipment and the investigation may require finding artifacts associated with Dropbox storage that may be a clue to the finding the needle in an even bigger stack of needles. Dropbox investigations require legal processes to be followed to preserve evidence and comply with the chain of custody to create evidence that holds up in a courtroom setting. The requirements for the use of cloud-based data is like the requirements of traditional data reports. The Data must be exact and verifiable, the RAM must be IDed and copied in to a virtual environment, proof that the suspect had access to or was the owner of the data with intent of the suspect, also an analysis of the data has been carried out following all rules of evidence and it must be preserved and available by the other legal team. The requirements may appear the same but are much more difficult for the forensic investigator who must do all of the work, when data must be reassembled and verified from sometime thousands

of machines could appear to be an impossible task. Using forensic tools available to us can make this task easier to handle.

One of the first things an investigator will want to do is determine if a cloud-based system was being used or if it has been removed from the device. The investigator may be able to find fragment of information on the system that leads them to believe that It may be Dropbox. This task can be completed by checking the indices created in the installation of the software application, discovering Dropbox info from browser history including the username or e-mails from account creation can also point toward the creation of a Dropbox. When it has been determined that Dropbox was used but is no longer installed on the system then the account may be obtained through the cooperation of Dropbox and their registry of Ip addresses for data transferred on their system. They will keep records of and locate the other machines the suspects device was communicating with.

It is important to ensure that we can reconstruct data that is spread over multiple storage devices while following good chain of custody requirements, there is a challenge to investigators may depend on how much recreation must be done as well as the problems faced from jurisdictions and technical problems. The cooperation with authorities is necessary to rid these impeding problems and implement cyber security disciplines to the evidence so that it may be constructed for presentation. Dropbox is good for storage and if used properly has great advantage but also has the possibility of being exploitable and therefore we must continue to develop means to track and control cloud based computational storage such as Dropbox.

Gigatribe Forensics

Gigatribe is peer-to-peer file sharing network. First developed in France 2005, an American version in November of 2008. The software formerly known as TribalWeb, GigaTribe is designed with a P2P connection the users, any encrypt files can be sent to another peer. GigaTribe P2P allows you to connect with others users that are not on GigaTribe. GigaTribe encrypts all files being sent with 256-bit Blowfish, and all files can be save and encrypted with a password.

GigaTribe is used by criminals to hide incriminating files and helps send encrypting files to others; GigaTribe is perfect for in this case, because it has encrypted all files and the files are not made public. The software is used in by the digital crime investigators to find evidence for cases that the person in question would have used major discretion the evidence. Cases such as cyberbullying/harassment, child pornography, fraud, and even drug trafficking. In these investigations time is of the essence the more the criminals have time the more they to hide the evidence. Gigatribe has become a staple in modern digital criminal investigation,

When investigating into child pornography the investigators use GigaTribe to go undercover. They monitor others public material until they find child pornography being shared publicly. From there the investigators will use the IP address to find the computer address. Then finally search warrant would be obtained to gain access to computer files. To obtain the search warrant to seize the computer; the investigator has examined the network to make sure there is something they are trying hide, such as WEP encryption, two Wi-Fi being present, or intriguing network names (e.g. DON'T_USE_MY_WIFI). These computer files will then be used to investigate the others the criminal is emailing.

In September 2010 an undercover FBI agent was using GigaTribe to investigate user "pedodad36569". The case seemed like a simple case, the user had hundreds of child

pornography images in his shared folder, and a publicly viewable IP address. After obtaining a search warrant, Illinois Internet Crimes Against Children, tried to seize the computer. IICAC found that the IP address lead to wrong address, because the network unsecure accessible by anyone. The FBI had to go back to the drawing board. Not until a year later in did a special agent find a new IP address; that was less than a block away. Then it took a year to obtain a search warrant to investigate the computer. Once the computer was obtaining and the criminal admitted to trading child porn online, the investigator found another user trading with the first criminal. The user was found out to be a former FBI agent. Being a former FBI agent, the digital investigator need to make sure that this was correct. The investigator examined found that the found that the house had two networks being to be accessed. One was WPA2 and the other was an encrypted WEP. The multiple networks made the assumption more corrected (Anderson 2012). Both were found guilty and sentenced to 30 years in prison.

Skype Forensics

Skype is one of the world's most popular social networks. Skype is used for voice or video calls, instant messaging, file transfers and even screen sharing. In 2012, Skype had 45 million users online at the same time (Lunden). Although popularity has significantly declined, it is still in the top 15 most popular social networks. With this being said, there is a high chance that computer crimes occur on this platform.

Computer crimes on Skype include, but are not limited to, harassment or bullying, sharing one's intent, accomplices and victims or even illicit images and IP theft. Proof of these crimes can be recovered from a user's account by a forensic examiner; this would be retrieved

from their calls, messages, group chats, contacts, file transfers, voicemails and sms messages (McQuaid). Most of this information is located in the main.db file. In the same folder as main.db, the chatsync folder provides important evidence. This folder contains the .DAT files which hold conversation details about who the chat was with, who started it, what time and date the messages were sent, status of each message.

Within the main.db file there are several tables for each aspect. The accounts table stores all the information about the user entered when creating the Skype account, including name, birthday gender and other information. This can be used to verify whose account it is as well as to look at recent modifications. The calls table lists each call, the date and time it started, type of call, local user details, remote user details and duration of the call (McQuaid). The contacts table stores details on contacts and any group the user is a part of. The information found here can also be found in the accounts table however this table includes whether a contact has been blocked and the timestamps of users last online time.

The file transfer table stores details about any file that was transferred between two users, such as file name, size, who sent it and the delivery status. This is used for forensic analysis especially in the case that an employee is leaking sensitive information because it is not where someone would think to transfer files, making it a good location to get away with crimes. Skype also stores IP addresses of the user and the outward facing IP address (McQuaid). This is especially important to forensic analysts because they can us the location and timestamp of a user to either find the user or draw relevant conclusions to prove they committed a crime.

Although forensic investigators can look through all these files, the process is tedious. Instead they can use Internet Evidence Finder (IEF) to make their job easier. This tool parses the artifacts found in these files and locations so that the investigator only has to focus on

relevant material and does not waste time searching through hundreds of records. The IEF Report Viewer sorts each artifact by group and lists relevant data. The tool will also convert the timestamps from UNIX time to a format that the investigator will understand. The IEF pulls account details and organizes them in a table and the user can choose the most relevant category. To go a step further, the tool collects all chat information and presents the results to the investigator, which can easily be sorted. IEF also threads chat messages to make the conversation easier to read and can parse IP address details for external IP addresses associated with the computer (McQuaid).

Most importantly, the IEF can find deleted records from memory dumps, unallocated space and other areas. These deleted records contain call data as well as chat message details in case the suspect tries to cover up their tracks by deleting the information. To conclude, Skype is a popular social network that can house important information about computer and non-computer crimes. This information is easily accessible but several tools, such as the IEF, can help make the information more user-friendly to investigators.

Works Cited

(n.d.). Retrieved from https://www-sciencedirect-com.saintleo.idm.oclc.org/science/article/pii/S174228761300011X

"An Introduction to Computer Forensics by Forensic Control." *Forensic Control*, forensiccontrol.com/resources/beginners-guide-computer-forensics/.

Anderson , Nate UTC. "Prosecutors: 'pedodave69' Was Former Top FBI Agent." *Ars Technica*, Ars, 16 May 2012, arstechnica.com/tech-policy/2012/05/prosecutors-pedodave69-was-former-top-fbi-agent/.

"Encrypted File Sharing with Gigatribe." Edited by ETP, *ETP*, Encrypt the Planet, 28 Oct. 2015, encrypt-the-planet.com/encrypted-file-sharing-with-gigatribe/

"Global Social Media Ranking 2018 | Statistic." *Statista*, www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/#0.

Lunden, Ingrid. "Skype Reaches A 45M Concurrent User Peak, And What Looks Like A New Stage Of Momentum." *TechCrunch*, TechCrunch, 14 Oct. 2012, techcrunch.com/2012/10/14/skype-reaches-a-45m-concurrent-user-peak-and-what-looks-like-a-new-stage-of-momentum/.

McQuaid, Jamie. "Skype Forensics: Analyzing Call and Chat Data From Computers and Mobile." *Magnet Forensics*, Magnet Forensics, 2014, https://www.magnetforensics.com/wp-content/uploads/2014/04/Skype-Forensics-Analyzing-Call-and-Chat-Data-From-Computers-and-Mobile-Magnet-Forensics.pdf

"Skype Forensics." *InfoSec Resources*, 25 Jan. 2016, resources.infosecinstitute.com/skype-forensics-2/#gref.