Yahoo! Messenger Forensics on Windows Vista and Windows 7

Matthew Levendoski, Tejashree Datar, and Dr. Marcus Rogers

Center for Education and Research in Information Assurance and Security
Purdue University, West Lafayette, IN, 47906
{mlevendo,tdatar,rogersmk}@purdue.edu

Abstract. The purpose of this study is to identify several areas of forensic interest within the Yahoo! Messenger application, which are of forensic significance. This study focuses on new areas of interest within the file structure of Windows Vista and Windows 7. One of the main issues with this topic is that little research has been previously conducted on the new Windows platforms. Previously conducted research indicates the evidence found on older file structures, such as Windows XP, as well as outdated versions of Yahoo! Messenger. Several differences were found within the Yahoo Messenger's registry keys and directory structure on Windows Vista and Windows 7 as compared to Windows XP.

Keywords: Yahoo Messenger, Instant Messenger Forensics, Windows Vista, Windows 7.

1   Introduction

Yahoo! Messenger (YM), among other forms of online communication, is used extensively by online predators to communicate with other predators, as a means of communication with victims, and also for trading of pictures and videos. Investigators often come across cases involving child pornography. Cases in which YM is specifically used as a medium for gathering images and videos are less frequent. Due to the small number of cases wherein YM is used, for gathering several forms of multimedia, there is a lack of a unified body of knowledge that can aide the investigative process. The Access Data Registry Quick Find Chart [1], with respect to YM, is limited to older versions of YM on Windows XP.

  The purpose of this research is to update the current registry artifacts found within Access Data's Registry Quick Find Chart. Most notably, this paper also pin points the difference in directory structure from Windows XP to that of Windows Vista and Windows 7. Additionally, this research sets out to create a unified source in which investigators can reference when dealing directly with the Yahoo Messenger service.

  The paper documents all the associated findings of these interactions with respect to YM chats, photo sharing, and file transfer. This paper focuses more on the relevance of the sharing and receiving of files and photos as it relates to identifying specific areas where potential evidence of content depicting child pornography may be found.

2   Previous Work

Dickson [2] presents an article with a general focus and overview of several pieces of evidence that can be found within the Yahoo Messenger chat service. The emphasis of the article is to help locate evidence that helps trace contact information about a known suspect and their potential victim. It gives insight into the location of evidence that specifies file transfers, user connections (YPAGER.LOG), chat logs (when enabled), fragments of conversations within the swap file, message fragments in RAM, as well as other directly contacted user's profile pictures (INDEX.INI)[2]. This article gives an insight into a broad range of evidential artifacts that can be sited and analyzed within the Yahoo application.

Wagner [3], in his white paper, writes an overview about Yahoo Messenger photo sharing. This article talks about the "S" folder in brief and also talks about the _m.jpg and _t.jpg file creations in this "S" folder. There is a similar white paper, by an unknown author [4], which also talks about Yahoo Messenger photo sharing with respect to the "S" folder and the _m.jpg and _t.jpg files. These articles gave us a quick perspective of where to start looking for evidence of photos and photo sharing sessions.

Additionally, Dickson's article [2] goes into further detail that will help identify an even more general view into identifying evidence in several case scenarios. But because these articles were written in 2006 and 2007, the studies at hand are outdated and need revision. Not all is lost though, for several core features have always been implemented within the Yahoo application that are still evident today.

3   Yahoo Messenger Overview

Yahoo! Messenger is one of the popular instant messaging clients from Yahoo. YM can be downloaded from http://messenger.yahoo.com/ in which a Yahoo account is needed to log into the service. A Yahoo account can be created by providing one's personal information like name and date of birth then proceed by creating a username and password. Once logged in, users can send instant messages and chat with other Yahoo users in their contact/buddy list. Users can also share photos, send/receive files, video chat, conference, and Internet phone calls along with instant messaging. Once YM is loaded on a machine, it has certain default preferences with respect to chats, archives, messages, privacy and all other general preferences like sounds, alerts, and signing into YM.

By default, all chat messages are archived and saved, but these messages are cleared out once the user signs out of YM. If a user does not log out of YM while closing the application, it is possible to view these archived messages. The user has an option to view and save these messages as a file before logging out of the YM session. A user can also change this default message archive option and opt to either save the messages at all times or to not save the messages at all. If a user decides to save the YM chat session in Windows Vista and Windows 7, by default these conversations are saved in the Documents folder as a text file. The chat messages can

alternatively be saved at any specified location on the computer as per the user's preference. These conversations need to be saved before logging out of the YM application.

4   Methodology

For the purpose of testing YM communication, two virtual machines were created on a Mac Pro environment running OS X 10.5 (Leopard). In each virtual machine Windows Vista Business Edition and Windows 7 Ultimate Edition were installed. These virtual machines were installed using the freely available VirtualBox software. The latest version of Yahoo! Messenger, version 10.0.0.1258 was installed on each of the virtual machines. This YM version was installed without the toolbar, browser, nor the extra options.

Three Yahoo accounts were set up in order to test the messenger. Two of these test accounts were created as potential "Bad guys" or predators, and one account as a potential victim. Several mock interactions were conducted in which chats, file transfers, and photo sharing were initiated. Different scenarios were conducted in which one user initiated photo sharing with another user and one user initiated photo sharing with multiple users simultaneously (for this paper, two users) was also tested. The data and the evidence left behind from these interactions were then tracked using screen shots for each of these interactions, as well as, specific evidential tracking.

5   Data Analysis

The evidence examination was first started by inspecting the registry structure for Windows Vista and Windows 7 using the built in registry editor for Windows. The registry was examined with respect to the YM files. It was found that this registry structure is fairly similar to the YM registry structure for Windows XP found in the Access Data Registry Quick Find Chart [1]. In order to better convey the findings, the registry evidence was placed in a tabular format similar to that of Access Data's chart.

For both Windows Vista and Windows 7, at the following location: \User\Software\Yahoo\Pager, an investigator can expect to find the Yahoo user id of the person using the account, the version of YM installed on the computer, all the revisions made to the YM version, if the save password option is turned on and also if the Auto sign in has been enabled. Windows Vista has an extra feature of P2P count that is not included in Windows 7. P2P count is the number of allowed P2P users who can send large data amongst each other. Please refer to Table 1 for further detail.

For both Windows Vista and Windows 7, information related to chat sessions can be found under the following location: User\Software\Yahoo\Pager\profiles \profile_name\chat, which gives the last selected chat room category, but not necessarily the exact chat room entered. This information can prove useful for investigators to understand the chat room category that the predators potentially use and frequent. Please refer to Table 1 for further detail.

User\Software\Yahoo\Pager\profiles\profile_name\chat\favorite_rooms gives the list of saved favorite rooms for the user. This stands true for both Windows Vista and

Windows 7. This information can be important to understand the different chat rooms that the predator frequents. Please refer to Table 1 for further detail.

For both Windows Vista and Windows 7, User\Software\Yahoo\Pager \profiles\profile_name\FT gives the last saved location of a received file. It also gives the last sent location of a transferred file, that is, the location from where the last sent file was uploaded. This is important data when validating whether a user has been sharing or receiving files. Please refer to Table 1 for further detail.

User\Software\Yahoo\Pager\profiles\profile_name\FriendIcons gives the icon that the user has set for himself/herself that will be displayed to the user's friends. The name of the file used will be visible in the path as well as where it is located on the hard drive. Location of the FriendIcon is essentially the same for Windows Vista and Windows 7. Please refer to Table 1 for further detail.

**Table 1.** Registry evidence within Windows Vista and 7 compared to Windows XP

Yahoo! Registry at a Glance for Windows Vista and 7

| File	Location	Description	XP[1]	Vista	Windows 7
HKEY_C URRENT _USER	\Software\Yah oo\Pager\	Gives User ID	Yahoo! User ID	Yahoo! User ID	Yahoo! User ID
		Gives the installed version	N/A	Version	Version
		Gives the version revisions	N/A	VersionRev	VersionRev
		Shows if the password is saved	Save Password	Save Password	Save Password
		Shows if auto sign in is turned on or off	N/A	Auto Login	Auto Login
		Number of P2P users	N/A	P2P count	N/A
HKEY_C URRENT _USER	\Software\Yah oo\pager\profil es\screenname\ Chat	Gives the last selected chat room category	Chat (Rooms visited or created)	Chat	Chat
HKEY_C URRENT _USER	\Software\Yah oo\pager\profil es\screenname\ Chat\Favorite Rooms	Gives the list of saved favorite rooms for the user	N/A	Favorite Rooms	Favorite Rooms
HKEY_C URRENT _USER	\Software\Yah oo\Pager\profil es\screenname\ FT	Location of last received file and last sent transferred file	File Transfer	FT	FT
HKEY_C URRENT _USER	Software\Yaho o\Pager\profile s\screenname\ FriendIcons	Location of user icon displayed to friends	N/A	FriendIcons	FriendIcons

5.1   Photo Sharing: Creation of the "S" Folder

Whenever a photo sharing session is initiated in Yahoo Messenger from a Vista machine, a photo sharing folder starting with the letter "S" is created in the Program Data folder. Additionally, randomly assigned numbers and alphanumeric characters are appended to the end of the naming structure. The path for the created "S" folder is as follows: C:\ProgramData\Yahoo!\Messenger\PhotoSharing\Sc8b0. The "S" folder is not created immediately when the user initiates the photo sharing session. Once the session is initiated, as soon as the other yahoo user accepts the photo sharing invite, the "S" folder is created in the PhotoSharing folder on the initiator's side. The "S" folder, in itself, is empty until a picture is shared. As soon as an image is shared (sent), a thumbs file '_t.jpg' is created followed by the image file '_m.jpg'. The name of this file appears to be a randomly assigned series of alphanumeric characters. For the purpose of this paper, the Windows Vista machine was used for initiating the photo sharing on Yahoo Messenger. The user sent the pictures from the Windows Vista machine to the user on the Windows 7 machine.

Figure 1 and Figure 2 below; illustrate the creation of the "S" folder for the Windows Vista machine. Figure 1 is an image of the "S" folder being created after a photo sharing session was initiated by the user on the Windows Vista machine. Figure 2 is an image of the "S" folder on Windows Vista when a photo was shared by the user on that machine. It can be seen that two files are created in the folder one after another simultaneously. One file is labeled '_t.jpg' and the other file is '_m.jpg', respectively. These two files indicate that the photo was sent by the user on the Vista machine. The name of the file is randomly generated alphanumeric characters and is different than the actual file name that was shared from that machine.
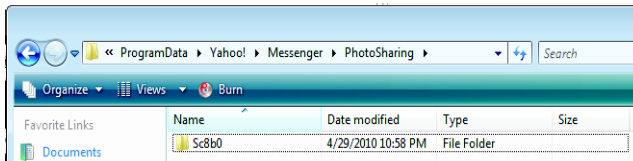
Fig. 1. Creation of "S" folder for Vista
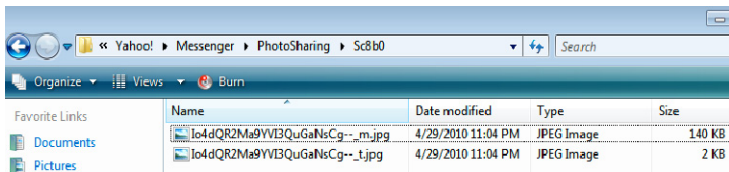
Fig. 2. "S" Folder when an image is shared from the Vista machine

Figure 3 is an image of the same "S" folder on Vista when a photo was shared by another user. It can be seen that only one file '_m.jpg' is created in the same "S" folder. The absence of the '_t.jpg' file indicates that the file was received by the user. The addition of the new files to the same "S" folder indicates that the photo sharing session that was initiated earlier is still being continued between the same two users.
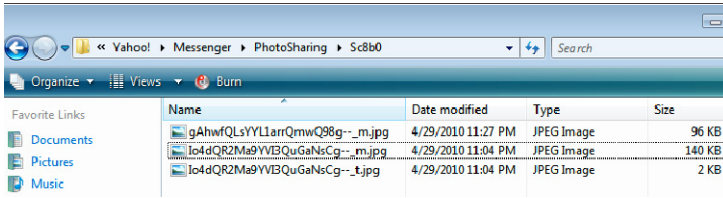
Fig. 3. "S" folder after an image is received

For the purpose of this paper, a photo sharing session was initiated by the user on Windows Vista machine with the user on the Windows 7 machine. On Windows 7, the "S" folder is created in the Program Data folder, similar to that of Windows Vista. The path for the "S" folder is: C:\ProgramData\Yahoo!\Messenger\PhotoSharing \S0e4e. The "S" folder is created as soon as a file is shared with this machine. The creation of "S" folder for Windows 7 is illustrated in Figure 4. The folder contains the received file. This file is of the '_m.jpg' naming convention. The name of the file is alphanumeric and is randomly generated. The name of the image in the "S" folder is not consistent with that on the sent machine. If Windows 7 is used to initiate photo sharing, the "S" folder creation will follow the same procedure as Windows Vista.
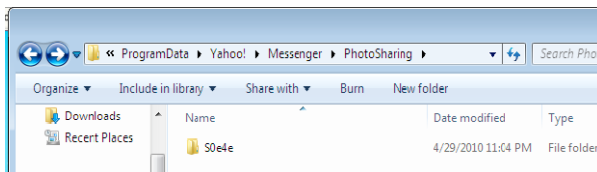

Fig. 4. "S" folder creation for Windows 7

If a user has multiple chat sessions and photo sharing sessions open simultaneously with different users, a different "S" folder is created for each chat session. This holds true for both Windows Vista and Windows 7. As soon as a new photo-sharing request is accepted, another "S" folder is created in the PhotoSharing folder. The folder stays empty until the images are shared. A file with the extension '_m.jpg' is created once an image is received or two files with extensions '_t.jpg' and '_m.jpg' each are created if the image is sent by the user.
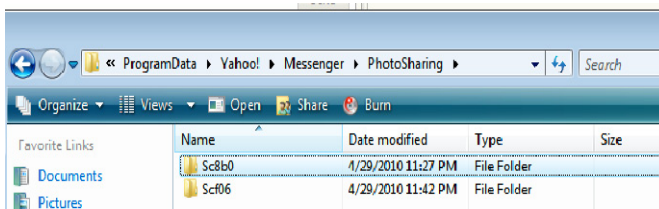

Fig. 5. "S" folders for multiple photo sharing sessions

Figure 5 shows two "S" folders present in the PhotoSharing folder under ProgramData. This is due to the fact that the user has multiple photo-sharing sessions open with in multiple chats at the same time. Unfortunately, the individual "S" folder does not specify which chat buddy the user was sharing photos with.

5.2   File Transfer

There are two ways of sharing a photo in Yahoo Messenger. One is via Yahoo Photo Sharing and the other is via the file transfer option. The "S" folder creation is applicable only for the photo sharing and does not apply to file transfer. If the user wishes to save the photos via Photo Sharing, the default folder where these pictures will be saved is in the 'Picture' folder. The 'Picture' folder is a shortcut located under 'Libraries'. The full path is 'C:\Users\UserName\Pictures'. The user can in turn save the photos to any location they desired on the computer.

The file transfer option can be used to transfer all kinds of media such as, photos, documents, or music. The default location while saving a file during a file transfer is "Documents". The Documents folder is a shortcut located under 'Libraries'. The full path is 'C:\Users\UserName\Documents'. But, if the user wishes to, the file can be saved anywhere on the computer. The default file name is same as the original file. The date-time stamp of the saved file is that of the local machine when the file was saved.

6   Summary and Future Work

It can be seen that Yahoo has changed the file directories slightly with the new file structure implemented in Windows Vista and Windows 7 as compared to Windows XP. One of the major changes from Windows XP to Windows Vista and Windows 7 is the new file path 'ProgramData', which is actually a hidden folder in the C:// drive. This new directory is now the location for the YM PhotoSharing folder. Investigators can expect to find important information in the Yahoo file directories with respect to photo sharing and file transfers. Chat message archives can be found on the machine if the user did not log out of YM and the ongoing conversations before closing the YM application. Investigators can also expect to find out shared and received photos in the "S" folder. Even though the "S" does not indicate with which user the photos were shared with, it is possible to find more information regarding users by comparing the date-time stamps of the "S" folder and the archived chat files.

Additionally, work needs to be done to improve the current research at hand. One addition is to possibly locate the IP addresses of YM buddies who have been in contact with a user on either a Windows Vista or Windows 7 machine. Other evidential paths and case by case scenarios have also been submitted for further research. These additions combined with this paper have been expressed to be of utmost importance by local and state police and have proven to be useful at several levels of investigations dealing with child pornography cases in which the Yahoo! Messenger has been utilized.

References

1. AccessData: Registry Quick Find Chart (2005)
2. Dickson, M.: An examination into Yahoo Messenger 7.0 contact identification: Digital Investigation, vol. 3, pp. 159–165. Elsevier (2006)
3. Wagner, Lt. (Ret.) S.: PhotoSharing Folder – Yahoo Messenger. In: Encase Message Boards (2007)
4. Unknown: Yahoo! Messenger Photo Sharing (n.d.)