The Forensic Recovery of Instant Messages from

MSN Messenger and Windows Live Messenger

MSN Messenger

MSN Messenger and its later incarnation Windows Live Messenger are one of many Instant Messenger programs. Their primary use is to communicate in real time with known contacts by typing messages and sending them to each other.

One of the most frequent requests to a forensic investigator is for any evidence of “chat logs” or any instant messaging conversations.

The purpose of this paper is to assist the forensic examiner to investigate all possible opportunities to recover evidence of instant message conversations from MSN Messenger and Windows Live Messenger.

The very fact that there have been a dozen or more main versions of MSN Messenger, since MSN Messenger 1 in 1999, mean that this paper is not version specific. It is meant as a starting point for anyone seeking evidence of a conversation in MSN Messenger and Windows Live Messenger, which will both be referred to as simply Messenger. Unless otherwise stated research has been conducted using MSNM 7.5 in WXPP SP2.

Background basics to Messenger

To access the messaging service the user must have a Microsoft .Net Passport.

The Microsoft Passport Network is an online service that lets you use a single e-mail address and password to sign in to any Passport-participating website or service. A Passport account allows Messenger to identify you and retrieve your settings no matter where you access the Internet.

It is possible to use any email address when signing up for a Microsoft Passport, it is not necessary to have a Microsoft related email address like somebody@msn.com.

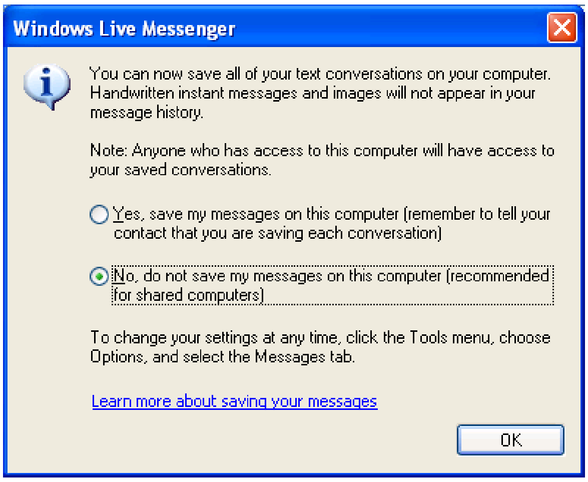
Although when signing up for a Passport it states that you must verify your address to use the service it is possible to send and receive instant messages having signed on with a totally fictitious email address. (11/01/06)

Where an address is not verified it is identified as such during any instant messaging conversations.

Saved Conversations

The best record of conversations is found in saved conversations. Unfortunately the saving of conversations by a user is not on by default. When a user takes part in their first instant message conversation, at the end of their conversation they are prompted by a dialog box with two radio button options.

The user can either NOT save conversations or save conversations. The default, as recommended by the dialog box is NOT to save conversations. (Figure 1)



Windows Live Messenger

You can now save all of your text conversations on your computer. Handwritten instant messages and images will not appear in your message history.

Note: Anyone who has access to this computer will have access to your saved conversations.

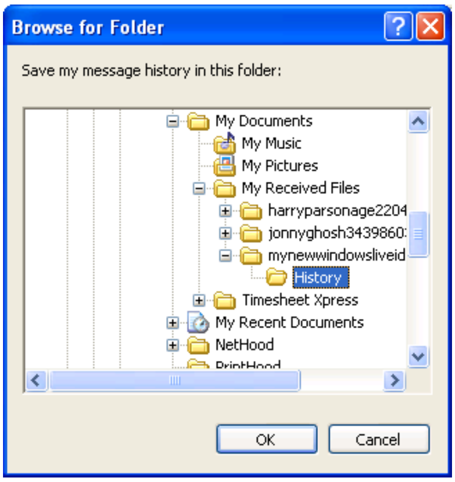
○ Yes, save my messages on this computer (remember to tell your contact that you are saving each conversation)

● No, do not save my messages on this computer (recommended for shared computers)

To change your settings at any time, click the Tools menu, choose Options, and select the Messages tab.

Learn more about saving your messages

Figure 1



Browse for Folder

Save my message history in this folder:

Figure 2

If the user has chosen not to take the recommended option all subsequent conversations, with any contact, are then saved. The option can be changed at a later date through the Messenger Tools\Options dialog. The default folder for the location of the saved messages (Figure 2) is the users *My Documents**My Received Files**PassportName############**History*. Where PassportName is the part of the users Passport email address before the @ sign followed by a series of numbers ############ allocated by the Messenger program. The numbers are created from the full Passport address which is passed through a simple algorithm. A simple program to convert the Passport address to the number is available for download. (1)

The message logs are saved in the xml file format. The filename takes the same form as the folder name PassportName############ except that the PassportName (and related ############) is the Passport name of the remote user with whom the conversation took place.

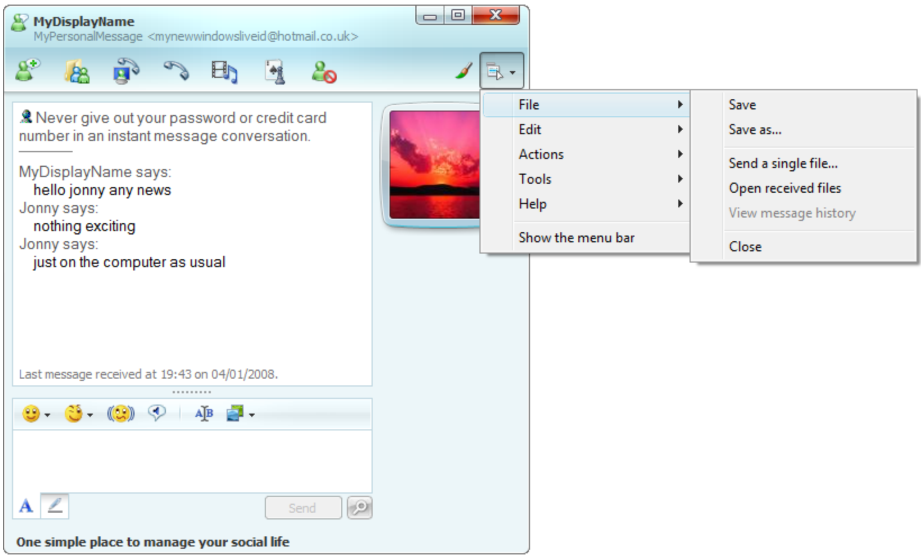
Conversations in subsequent sessions are appended to previous conversations and are stored in the one file. If the xml file is extracted from the case, in order to view the conversation the style sheet *MessageLog.xsl* which is found in the History folder with the xml file should be extracted to the same folder so the xml file will display properly in a web browser.

The possibility exists that the messages have been saved in a folder other than the default, moved or copied, so a simple way to identify them is to filter by file extension - xml.

Other Saved Conversations

As well as setting conversations to be saved from the options in the main Messenger program it is also possible to save individual conversations from the chat window (Figure 3).

Messages saved this way will default to rtf file format (Figure 4).



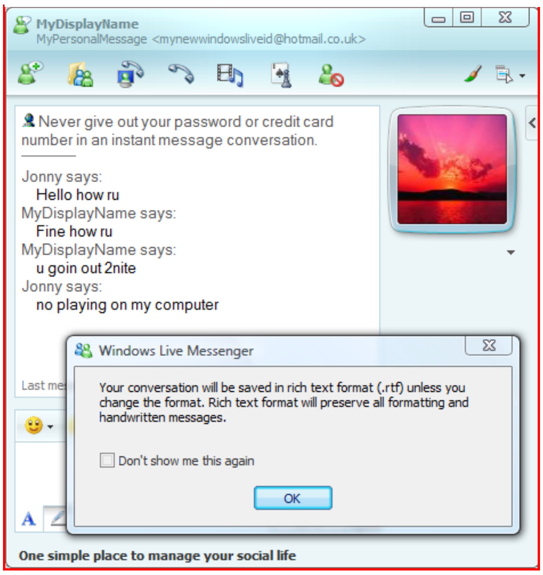
MyDisplayName
MyPersonalMessage <mynewwindowsliveid@hotmail.co.uk>

Never give out your password or credit card number in an instant message conversation.

MyDisplayName says:
hello jonny any news
Jonny says:
nothing exciting
Jonny says:
just on the computer as usual

Last message received at 19:43 on 04/01/2008.

Figure 3



MyDisplayName
MyPersonalMessage <mynewwindowsliveid@hotmail.co.uk>

Never give out your password or credit card number in an instant message conversation.

Jonny says:
Hello how ru
MyDisplayName says:
Fine how ru
MyDisplayName says:
u goin out 2nite
Jonny says:
no playing on my computer

Windows Live Messenger

Your conversation will be saved in rich text format (.rtf) unless you change the format. Rich text format will preserve all formatting and handwritten messages.

□ Don't show me this again

Figure 4

After confirming the message the standard Save As dialog opens and the conversation can be saved at any location with a file name of the user's choice (no default name is offered).

The user also has the options to Save As Type rtf (default), text, Unicode text.

So the examiner can look for these files by filtering on file extension rtf and txt.

Messenger Plus!

Messenger Plus! by Patchou is a commonly used extension to Messenger and if this is being used (*C:\Program Files\Messenger Plus! Live*) the chat logs are saved by default in -

My Documents\My Chat Logs\MonthName YearNumber,

e.g. *My Documents\My Chat Logs\September 2007*.

The saving of conversations is set on by default if Messenger Plus! is used.

The logs can be saved as *remoteparticipantsemailaddress.txt* or .html or .ple encrypted logs. These formats have changed over the years and depend very much on the version of Plus!, the current default (Jan 2008) is html.

Artefacts from Saved Conversations

In the event that saved conversations are not found, the next step is to consider that conversations might previously have been saved but deleted and search for any traces of those.

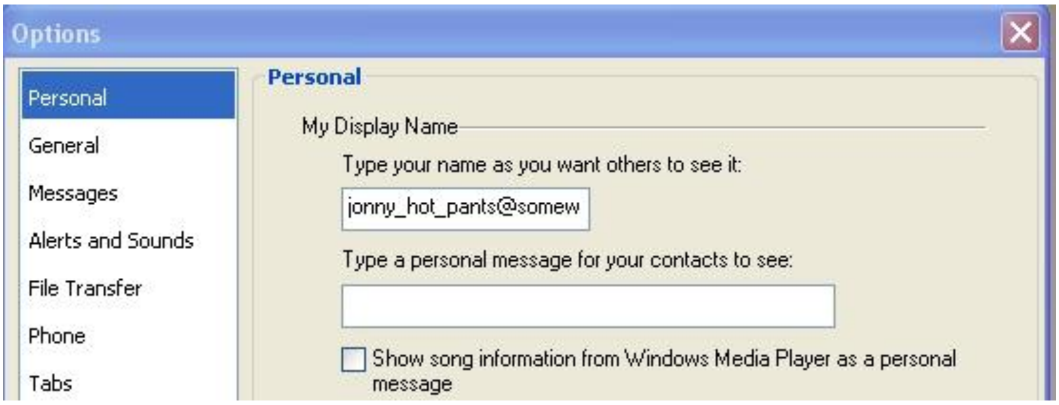
The xml message logs take the following format

```
xml version="1.0"?> <?xml-stylesheet type='text/xsl' href='MessageLog.xsl'?> <Log
FirstSessionID="1" LastSessionID="1"><Message Date="20/01/2006" Time="18:36:33"
DateTime="2006-01-20T18:36:33.281Z" SessionID="1"><From><User
FriendlyName="jonny_hot_pants@somewhere.com"/></From><To><User FriendlyName="Hi 2
Ya"/></To><Text Style="font-family:MS Shell Dlg; color:#000000; ">hello
h</Text></Message><Message Date="20/01/2006" Time="18:36:42" DateTime="2006-01-
20T18:36:42.750Z" SessionID="1"><From><User FriendlyName="Hi 2 Ya"/></From><To><User
FriendlyName="jonny_hot_pants@somewhere.com"/></To><Text Style="font-family:MS Shell Dlg;
color:#000000; ">how ru</Text></Message></Log
```

Any of the xml tags could be used to search for artefacts of saved logs. For example, individual messages are delimited by *<Message> </Message>*, so a potential search term to identify the start of any messages could be *<Message Date="*.

If the investigator is using Encase then it is possible to use the File Finder Module in the Enscript Case Processor (as it is named in V6). A custom search could be defined with the header *<Message Date="* and the footer *"</Message>*.

The investigator could use other search strings based on known information. A search based on the FriendlyName is one possibility. Note that in the example message log above the FriendlyName of the host user contains an email address, this is unusual and is because that user has not edited his personal setting *My Display Name* in the Tools\Options dialog (Figure 5). It is not unusual for Messenger users to change their Display Name on a regular basis. If the Display Name is known it is likely to be a good search term for chat artefacts. The Display Name is the text that is shown in the



My Display Name

Type your name as you want others to see it: jonny_hot_pants@somew

Type a personal message for your contacts to see:

□ Show song information from Windows Media Player as a personal message

Figure 5

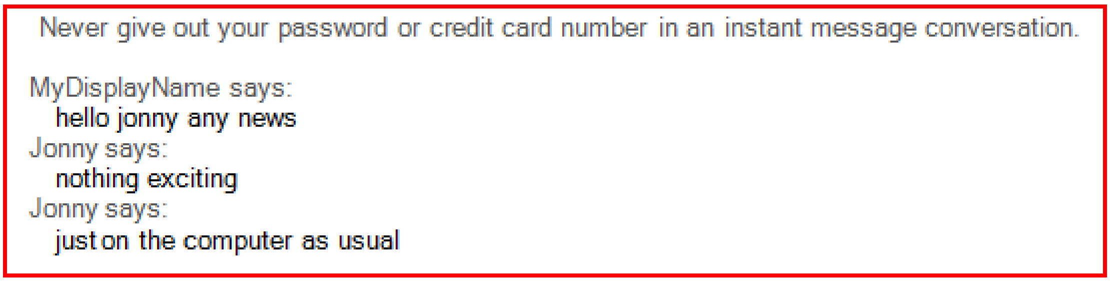
message log as FriendlyName.

Near the start of the message log there is an entry –

FirstSessionID="1" LastSessionID="1"

As the user conducts different sessions of conversations with the other participant the SessionID is incremented and the LastSessionID is updated. The SessionID for any one session is included within each message. It is not clear what constitutes a single session as examinations show that sessions can on occasions be just a few seconds apart.

If the chat logs had been saved from the chat log window as rtf or txt files an option is to search for the Display Name and email address if they are known, or indeed the text of the standard warning at the head of each chat (Figure 6).



Never give out your password or credit card number in an instant message conversation.

MyDisplayName says:
  hello jonny any news
Jonny says:
  nothing exciting
Jonny says:
  just on the computer as usual

Figure 6

Alternatively if the participants are not known then the most obvious search term is

says:

which in the case of rtf files this can be improved to

says:\par

(this includes the paragraph-end formatting marker)

Or for txt files, if the search is done in hex, a space can be added before **says:** and a carriage return and line feed after, i.e. 20 73 61 79 73 3A 0D 0A.

If Messenger Plus! has been used and the logs have been saved in the default mode they will be html and each session of conversation starts in the form –

<div class="mplsession" id="Session_2008-01-05T11-38-05">

So a reasonable search term could be –

id="Session_

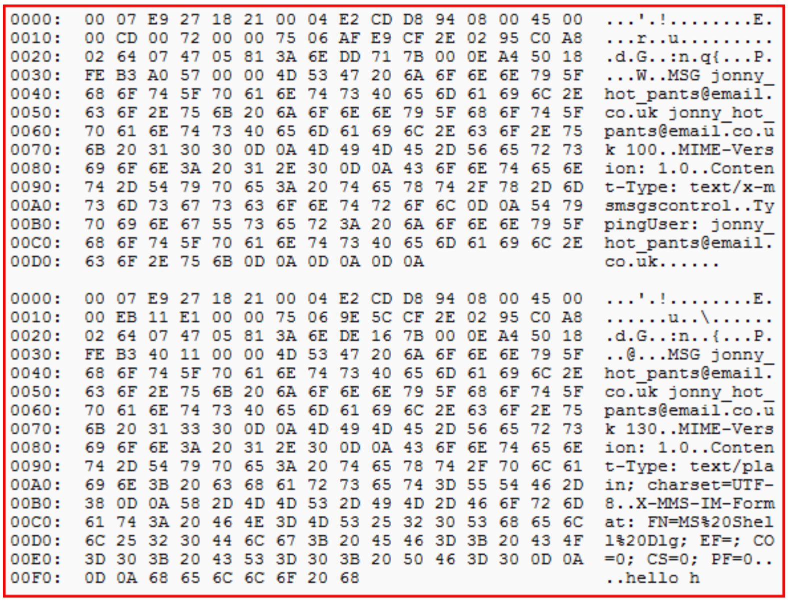
Note that the word **says** does not appear in these Messenger Plus! html logs.

Artefacts from connection logging

On a rare occasion when the user has enabled connection logging, or where it might have been a beta version when it was set by default, it may be possible to find the log. If this is the case search for a file named MsnMsgr.txt, usually found in the folder C:\Documents and Settings\UserName\My Documents\My Received Files. This file contains detailed debugging information captured whilst Messenger is running. It also captures the detail of conversations and participants, but it is obscured somewhat, simply by the volume of other information captured in the log.

Artefacts from Messenger Protocol

MSN Messenger uses the Mobile Status Notification Protocol (MSNP) for communications. The protocol was originally published in draft by Microsoft in 1999, but a completed version has never since been published. The protocol has been updated often since then and for MSN Messenger v 7.5 the protocol was MSNP12. As the protocol is unpublished by Microsoft any information on has come from individual research and a number of sites have published some details (2). It is easy enough for an examiner to carry out their own research by capturing packets during a Messenger session.



```
0000:  00 07 E9 27 18 21 00 04 E2 CD D8 94 08 00 45 00  ...'.!........E.
0010:  00 CD 00 72 00 00 75 06 AF E9 CF 2E 02 95 C0 A8  ...r..u.........
0020:  02 64 07 47 05 81 3A 6E DD 71 7B 00 0E A4 50 18  .d.G..:n.q{...P.
0030:  FE B3 A0 57 00 00 4D 53 47 20 6A 6F 6E 6E 79 5F  ...W..MSG jonny_
0040:  68 6F 74 5F 70 61 6E 74 73 40 65 6D 61 69 6C 2E  hot_pants@email.
0050:  63 6F 2E 75 6B 20 6A 6F 6E 6E 79 5F 68 6F 74 5F  co.uk jonny_hot_
0060:  70 61 6E 74 73 40 65 6D 61 69 6C 2E 63 6F 2E 75  pants@email.co.u
0070:  6B 20 31 30 30 0D 0A 4D 49 4D 45 2D 56 65 72 73  k 100..MIME-Vers
0080:  69 6F 6E 3A 20 31 2E 30 0D 0A 43 6F 6E 74 65 6E  ion: 1.0..Conten
0090:  74 2D 54 79 70 65 3A 20 74 65 78 74 2F 78 2D 6D  t-Type: text/x-m
00A0:  73 6D 73 67 73 63 6F 6E 74 72 6F 6C 0D 0A 54 79  smsgscontrol..Ty
00B0:  70 69 6E 67 55 73 65 72 3A 20 6A 6F 6E 6E 79 5F  pingUser: jonny_
00C0:  68 6F 74 5F 70 61 6E 74 73 40 65 6D 61 69 6C 2E  hot_pants@email.
00D0:  63 6F 2E 75 6B 0D 0A 0D 0A 0D 0A                 co.uk......

0000:  00 07 E9 27 18 21 00 04 E2 CD D8 94 08 00 45 00  ...'.!........E.
0010:  00 EB 11 E1 00 00 75 06 9E 5C CF 2E 02 95 C0 A8  ......u..\......
0020:  02 64 07 47 05 81 3A 6E DE 16 7B 00 0E A4 50 18  .d.G..:n..{...P.
0030:  FE B3 40 11 00 00 4D 53 47 20 6A 6F 6E 6E 79 5F  ..@...MSG jonny_
0040:  68 6F 74 5F 70 61 6E 74 73 40 65 6D 61 69 6C 2E  hot_pants@email.
0050:  63 6F 2E 75 6B 20 6A 6F 6E 6E 79 5F 68 6F 74 5F  co.uk jonny_hot_
0060:  70 61 6E 74 73 40 65 6D 61 69 6C 2E 63 6F 2E 75  pants@email.co.u
0070:  6B 20 31 33 30 0D 0A 4D 49 4D 45 2D 56 65 72 73  k 130..MIME-Vers
0080:  69 6F 6E 3A 20 31 2E 30 0D 0A 43 6F 6E 74 65 6E  ion: 1.0..Conten
0090:  74 2D 54 79 70 65 3A 20 74 65 78 74 2F 70 6C 61  t-Type: text/pla
00A0:  69 6E 3B 20 63 68 61 72 73 65 74 3D 55 54 46 2D  in; charset=UTF-
00B0:  38 0D 0A 58 2D 4D 4D 53 2D 49 4D 2D 46 6F 72 6D  8..X-MMS-IM-Form
00C0:  61 74 3A 20 46 4E 3D 4D 53 25 32 30 53 68 65 6C  at: FN=MS%20Shel
00D0:  6C 25 32 30 44 6C 67 3B 20 45 46 3D 3B 20 43 4F  l%20Dlg; EF=; CO
00E0:  3D 30 3B 20 43 53 3D 30 3B 20 50 46 3D 30 0D 0A  =0; CS=0; PF=0..
00F0:  0D 0A 68 65 6C 6C 6F 20 68                       ..hello h
```

Figure 7

The MSN protocol uses commands which are three letters in length. For example during the sending of a text message the command is MSG. Anyone that has used Messenger will have noticed that as the other party is typing a message to you, you are notified of this in the Messenger window. It appears that each individual message comprises a MSG command telling the other party that a message is being typed, followed by a second MSG command with the message itself. The text of the message (Figure 7) was simply "hello h".

It has been found in a recent case, where searches for fragments of chat in unallocated space were required, that the search string

; PF=

(that is semi-colon followed by one space, then **PF**, followed by an equal sign)

was most successful and had very few false hits. This defines the pitch and formatting of the message and is almost without exception the last of the message formatting parameters before the message itself.

Based upon the search string "; PF=" an Enscript is available to extract hits and bookmark them (1).

Artefacts of Conversations from MSN Protocol - gateway files

It is also possible to find artefacts from the MSN protocol in the Temporary Internet Files in files named in the form –

gateway[1].32125 (file extension is variable number of digits)

and also reported elsewhere (3),

gateway.dll?SessionID=12345678.1234

gateway.dll?Action=poll&SessionID=12345678.1234

These gateway files contain MSN protocol packets and can contain any commands but that does include MSG packets carrying a message.

Filtering on filename “gateway” is a reasonable method for identifying such files. If the **; PF=** search string is used artefacts of conversations from these files will be picked up by that.

These files are not commonly observed and it appears that they are only present when a particular port is not available on the user's computer.

Web Messenger

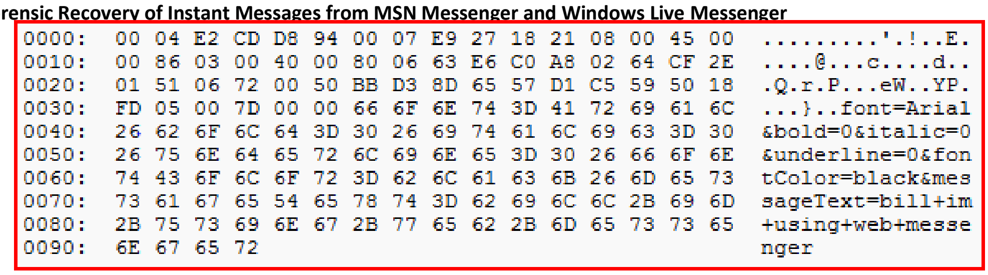
If the steps so far have failed to reveal any evidence consider the possibility that Web Messenger has been used and this will have left different artefacts. Examination of the Internet History is likely to reveal the use of Web Messenger.

The Web Messenger site explains the difference between the two thus -

"MSN Messenger is a fully featured instant messaging program that you install on your own computer or one you have permission to install on. MSN Web Messenger enables you to quickly and easily use basic instant messaging features on a web browser on any computer without installing any software."

Web Messenger uses HTTP protocol and the data is in the form of html and java script.

Scraps of messages might be easily identified if the following examples are typical (Figure 8 & 9), as some good search strings are available. Here the text of the message was "bill im using web messenger" which is preceded by the string **&messageText=**.

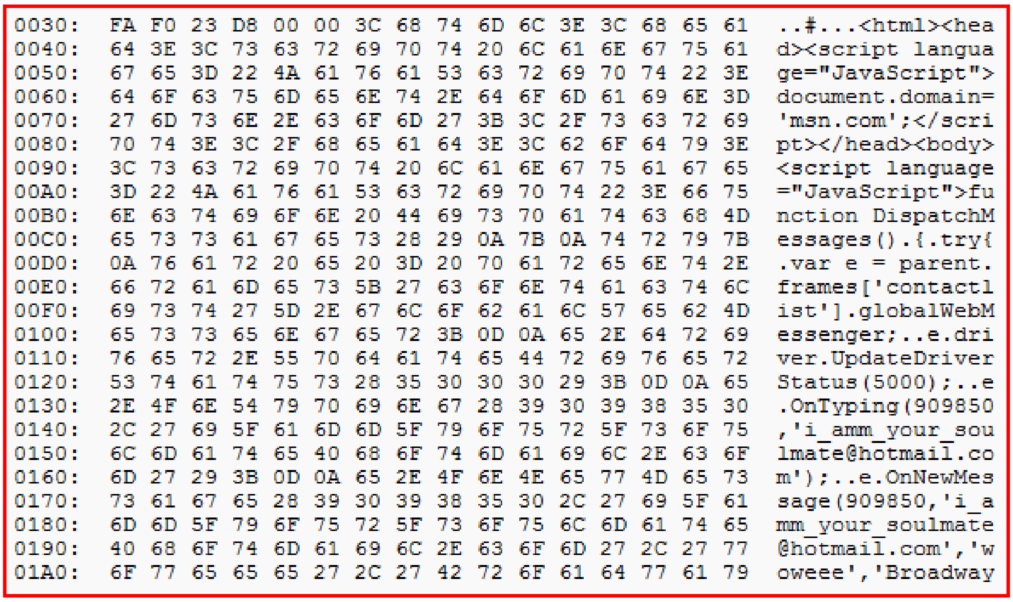


```
0000:  00 04 E2 CD D8 94 00 07 E9 27 18 21 08 00 45 00  .........'.!..E.
0010:  00 86 03 00 40 00 80 06 63 E6 C0 A8 02 64 CF 2E  ....@...c....d..
0020:  01 51 06 72 00 50 BB D3 8D 65 57 D1 C5 59 50 18  .Q.r.P...eW..YP.
0030:  FD 05 00 7D 00 00 66 6F 6E 74 3D 41 72 69 61 6C  ...}..font=Arial
0040:  26 62 6F 6C 64 3D 30 26 69 74 61 6C 69 63 3D 30  &bold=0&italic=0
0050:  26 75 6E 64 65 72 6C 69 6E 65 3D 30 26 66 6F 6E  &underline=0&fon
0060:  74 43 6F 6C 6F 72 3D 62 6C 61 63 6B 26 6D 65 73  tColor=black&mes
0070:  73 61 67 65 54 65 78 74 3D 62 69 6C 6C 2B 69 6D  sageText=bill+im
0080:  2B 75 73 69 6E 67 2B 77 65 62 2B 6D 65 73 73 65  +using+web+messe
0090:  6E 67 65 72                                      nger
```

Figure 8

The reply seems to take a slightly different format, although in this case the person replying was using the standard Messenger program and not Web Messenger, tests show that the reply format is actually the same for both communication methods.

The email address of the person replying can be seen "i_amm_your_soulmate@hotmail.com" (Figure 9) in the format OnTyping/emailaddress/OnNewMessage/emailaddress followed by the content of the message "woweee". This seems to be similar to the earlier capture from Messenger (Figure 7) where TypingUser was followed by MSG and the message.



```
0030:  FA F0 23 D8 00 00 3C 68 74 6D 6C 3E 3C 68 65 61  ..#...<html><hea
0040:  64 3E 3C 73 63 72 69 70 74 20 6C 61 6E 67 75 61  d><script langua
0050:  67 65 3D 22 4A 61 76 61 53 63 72 69 70 74 22 3E  ge="JavaScript">
0060:  64 6F 63 75 6D 65 6E 74 2E 64 6F 6D 61 69 6E 3D  document.domain=
0070:  27 6D 73 6E 2E 63 6F 6D 27 3B 3C 2F 73 63 72 69  'msn.com';</scri
0080:  70 74 3E 3C 2F 68 65 61 64 3E 3C 62 6F 64 79 3E  pt></head><body>
0090:  3C 73 63 72 69 70 74 20 6C 61 6E 67 75 61 67 65  <script language
00A0:  3D 22 4A 61 76 61 53 63 72 69 70 74 22 3E 66 75  ="JavaScript">fu
00B0:  6E 63 74 69 6F 6E 20 44 69 73 70 61 74 63 68 4D  nction DispatchM
00C0:  65 73 73 61 67 65 73 28 29 0A 7B 0A 74 72 79 7B  essages().{.try{
00D0:  0A 76 61 72 20 65 20 3D 20 70 61 72 65 6E 74 2E  .var e = parent.
00E0:  66 72 61 6D 65 73 5B 27 63 6F 6E 74 61 63 74 6C  frames['contactl
00F0:  69 73 74 27 5D 2E 67 6C 6F 62 61 6C 57 65 62 4D  ist'].globalWebM
0100:  65 73 73 65 6E 67 65 72 3B 0D 0A 65 2E 64 72 69  essenger;..e.dri
0110:  76 65 72 2E 55 70 64 61 74 65 44 72 69 76 65 72  ver.UpdateDriver
0120:  53 74 61 74 75 73 28 35 30 30 30 29 3B 0D 0A 65  Status(5000);..e
0130:  2E 4F 6E 54 79 70 69 6E 67 28 39 30 39 38 35 30  .OnTyping(909850
0140:  2C 27 69 5F 61 6D 6D 5F 79 6F 75 72 5F 73 6F 75  ,'i_amm_your_sou
0150:  6C 6D 61 74 65 40 68 6F 74 6D 61 69 6C 2E 63 6F  lmate@hotmail.co
0160:  6D 27 29 3B 0D 0A 65 2E 4F 6E 4E 65 77 4D 65 73  m');..e.OnNewMes
0170:  73 61 67 65 28 39 30 39 38 35 30 2C 27 69 5F 61  sage(909850,'i_a
0180:  6D 6D 5F 79 6F 75 72 5F 73 6F 75 6C 6D 61 74 65  mm_your_soulmate
0190:  40 68 6F 74 6D 61 69 6C 2E 63 6F 6D 27 2C 27 77  @hotmail.com','w
01A0:  6F 77 65 65 65 27 2C 27 42 72 6F 61 64 77 61 79  oweee','Broadway
```

Figure 9

Other Options

In the event that no evidence has been found from the methods above, and it is believed that the user has been taking part in messenger conversations, consider the use of a Messenger clone (e.g. Jan 2008 – Spark, Miranda, Trillian), or one of many other web based Messenger services (e.g. Jan 2008 – iloveim.com, ebuddy.com, imhaha.com, koolim.com, meebo.com).

It would not be too difficult to research what artefacts are produced using these alternatives to Messenger.

Research Methods

What has become a standard research tool for forensic examiners, Filemon and Regmon, have been used to conduct research. These have now been combined into the new Process Monitor. (4)

Packet capture has been done with Packetyzer. (5)

The MSNPiki is a useful unofficial provider of MSN Protocol documentation. (2)

Anyone experimenting with Messenger , should go into the Messenger Tools/ Options/ Connection/ Connection Settings/ Advanced Settings/ Messenger Settings – Connection Logging, and check the option to "save a log of my server connections to help troubleshoot connection problems". This will save a very detailed debug log in C:\Documents and Settings\UserProfileName\My Documents\My Received Files\MsnMsgr.txt. This together with Process Monitor, Internet History and packet capture will provide useful information on which to base research.

Summary

So to summarise, the following method will identify any Messenger conversations or artefacts from conversations.

1) Check known default paths for saved conversations in each user's profile -

My Documents\My Received Files\PassportName############\History

My Documents\My Chat Logs\MonthName YearNumber

2) Filter on file extension xml, rtf, and txt to check if any conversations have been saved in locations other than the defaults.

3) Search for the connection logging file MsnMsgr.txt.

4) Search for any files named gateway in the Temporary Internet Files.

5) Use search strings to identify whether there are any artefacts from MSN conversations.

If no saved logs have been found then it would be prudent to use the search terms across the whole of the physical drive in order to identify any files that might have been missed, otherwise search any allocated areas plus any memory/dump type files (pagefile, hiberfil, *.chk and *.dmp).

For artefacts of saved xml conversations -

User FriendlyName="

(that is the word **User** followed by one space, then **FriendlyName** followed by an equal sign and a double quote all without any spaces)

For artefacts of saved rtf and txt conversations,

says:

(or its refined versions detailed earlier)

For artefacts from MSN protocol

; PF=

If Web Messenger is suspected

&messageText=

If Messenger Plus! is in use

id="Session_

The author welcomes any comments or further information regarding the contents of this document to digitalforensics at parsonage dot co dot uk.

References

1. **Parsonage, Harry.** *Computer Forensics Miscellany.* [Online] January 2008. http://computerforensics.parsonage.co.uk.

2. MSNPiki. [Online] http://msnpiki.msnfanatic.com/index.php/Main_Page.

3. *Forensic artefacts left by Windows Live Messenger 8.0.* **Dongen, Wouter S. van.** 2, s.l. : Elsevier - Digital Investigation, 2007, Vol. 4. ISSN 1742-2876.

4. Windows Sysinternals. [Online] http://technet.microsoft.com/en-gb/sysinternals/default.aspx.

5. Packetyzer. [Online] http://www.paglo.com/opensource/packetyzer.