Forensic Investigation for Instant Messenger:

Evidence Extraction Tools and Techniques

Barry Lun

a thesis submitted to the graduate faculty of design and creative technologies
Auckland University of Technology
in partial fulfilment of the
requirements for the degree of
Master of Forensic Information Technology

School of Computing and Mathematical Sciences

Auckland, New Zealand
2012

Declaration

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the qualification of any other degree or diploma of a University or other institution of higher learning, except where due acknowledgement is made in the acknowledgements.

....

Signature

Acknowledgements

I would like to extend my sincere thanks and gratitude to the following individuals who have contributed towards the completion of my master's thesis:

Million thanks to my primary supervisors, Petteri Kaskenpalo and Dr Brian Cusack, for introducing information technology forensic to me since my study in graduate diploma and throughout my master course. They have given me an excellent foundation to set my study into the right direction. If it wasn't for your encouragement, your patience and your tolerance over the last two years, I would have missed out such a fantastic opportunity to enter master degree. Your appearance has positively changed my life and there is never a suitable word to express how much I appreciate in your help.

I am deeply indebted to Dr Brian Cusack for founding the MFIT course in AUT who made it possible for me to participate in the course. You have not just introduced me to the knowledge of computer forensic but also aid me to improve both my presentation and technical writing skill. Without you organising the MFIT computer lab, I wouldn't have such an enjoyable study environment.

I also would like to extend my gratitude to the awesome students and staff members who provided their time and energy to assist me during my study.

I would like to acknowledge the charitable support of Auckland University of Technology for providing me the good education and the great study environment.

I would like to thank forensic software vendor Belkasoft for their sponsorship on the Evidence Center 2012 license. Without their support, my research would be much difficult to process.

Thanks also to my family. Thank you for all the support in many practical ways during my study.

Lastly I would like to thanks my friend Wing Yee Lo. She has been helping me by reviewing separate drafts that I have written and assist me to conduct my experiments. I was unlikely to take on the extra workload without her.

Abstract

Currently instant messaging is one of the most popular ways for people to interact with each other's over the cyber space.

Due to its popularity, user-friendliness, rich functionality and the ability to conceal identity of the user, instant messenger is often found to be used as a communication tool to conduct sinister and illegal activity.

Law enforcement agency may find traces of illegal activity by extracting information hidden beneath instant messenger.

However collecting digital evidence from instant messenger can present some challenges. Existing forensic guides such as the forensic handbooks published by United State Department of Justice does not offer a comprehensive solution and procedure to counter the increasing problems arise from instant messaging investigation.

Without the proper tools and technique, information stored in the instant messenger might not be thoroughly extracted, integrity of the digital evidence can be affected and in worse scenario, evidence might be lost.

In order to efficiently collect digital evidence from instant messenger, my research has reviewed techniques and forensic tools designed by different developers that featured to extract information from instant messenger.

After careful consideration based on several criteria, Evidence Center Pro developed by Belkasoft was selected to perform further simulation to extract information from Window Live Messenger 2011.

My approach has been implemented and comprehensively tested. The result illustrated that the approach presented in my thesis are able to extract information from instant messenger in a more efficient manner in compare to the traditional approaches.

.

Table of Contents

Chapter 1 – Introduction

Chapter 2 – Literature Review

Chapter 3 – Research Methodology

Chapter 4 – Research Findings

Chapter 5 – Research Discussion

Chapter 6 – Conclusion

List of Tables

List of Figures

Abbreviations

AOL:	America Online
AIM:	AOL Instant Messenger
AUT:	Auckland University of Technology
CMD:	Command prompt
CTSS:	Compatible Time-Sharing System
Dr:	Doctor
FTK:	Forensic Toolkit
GB:	Gigabyte
GPG:	GNU Privacy Guard)
HTTP:	Hypertext Transfer Protocol
ID:	Identification
IM:	Instant Messaging
IP:	Internet Protocol
ISP:	Internet Service Provider
MAC:	Media Access Control
MB:	Megabyte
MFIT:	Master of Forensic Information Technology
MIT:	Massachusetts Institute of Technology
MS:	Microsoft
MSN:	Microsoft Network
NCJRS:	National Criminal Justice Reference Service
OS:	Operating System
PGP:	Pretty Good Privacy
RAM:	Random Access Memory
U.S:	United State of America
VM:	Virtual Machine
WLM:	Window Live Messenger

Chapter One

INTRODUCTION

1.0 INTRODUCTION

Instant messaging (IM) is one of the most popular digital communication technology and have been widely used across the cyber-world in the form of instant messenger programs. Traditionally the tool was designed to transfer text messages only but over the last decade, it has been enhanced with additional features such as voice/video message, file transfer and links to public networks such as Facebook. Previous studies have shown that this technology has been directly and indirectly involved in criminal activities. Hence, there is always a need to gather digital evidence from instant messaging. However are the current forensic techniques and tools adequate? The purpose of this research is to review the current literature and then to test one IM in the laboratory to authenticate advocated processes and to make recommendations for best practices.

According to the forensic handbooks that have published between 2007 to 2008 by the United States Department of Justice, there seems to be a lack of information for forensic analyst to understand the processes and techniques required for evidence acquisition from instant messenger under various scenarios such as investigation on volatile instant messenger (a web based IM). The advice is generic and disproportionally small compared to other devices. Many cases and studies (these will be presented in chapter 2) show the involvement of instant messenger in criminal activity.

Thus, the research presents different techniques that might apply on extracting information from instant messenger under different scenarios and a current knowledge base for IM forensic investigation. Chapter 1 is structured to define the problem, discuss the motivation for this research, to summarise the findings, and to elaborate the overall structure of the thesis.

1.1 PROBLEM

The traditional investigation method of IM has been described in the "Investigations Involving the Internet and Computer Networks" handbook published by the U.S Department of Justice. The handbook has covered basic instructions on the procedures to gather digital information from IM. The scenario given in the handbook assumed that the digital device was turned on and instant messaging activities can be observed from the screen when the investigator arrived at the scene. In such scenario, the investigator may easily gather information directly from the instant messenger program and chat window to collect direct evidence such as the content of the conversation, user status and friend list. However these procedures were non-technical and additional techniques are required to obtain digital evidence from different scenarios. The handbook itself has specifically stated that additional expertise may be needed for a more detailed investigation.

It is essential to specify and establish the research scope and focus in order to create research that is educational, professional, informative and meaningful. Instant messenger is a popular digital communication tool that is potential to be used to conduct illegal operation. According to Kiley (2008), volatile instant messenger presents challenge to the digital forensic expert due to the usability scope compared to traditional instant messenger (non web based). The traditional evidence acquisition techniques and procedures might not be effective and applicable on volatile instant messenger.

The scope scaled to be in keeping with the problem is hence concentrated onto techniques that can possibly overcome the challenges in evidence acquisition from different scenario where evidence acquisition is usually not too straight forward. The techniques include examination of unallocated storage space, live memory dump and network evidence acquisition can be considered. The work can be developed into a system to be used later to enhance instant messenger investigation procedures. Some examples of traditional instant messenger include: MSN, AIM. Examples of volatile instant messenger include: Meebo, Facebook chat, MSN (browser version).

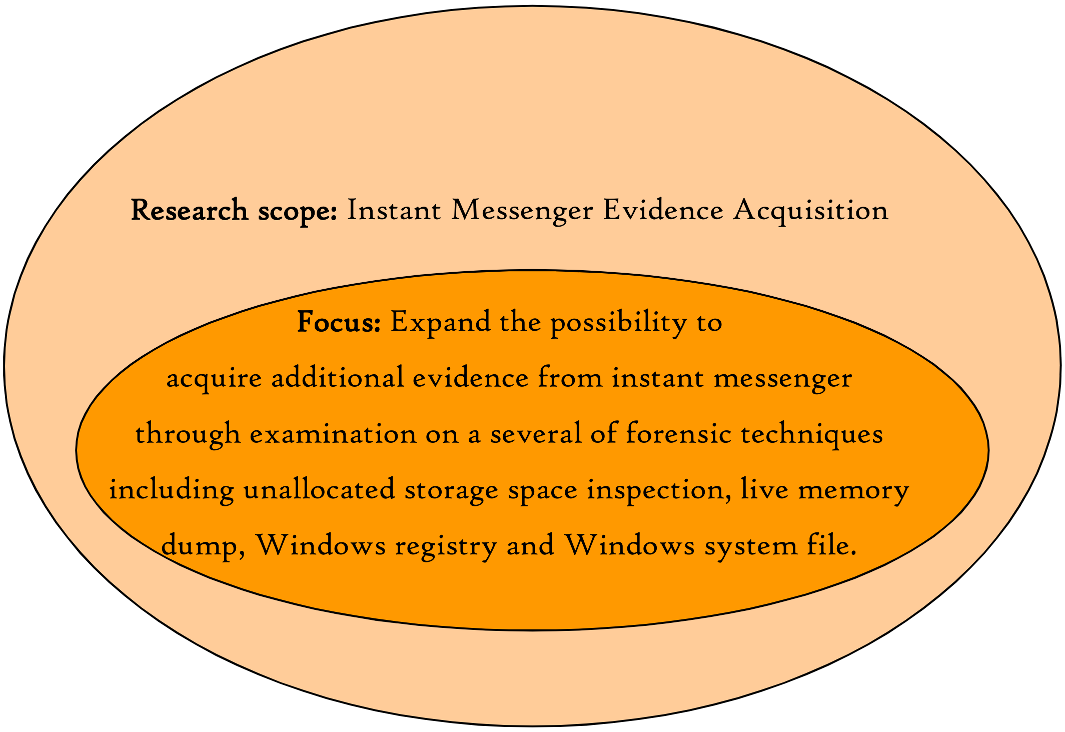

Research scope: Instant Messenger Evidence Acquisition
Focus: Expand the possibility to acquire additional evidence from instant messenger through examination on a several of forensic techniques including unallocated storage space inspection, live memory dump, Windows registry and Windows system file.

Figure.1.1 Research scope and focus

The objective of this research is to examine the strength of various forensic techniques and out of-the-shelf forensic tool and study how the they can be useful in the process to recover evidence from various scenarios.

Additionally, opening questions which need to be addressed and studied in this study are as follow:

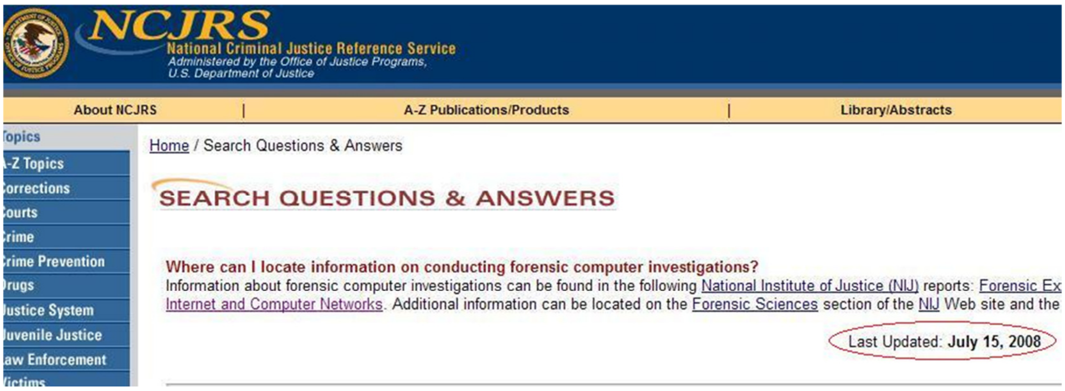
Can later forensic tool and technique add value to the traditional approach in evidence acquisition from instant messaging?

1.2 MOTIVATION OF THE RESEARCH

During the paper studies for this degree I read a set of handbooks that were published in between 2007 to 2008 by the United State Department of Justice provided. A portion in the handbooks indentified the process, collection and seizure of potential evidence from a forensic investigation involving instant messaging. The concept and the potential for miss-use of the technology grew in my imagination. A further literature search showed that there were few other resources that detailed instant messaging investigations, the tools and techniques.

The guides provided the foundation and generic guidance for doing IM investigations. However investigations involving internet are always complicate and very often a successful investigation requires experience knowledge beyond the generic guides. For example, the guide has recommended to leave the computer power on and look for personnel who have experience and training to capture the data from the conversation on screen (Hagy, 2008). Such procedure leaves a time gap for an after-seizure communications and a potential of tampering of evidence in custody (Turnbull & Slay, 2007). An Investigator usually does not have the choice of waiting around for other people to be found and chancing on someone else to have the skills. Also a lack of forensic understanding and blindly following the instruction given by the guides could lead to loss of evidence. Techniques such as evidence collection from live memory have not been detailed in these guides. The live acquisition technique would enable the collection from IM other evidence such as conversation history, timestamp, screen name from the random access memory, and scenarios where someone has turned the instant messenger off or closed the conversation window (Gao & Cao, 2010). Apart from the typical conversation log showing on screen, and possible chat log saved on the logical drive, evidence of conversation could also be found in unallocated hard disk space and the temporary internet file folder (Kiley, Dankner, & Rogers, 2008).

Given the pace of change in the IT industry, to develop and maintain a procedural guide is never easy (Turnbull & Slay, 2007). Continuous and rapid updating is required to maintain the effectiveness on these guides. The guides provided from National Criminal Justice Reference Service on forensic computer investigations was last updated on 15th July, 2008 (figure 1) and have not been updated for over two years.


NCJRS
National Criminal Justice Reference Service
Administered by the Office of Justice Programs,
U.S. Department of Justice
About NCJRS
A-Z Publications/Products
Library/Abstracts
opics
-Z Topics
orrections
ourts
rime
rime Prevention
rugs
ustice System
uvenile Justice
aw Enforcement
ictims

Home / Search Questions & Answers

SEARCH QUESTIONS & ANSWERS

Where can I locate information on conducting forensic computer investigations?

Information about forensic computer investigations can be found in the following National Institute of Justice (NIJ) reports: Forensic Ex Internet and Computer Networks. Additional information can be located on the Forensic Sciences section of the NIJ Web site and the

Last Updated: July 15, 2008

Figure 1.2 The NCJRS forensic computer investigation guide update

Recent studies have proposed several advanced techniques to search for evidence from unallocated space and live memory. Gao and Cao (2010) has proposed a method of memory forensic in regards to the very popular Chinese instant messenger QQ. Kiley, Dankner, & Rogers (2008) has also presented the possibility to search for evidence in unallocated space. It should be noted that these methods might not be valid for all types of instant messengers and are bound to several constraints depends on the circumstances of the investigation. A variety of evidence are available from a client-based instant messenger including chat logs, file transfers and registry configuration (Kiley et al., 2008). However, with the complexity of evidence acquisition from instant messaging, it can be challenging to gather evidence with the standard instant messenger investigation procedure listed in the forensic guide due to the fact that evidence might lie in area that require special extraction technique. As a result, the gaps in the literature and my reading have left a distinct impression that knowledge in this area is currently incomplete. I am motivated to look further into the area of "*Evidence Acquisition from instant messenger*".

1.3 FINDINGS OF THE RESEARCH

Thus, the research presents different techniques that might apply for extracting evidence from instant messenger and the result can add to the knowledge base for the instant messenger forensic investigations and provide additional knowledge for forensic investigator when attempt to acquire evidence from an instant messenger.

The research experiment consist of selecting an off the self forensic tool designed to carry out forensic examination on instant messaging. In my case, Evidence Center developed by Belkasoft was selected and tested to extract evidence from an IM. Based on the result of my experiment, it was able to simplify the processes in digital evidence extraction for the areas of:

- Messenger history profile
- Allocated disk space
- Unallocated disk space
- RAM
- Pagefile
- Hibernation file

It could potentially retrieve digital evidence from Pagefile however nothing was found in pagefile during my experiment which could be due to the usage of pagefile was subjective. Generally the computer system will only store information in pagefile when RAM is insufficient and the experiment was not designed to particularly trigger that element.

The current version of Belkasoft Evidence Center was able to store the digital evidence extracted from instant messenger in a database for further analysis and it was able to provide useful function such as keyword search to aid an investigation. Based on the literature research, an instant messenger could leave a trace in Window Registry, however the tool did not provide the function to capture information from the registry. Another off the shelf application was required to capture the image of the hard drive and perform memory dump from the RAM before Belkasoft Evidence Center could analyse the data.

The experiment showed that the tool did not provide the function to extract the following type of digital evidence:

- Indication of picture sharing
- Content of the picture shared
- Content of video call
- Content of voice message

The finding indicated that the forensic tool in the experiment was able to aid the forensic examiner to extract digital evidence from instant messenger but it was not comprehensive enough at its current form. Forensic examiners could not rely on one tool during an investigation.

The tool had proven to greatly simplify the processes of evidence extraction. However there are many variables that lie in the process of instant messenger forensic examination. Therefore a comprehensive knowledge of forensic techniques was still essential in order to carry out an investigation. The tool was not powerful enough to allow general enforcement agents to extract digital evidence from instant messenger without the supervision from an expert.

1.4 STRUCTURE OF THE THESIS

Chapter 1 provides a brief overview and summary of the completed project. Chapter 2 summarises the literature reviewed and identifies researchable problems that arise from gaps and logical contradictions in the literature read. Chapter 3 then proceeds to specify a research method that is in keeping with the problem that is selected as being feasible to research. The research question is selected and suitable hypotheses asserted. The data collection, processing and analysis methods are also specified. In Chapter 4 the findings are reported. In Chapter 5 the research question is answered and then discussed with respect to the wider issue of guideline currency and relevancy to professional practice. Advice is provided for assessing guidelines. Chapter 6 concludes the thesis by summarising the outcomes and making recommendations for further research. The references used and appendix for data are the last two chapters.

Chapter Two

LITERATURE REVIEW

2.0 INTRODUCTION

The focus of this research is evidence extraction from Instant Messenger applications (IM). The literature has been selected by key word searching on three library data bases. In particular literature that provides technical guidance to professionals has been selected so the principle concern of best practice could be evaluated.

One of the concerns with the current state of guidance for doing digital evidence extraction from IM is the generality of the statements found in the selected literature. In section 2.1 the IM system is defined. In section 2.2 techniques for evidence extraction from IM are discussed. In section 2.3 the tools that can be used for evidence extraction are reviewed. In section 2.4 investigation procedures are summarised and documented. In section 2.5 the preceding sections are evaluated to identify issues and problems that have potential for research.

2.1 IM SYSTEM

What is instant messaging? The elderly generation might not have a clue, while the younger generation should be familiar with using the artefact, but many might not understand how to define an instant messaging system. The forensic guide published by United State Department of Justice describe Instant messaging as a software that allows users connected to a network (generally the Internet) to send messages to each other (Hagy, 2007b). In detail, IM is software written in computer code. The application allows two electronic devices to send text messages to each others in real time (Network Dictionary, 2011).

Van Vleck (2012) reported that the first form of computer instant messaging appeared in the 1960s. During that time, the technology was called Compatible Time-Sharing System (CTSS) and was developed in the MIT (Massachusetts Institute of Technology) Computation Center. The system allowed users to send simple text messages to another user with a simple *MAIL* command which is the fundamental form of electronic communication. By 1965, there were hundreds of users using the CTSS system to communicate daily. The system was later developed into email and text messaging and the two system has been widely use in electronic communication in into the present.

Followed by the success of CTSS, Van Vleck and his colleague Noel Morris started their implementation of text messaging in 1965. The concept was to add more features to CTSS such as the *.WRITE* feature which was an additional to the original CTSS *.SAVED* feature. The *.SAVED* feature allows user to the sending of a message to another user logged in to the terminal. The feature was limited to sending a one line message during the time period. The *.WRITE* feature carried a buffer-sharing code and was able to display on the receiver's terminal when the user on the other end resumed the terminal session. This turned out to be the prototype of instant messaging. Since then the communication tools have gone through many incremental developments to become of the form in the present age (Vleck, 2012).

Apart from the basic text messaging, instant messengers nowadays are generally equipped with multiple features such as friend list, video call, voice call, file transfer or sharing (Chiu, Wu, Tut, Lin, & Yuan, 2007) and the ability to connect to social networks such as Facebook (Microsoft, 2012). Some well known messenger such as AOL, MSN Messenger and Yahoo Messenger carry large volumes of traffic daily (Chiu et al., 2007). The IM application has been developed to be used on other electronic device such as the Smartphone and computer tablet (Microsoft, 2012) to enhance mobility and was no longer bound to workstations. It allows the users of IM to communicate between different platforms.

In recent years, a new form of volatile based instant messenger also known as web-based instant messenger has become increasingly popular (Kiley, Dankner, & Rogers, 2008). The new type of instant messenger carries similar functionality as the traditional instant messenger but it does not require any form of installation on the hosting platform (Kiley et al., 2008). As stated by Matthew Kiley, Shira Dankner and Marcus Rogers (2008), the new form of instant messenger can be easily accessed with a web browser and does not leave much information on the hosting platform unlike the traditional instant messenger. Some of the web-based instant messenger such as Meebo was equipped with powerful ability to connect to different instant messenger carriers simultaneously (Meebo, 2012).

According to a patent document published in 2007 (Belkasoft, 2012a). The basic instant messaging system should include a message receiver, message sender, a display device for displaying messages, a natural language processor that can determine the meaning of the message to some extend by analysing the natural language used, and an animation controller than change the aspect of the appearance of display device. The instant messaging system diagram is shown in figure 2.2.0.

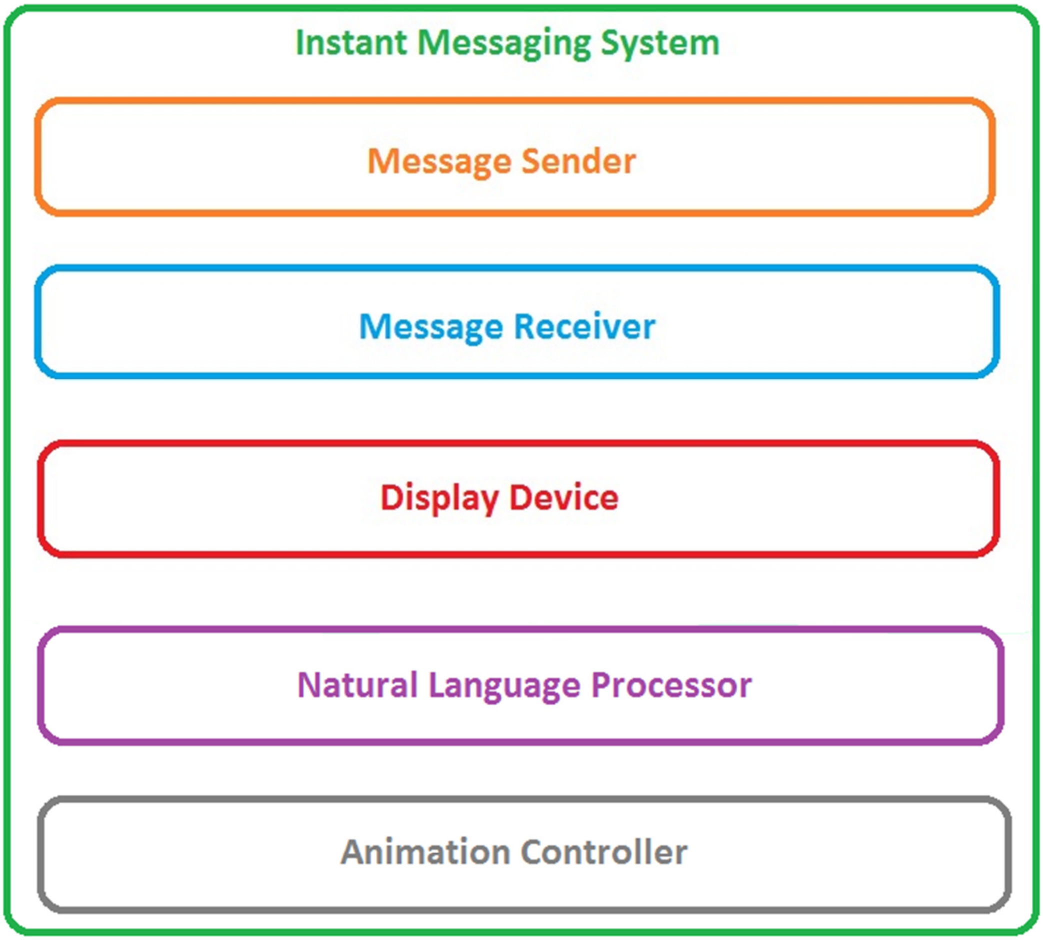


Figure 2.2.0: Basic instant messaging system.

There were several types of instant messaging systems. The first type consisted of a centralised network with a messaging server cluster, upon receiving the message from the sender, the messaging server will route the message through the network until the recipient received the message. Such a system generally stores information such as user names, password and friend list in the server. The second type only uses the server to track if users are online. Once the server determines who has logged in. The users can then send message directly between each other and the server does not hold information transferred between users.

The third type was a hybrid method between the two methods mentioned above, where the server holds the connection information of users and their contact list, the system then checks for users if they have logged in to the system and informs other users of the information.

2.2 IM EVIDENCE EXTRACTION TOOLS

Tools selection requirements and criteria are driven by the objective of the investigation and the applicability of new tools and techniques to digital evidence extraction from an IM. From the requirement, the main criteria were divided into four main categories:

Functionality;
Processing time;
Skill level required; and,
Cost of the project.

Furthermore priorities can be set for acquisition of evidence based on the risk or volatility of the evidence. For example,

Live memory investigation
Unallocated space search
IM Sniper
MSN Shadow
Belkasoft Evidence Center

Chat sniper is an IM forensic analysis tool developed by Alex Barnett (2006), a Master of Science in Cyber Forensics student in Purdue University. Its primary functions included:

Search for Chat log
Collect Usernames
Generate Buddy lists
Retrieve image file transferred over messenger

While every extraction function can be done manually by a forensic investigator, the application is aimed to simplify the process and shorten the time of evidence acquisition from instant messenger. Currently it only works for AIM, Yahoo instant messenger and MSN (Live) that installed in window operating system under English regional settings. The application is capable to run from a removable device such as a memory stick and the cost of a perpetual license is $50USD. The cost covers email support and software update.

Chat Examiner is a forensic application focused on auto chat log searching for a wide range of messengers included ICQ, Yahoo, MSN, Trillian, Skype, Hello and Miranda. The application is developed by Paraben Corporation, a firm that specialized in developing forensic software since 1999. Other than the chat examiner, the company also provides products to support other IT forensic investigation areas such as mobile forensic and hard drive forensics The cost of the licence is $99USD and it only runs on window system.

The chat examiner was in-used in the current industry and is recommended by experts. Some questions remain open with regard to capabilities. Is the Chat Examiner able to search deleted or renamed chat logs? The description of the chat examiner stated that AIM does not leave any chatlog or traditional data stores, however there is another application called a Chat Sniper (http://www.alexbarnett.com/chatsniper.htm) that claims to recover chatlog of AIM, is this correct? How does the software ensure the files integrity of the data source? Will it function with a web-based messenger such as Yahoo live? If it cannot function with web-based messenger, what other product or development can handle web-based messenger?

Under the description of chat examiner, it stated that AOL Instant Messenger (AIM) does not save a chat logs therefore it is not covered by chat examiner. However Chat sniper has offered the function to search for the chat log for AIM. Further research is required for to establish the justification and potential capabilities.

Belkasoft Evidence Center is an off-the-shelf forensic tool that provided the functions to support forensic exanimation of instant messaging. It was advertised as easy to use without training required and it was being used by well-known organization across the industry such as Deloitte, FBI, PricewaterhouseCoopers, U.S. Army, U.S. Secret Service, New Zealand Police

E-Crime Lab in Auckland and New Zealand Department of Internal Affairs, Censorship Compliance Unit (Belkasoft, 2012a). According to information listed in Belkasoft website, the Evidence Center offer support to over 40 different instant messengers. The primary functions included retrieval of historical data from regular history, deleted data and live memory for many popular instant messengers such as AIM, ICQ7 and Microsoft live messenger (Belkasoft, 2012b). According to description, it was able to extract messages, invitations and invitation responses, participants and dates from **Regular history of Microsoft live messenger.** Messages, participants and can be extracted through its carving function, sender and messages are extracted from **live memory.**

2.3 IM EVIDENCE EXTRACTION TECHNIQUES

In the handbook 'Investigative uses of technology: devices, tools, and techniques' published by U.S. Department of Justice. It stated that an instant messenger can possibly link to evidence such as:

Possible point of origin and that could be suspect's physical location;

Provide hint of suspect's true identity through screen name or conversation;

Transactional information related to the internet connection;

Direct evidence to the crime such as an incriminating conversation; and,

Other related information of suspect such as bank account number or email address.

The principle areas for evidence stored on the hard drive by the IM can be summarised as: Information stored on a hard drive by the system; Information stored in the memory; and, Information stored in the network. "Some IM services have the ability to log information on the user's hard drive" (Hagy, 2007a).The NIJ guide has given examples for how to search for the chatlog file that could contain conversation history between user of the IM and another party on the other end of the wire. However the guide did not provide comprehensive information on other files such as login history stored on the hard drive that could contain key evidence.

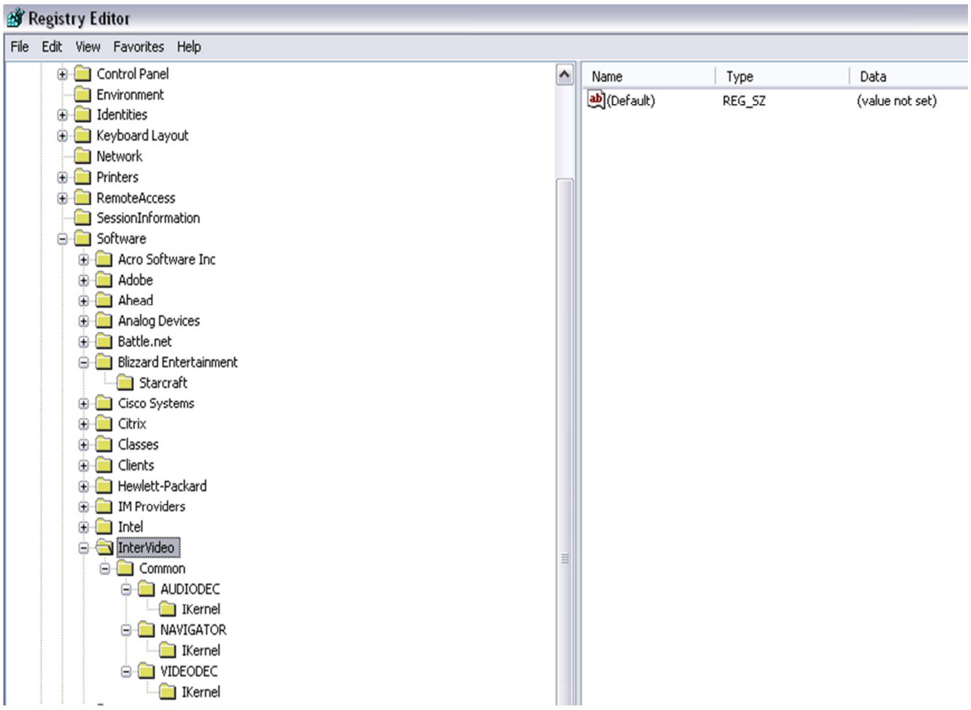
If a computer in the scene is left powered on with instant messenger showing in the screen then it is recommended not to disconnect the power immediately (Hagy, 2008). To use an IM, an account must be established to create a screen name provided with user information. Some instant messenger providers might assist the investigation with information of the account owner (Hagy, 2007a). Evidence can be found in various internet file caches used by Internet Explorer for volatile IM and each cache holds different pieces of data (Kiley et al., 2008). Research done by Wouter S. van Dongen in the Netherlands on evidence files left behind by windows live messenger 8.0 (Dongen, 2007) demonstrates where to locate evidence. The examination was carried out in a Microsoft Window XP environment using instant messenger 8.0. Files such as the AppEvent.evt (Dongen, 2007) were found to have been automatically generated by the messenger and saved on the user's hard drive. The AppEvent.evt file contained information on each successful login and logout from the messenger. Records were used to provide information on the period a user was connected to the messenger and viewed by users on the contact list. The name of files and location on the hard drive vary with different messengers.

Apart from the normal files, files left by instant messenger on a hard drive can be in temp file format and will generally be deleted could be very difficult to retrieve once the machine is power down. In the example of window live messenger 8.0, some files such as the record of contact was saved under '~<name of contact>.tmp' and could be deleted once the system is shut down or logged off. Encrypted files are also relevant. IMs such as window live messenger 8.0 allows the user to encrypt saved contact files (Dongen, 2007). It is an option for the user and often set as default. Additional application such as Forensic Box (Dongen, 2007) are required to decrypt the content of these files. Unintentionally/Intentionally deleted file are also available. An instant messenger such as AIM will automatically deleted old temp files (Reust, 2006). For example when a new buddy list is created, the previous file that contains the buddy list record will be deleted. Files that have been deleted are often left in the unallocated space of a hard drive and can be retrieve by additional application such as EnCase.

Files may be located in different folders. In some systems such as window live messenger 8.0, evidence files might not be saved only within the folder where the messenger is installed. They could spread across different folders. In the research done by Dongen (Dongen, 2007), it shows that a set of files containing MSN protocol traces were saved in a set of gateway[1].<session_DI> files under the \Temporary Internet

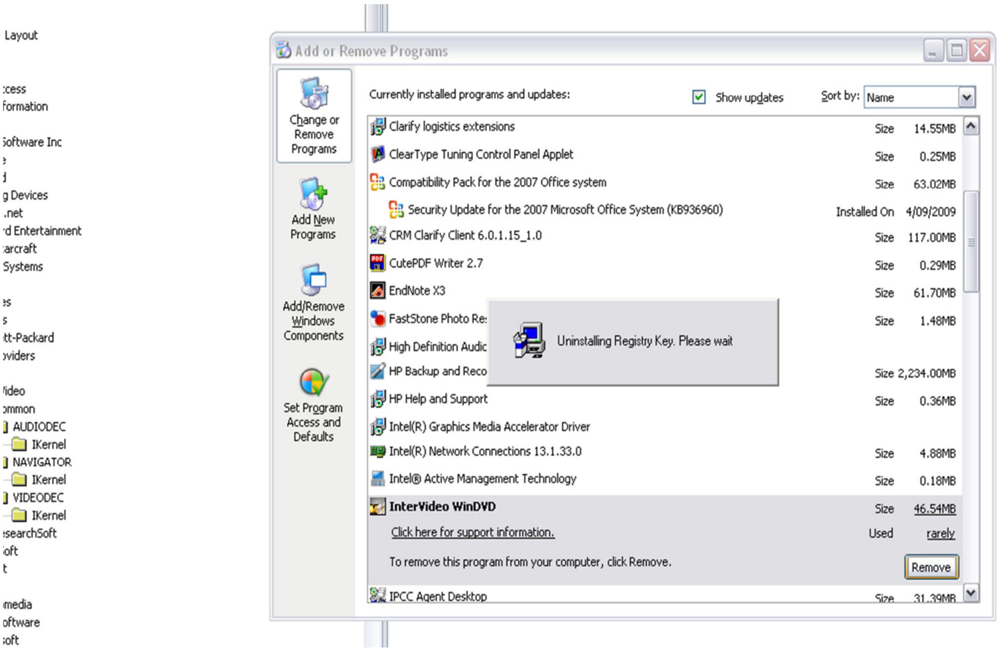
Files\content.IE5\directory (Dongen, 2007). The files can only be found if the default port of the window live messenger is blocked and they contain the gateway information of the conversation with date and time. Very often, the instant messenger application is not the only one that has left a fingerprint on a hard drive. An operating system generally stores information of all the installed/uninstalled applications in the system. For example, Microsoft windows 3.1 or later version stores the information in the Window registry. Information such as implicit application settings can often be found in the registry.

The Uninstalled application also leaves evidence. Originally, the application InterVideo was installed in a MS Window XP environment and records can be found in the window registry as shown in figure 2.3.0. Using the system default uninstall option from "Add or Remove Programs", the system automatically removes the application from the system and also explicitly states that registry key of the associated application has been uninstalled as shown in figure 2.3.1. However after the uninstall process has been completed, the registry record of InterVideo remains unchanged (See figure 2.3.2). This finding shows that even if a user has deleted an instant messenger application, there is a chance that a record can be found in the registry to prove that the instant messenger has once installed onto the system.



Name	Type	Data
(Default)	REG_SZ	(value not set)

Figure 2.3.0: InterVideo and its associated folders found in Window registry



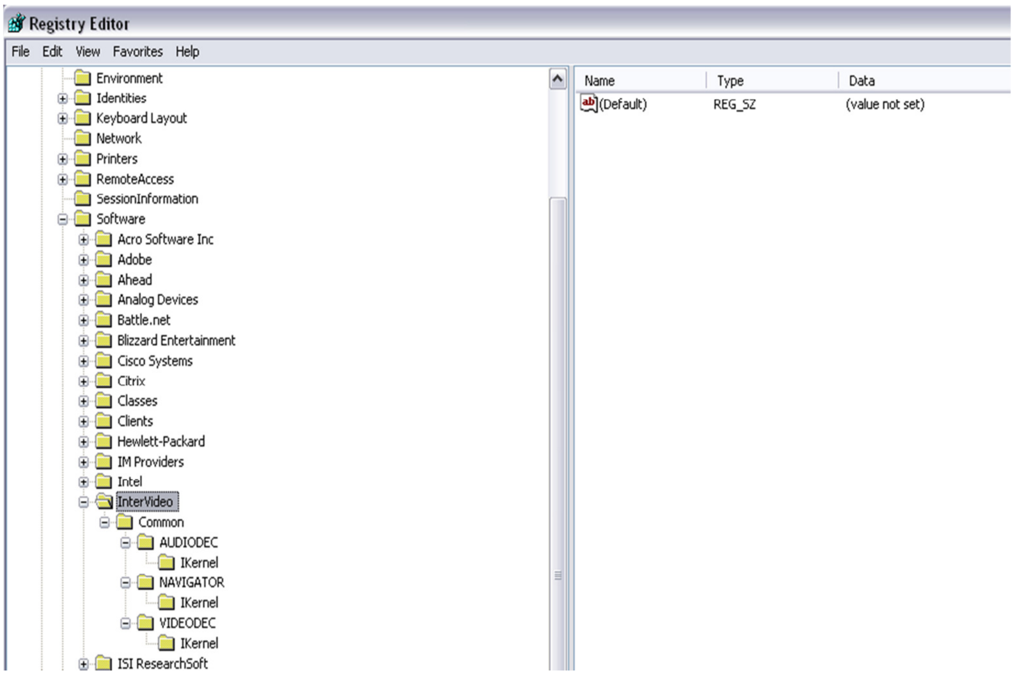
Currently installed programs and updates: ☑ Show updates

Clarify logistics extensions	Size	14.55MB
ClearType Tuning Control Panel Applet	Size	0.25MB
Compatibility Pack for the 2007 Office system	Size	63.02MB
Security Update for the 2007 Microsoft Office System (KB936960)	Installed On	4/09/2009
CRM Clarify Client 6.0.1.15_1.0	Size	117.00MB
CutePDF Writer 2.7	Size	0.29MB
EndNote X3	Size	61.70MB
FastStone Photo Re	Size	1.48MB
High Definition Audic		
HP Backup and Reco	Size	2,234.00MB
HP Help and Support	Size	0.36MB
Intel(R) Graphics Media Accelerator Driver		
Intel(R) Network Connections 13.1.33.0	Size	4.88MB
Intel® Active Management Technology	Size	0.18MB
InterVideo WinDVD	Size	46.54MB
Click here for support information.	Used	rarely
IPCC Agent Desktop	Size	31.39MB

To remove this program from your computer, click Remove.

Uninstalling Registry Key. Please wait

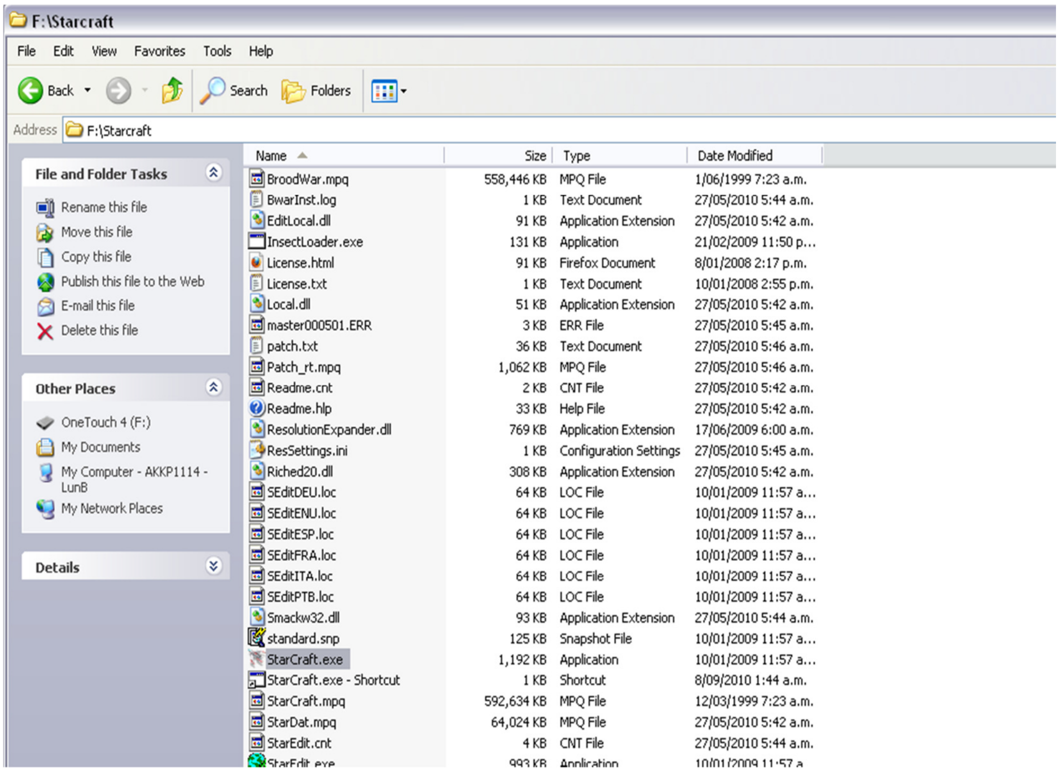
Figure 2.3.1: “Add or Remove Programs” inform the user registry key is being uninstalled.



```
Environment
Identities
Keyboard Layout
Network
Printers
RemoteAccess
SessionInformation
Software
    Acro Software Inc
    Adobe
    Ahead
    Analog Devices
    Battle.net
    Blizzard Entertainment
    Cisco Systems
    Citrix
    Classes
    Clients
    Hewlett-Packard
    IM Providers
    Intel
    InterVideo
        Common
            AUDIODEC
                IKernel
            NAVIGATOR
                IKernel
            VIDEODEC
                IKernel
    ISI ResearchSoft
```

Name	Type	Data
(Default)	REG_SZ	(value not set)

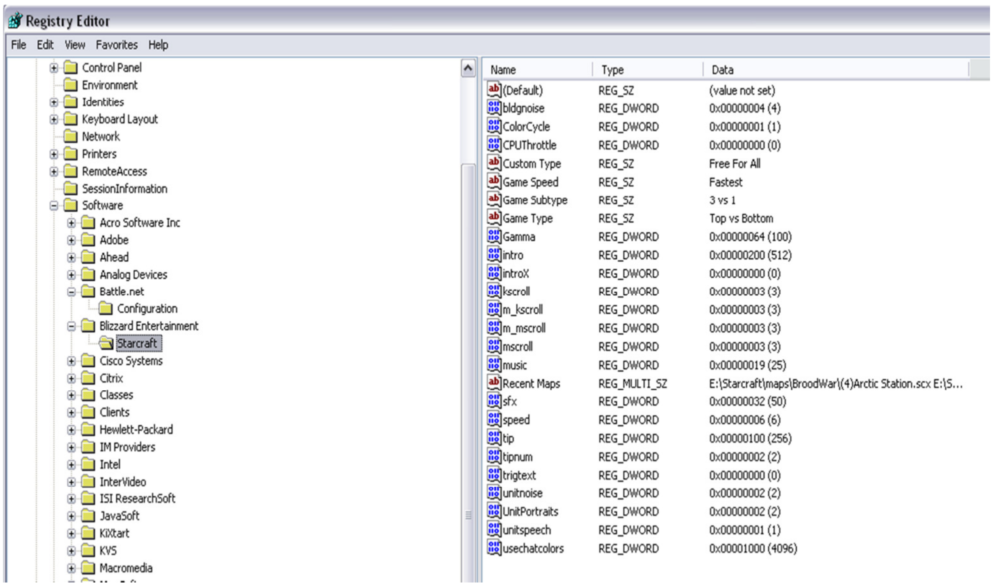
Figure 2.3.2: After the uninstall process is completed, record of InterVideo and its associated folder remain unchanged in Window registry.



Name	Size	Type	Date Modified
BroodWar.mpq	558,446 KB	MPQ File	1/06/1999 7:23 a.m.
BwarInst.log	1 KB	Text Document	27/05/2010 5:44 a.m.
EditLocal.dll	91 KB	Application Extension	27/05/2010 5:42 a.m.
InsectLoader.exe	131 KB	Application	21/02/2009 11:50 p...
License.html	91 KB	Firefox Document	8/01/2008 2:17 p.m.
License.txt	1 KB	Text Document	10/01/2008 2:55 p.m.
Local.dll	51 KB	Application Extension	27/05/2010 5:42 a.m.
master000501.ERR	3 KB	ERR File	27/05/2010 5:45 a.m.
patch.txt	36 KB	Text Document	27/05/2010 5:46 a.m.
Patch_rt.mpq	1,062 KB	MPQ File	27/05/2010 5:46 a.m.
Readme.cnt	2 KB	CNT File	27/05/2010 5:42 a.m.
Readme.hlp	33 KB	Help File	27/05/2010 5:42 a.m.
ResolutionExpander.dll	769 KB	Application Extension	17/06/2009 6:00 a.m.
ResSettings.ini	1 KB	Configuration Settings	27/05/2010 5:45 a.m.
Riched20.dll	308 KB	Application Extension	27/05/2010 5:42 a.m.
SEditDEU.loc	64 KB	LOC File	10/01/2009 11:57 a...
SEditENU.loc	64 KB	LOC File	10/01/2009 11:57 a...
SEditESP.loc	64 KB	LOC File	10/01/2009 11:57 a...
SEditFRA.loc	64 KB	LOC File	10/01/2009 11:57 a...
SEditITA.loc	64 KB	LOC File	10/01/2009 11:57 a...
SEditPTB.loc	64 KB	LOC File	10/01/2009 11:57 a...
Smackw32.dll	93 KB	Application Extension	27/05/2010 5:44 a.m.
standard.snp	125 KB	Snapshot File	10/01/2009 11:57 a...
StarCraft.exe	1,192 KB	Application	10/01/2009 11:57 a...
StarCraft.exe - Shortcut	1 KB	Shortcut	8/09/2010 1:44 a.m.
StarCraft.mpq	592,634 KB	MPQ File	12/03/1999 7:23 a.m.
StarDat.mpq	64,024 KB	MPQ File	27/05/2010 5:42 a.m.
StarEdit.cnt	4 KB	CNT File	27/05/2010 5:44 a.m.
StarEdit.exe	993 KB	Application	10/01/2009 11:57 a

Figure 2.3.3: The application "Starcraft" is stored on F drive, a USB hard drive.

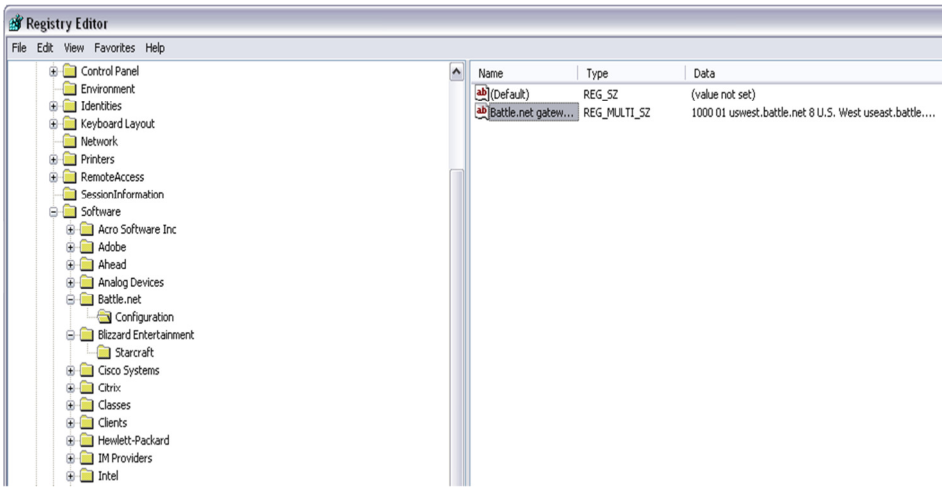
Application executed from a remote location can be found. An application was stored on a removable hard drive as shown in figure 2.3.3. The application StarCraft.exe from F drive was executed via the Window XP operating system and records was automatically generated in the Window registry as shown in figure 2.3.4. Several application settings can also be found in the registry entry. The application was neither installed on the operating system nor run from a local drive; somehow entries were automatically generated in the Window registry.



Name	Type	Data
(Default)	REG_SZ	(value not set)
bldgnoise	REG_DWORD	0x00000004 (4)
ColorCycle	REG_DWORD	0x00000001 (1)
CPUThrottle	REG_DWORD	0x00000000 (0)
Custom Type	REG_SZ	Free For All
Game Speed	REG_SZ	Fastest
Game Subtype	REG_SZ	3 vs 1
Game Type	REG_SZ	Top vs Bottom
Gamma	REG_DWORD	0x00000064 (100)
intro	REG_DWORD	0x00000200 (512)
introX	REG_DWORD	0x00000000 (0)
kscroll	REG_DWORD	0x00000003 (3)
m_kscroll	REG_DWORD	0x00000003 (3)
m_mscroll	REG_DWORD	0x00000003 (3)
mscroll	REG_DWORD	0x00000003 (3)
music	REG_DWORD	0x00000019 (25)
Recent Maps	REG_MULTI_SZ	E:\Starcraft\maps\BroodWar\(4)Arctic Station.scx E:\S...
sfx	REG_DWORD	0x00000032 (50)
speed	REG_DWORD	0x00000006 (6)
tip	REG_DWORD	0x00000100 (256)
tipnum	REG_DWORD	0x00000002 (2)
trigtext	REG_DWORD	0x00000000 (0)
unitnoise	REG_DWORD	0x00000002 (2)
UnitPortraits	REG_DWORD	0x00000002 (2)
unitspeech	REG_DWORD	0x00000001 (1)
usechatcolors	REG_DWORD	0x00001000 (4096)

Figure 2.3.4: Automatic Entry Generation Example

Furthermore, the application has been used to connect to a server and the address of the remote server has been recorded in an associated registry folder as shown in figure 2.3.5.



Name	Type	Data
(Default)	REG_SZ	(value not set)
Battle.net gatew...	REG_MULTI_SZ	1000 01 uswest.battle.net 8 U.S. West useast.battle....

Figure 2.3.5: Network Information

Network information associated to an application that has never been installed onto the operating system was saved in Window registry. The research has illustrated that even if an application is not installed onto the operating system or stored locally, there is a chance that the record can be found in the registry if the application has been executed on the operating system. It is possible that an instant messenger was stored and installed in a remote location and Window registry hold the information if the messenger has been executed from the machine.

It has been proven that information such as MSN passport ID and WLM (Window Live Messenger) credential data are created in the Window registry after an attempt to login (Dongen, 2007). The MSN passport ID will store the preferences and a setting of the user if a login is successful, which might lead to discovery of important evidence such as location of chatlog storage (Dongen, 2007). The WLM record contains the account login name, which is also the email address of the user (Dongen, 2007). Some of the information stored in the window registry is encrypted but can be decrypted easily by application such as forensicbox (Dongen, 2007). AIM can stores a list of customized auto response message in the registry (Reust, 2006). The following list is a summary of possible information stored by the system in the Window registry that relates to instant messaging:

Table 2.3.7: Summary of possible information stored by the system

Items	Description/Summary
Global WLM settings	State if the WLM user has configured audio and video devices
Webcam	Timestamp showing the last initiation of a webcam in WLM, also show information on whether only the user is broadcasting, only the contact is broadcasting or both parties are broadcasting.
MSN passport ID	Contain WLM account ID which is one of the email account of the user, directory where the chatlog is logged if the location has been changed from the default location, location at which received file are saved and other minor settings of the messenger.
Windows credential	Hold information such as the remembered account name of WLM
File saved	Contain a record of all files received by WLM using the 'save as' function. With all the path of file that has been saved to, the full name and extension of the file.
Server	Information of server if the application has connected to a remote location, port used and proxy setting might also be found
Away message	Customized auto response message is stored in the registry for AIM

Information is also stored within the memory. Traditional digital forensics usually focuses on analysis of permanent storage media including hard drives, CDs, and DVDs (Mrdovic, Huseinovic, & Zajko, 2009). However due to an increasing popularity in mobile storage devices and portable applications, very often limited evidence can be found with a traditional digital forensic analysis. Since every application requires memory to execute, it is logical to think that there evidence could be left behind in the system's memory. The analysis on live memory has allows us to extend the possibility in providing additional contextual information for any cases. We can now receive a more comprehensive view on the event that has occurred on a computer system (Mrdovic et al., 2009).

Every operating system uses a different physical memory structure (Mrdovic et al., 2009). For any Window based operating system, it is important evidence can usually be found beneath the physical memory(RAM), hibernation file and pagefile (Gao & Cao, 2010). Physical memory refers to the RAM

(Random Access Memory) and RAM is used to execute process and command given from an application. Hibernation files are files created on the hard drive containing the content of the RAM. They are generally created before a computer shuts down and stores the state of the computer and can be used to restore to the initial state when the computer power up next time. Pagefile is a portion of hard drive storage that was reserved to act as an extension of RAM. Pagefile are generally used when the RAM is full and the data on the RAM are being used. The Pagefile could potentially contain the same information that primarily stored on RAM and the data remain even if a computer is shut down if it is saved in the page file.

Previous research has shown that instant messenger may leave information on the system's memory once the application is executed, information such as IP address of the instant messenger chat session initiator's can be found in the live memory (Carvey, 2004). In some rare cases, it is possible to retrieve the chat history from the memory, for example if the messenger encrypts the message before sending over network such as QQ (Gao & Cao, 2010), since the encryption process require the use of live memory, testing done in a previous study and has found that the pre-encrypt message from the memory (Gao & Cao, 2010). Other information such as contact lists, which accounts are used, discussion groups, display names and filenames of uploaded/downloaded files by the user were proven to be recovered from the live memory were also found in the study (Gao & Cao, 2010).

These Processes can be reconstructed. In a modern computer system, the size of live memory can be huge in terms of forensic analysis, 4GB of RAM is common in a computer for home users and the size can go up significantly on a server. When the size of physical memory and the page file memory are combined, the scope of the searching area can get even larger. The evidence required for a case might be divided into small fragment throughout the memory (Gao & Cao, 2010). Therefore it is more effective if we can reconstruct the process space during an investigation so the examiner can minimize the area to search. In 2006, an article 'Searching for processes and threads in Microsoft Windows memory dumps' published by Andreas Schuster was published on how to search for processes and threads for Microsoft Window and lead to process reconstruction (Schuster, 2006). The research was done based on Window NT system. Every resource in a Window NT operating system live memory system is represented as an object and every object in the memory was prefixed by an object header. The object header structure contains information about the instance of an object (Schuster, 2006). A research has successfully reconstructed the process space by following Andreas Schuster's method (Gao & Cao, 2010).

After the process has been reconstructed, it is important for the investigator to know the executable file associated with the instant messenger, for example aim.exe or aim95.exe were the associated execute file for AOL Instant Messenger that appear in the system file log (Carvey, 2004). After locating the process associated with the messenger, utility such as pmdump.exe can be used to retrieve the content of the memory (Gao & Cao, 2010). It is important to note that executing a forensic tool to collect information from the live memory can possibly overwrite the data stored on the memory. However the chance to overwrite important data is very slim in a modern computer system, every process to retrieve evidence from a live system must be carefully documented (Gao & Cao, 2010). A summary of information possibly hidden within the memory is:

IP address of the chat initiator;
Chat history;
Contact list;
Which accounts are used;
Discussion group;
Display name;
Filename of the uploaded/downloaded file;
Session information; and,
Possible keys.

Information within the network can also be available. Instant messenger is primarily a digital communication tool. In order to transmit information from one end to another, every piece of information has to be encapsulated into packets and send through the network over various type of protocol. Previous researches have proven messenger packets can be identified and captured from the network using different techniques. Identifying messenger packets is possible. Different type of packets is being sent over network daily in network of different size. In order for an effective network forensic acquisition, the scope of search should be minimize and focus only on the packets that contain useful forensic information. A group of researchers has presented their experiment to identify Google Talk (A popular messenger) packets over a small network in 2009 (Ho, Chen, & Hsieh, 2009). By filtering out and capturing packets transmitted by the instant messenger, chat record between two users has been successful retrieved from the network. The experiment was done by using Wireshark (Ho et al., 2009), a popular network sniffer used mainly be network engineer to diagnose network problem. The experiment was setup and conducted through a small private network, Wireshark was used to monitor both the incoming and outgoing network packets from the computers. It is known that Google talk client was based on Jabber protocol (Ho et al., 2009) and packets sent via Jabber protocol were spotted with Wireshark. The research has found that the content of those captured Jabber packets cannot be recognize because they were encrypted message transmitted between the Google talk client and Google talk server (Ho et al., 2009). Even the content of the message could not be read, there are some packets used for updating contact list and user status such as away, available are readable from a small amount of packets. The packet has clearly shown the source and destination IP address and Port number of the sender and receiver of the messenger (Ho et al., 2009).

The scope of the search was then shifted to focus on the packets initiated and received by the IP address and port found in the previous packets. However the packet payloads cannot be recognized, therefore no useful information can be extracted from this trail. The next approach was to focus on the default Google IP address range from 64.233.160.0 – 64.233.191.255 and 72.14.192.0 – 72.14.255.255 (Ho et al., 2009). Wireshark was able to captured packets sent within the IP range; however these packets are also encrypted. It is likely that the Google talk packets were mixed with Gmail activity and both are encrypted with SSL and since many ports are arbitrarily used, therefore it is very difficult to differentiate between the two.

However it has been found that Gmail chat over http is not encrypted in another approach that observe packet sent through http source (Ho et al., 2009). Research has shown that Wireshark was able to extract a clear chat content from these unencrypted http packets. Each packets has also shown the time stamp of when the packets being transmitted, the Gmail address of both the sender and receiver (Ho et al., 2009). More testing can be conduct in the later experiment section to experiment if digital evidence from the other messengers can be found by going through similar trials. Most instant messenger send plaintext over the network while some instant messenger will always encrypt the message before sending over the network due to security purpose (Gao & Cao, 2010).

Therefore, in theory we can acquire any information generated by an instant messenger in within the network. However there are many constraints limiting the performing of a network digital evidence acquisition. A list of digital evidence found within the network is:

Chat Content;
IP address;
Messenger Status; and,
Port number.

2.4 IM INVESTIGATION PROCEDURES

It is essential to gather as much information as possible about the site and the situation in the pre-search preparation. Very often, specific forensic tools are required in the evidence collection process on site and these can be selected based on past experience and the analysis of the available information. For any case that involves criminal evidence, most of the time a search warrant is required before any action can be legally performed on the equipment that might contain the evidence.

In a case that involves evidence collection from messenger, information of the operating system, storage devices that contain the messenger, hardware specifications, location of messenger in the storage device and its associated files should be included in the warrant application. Knowing the information of the site can aid the investigator to decide on the scope of area to search in the search warrant application. For example if the target messenger is a traditional messenger, then the search warrant should be the file associated with the messenger including the chat log. If the target messenger is a volatile type messenger, then the search warrant application should cover the unallocated space in the target storage device.

Data stored in the messenger could be a source to locate critical evidence such as suspect’s location, point of origin of the offender, screen names, bank transaction information, direct and indirect information of the crime, information to identify suspect, date and time of every item in the conversation history. The objective of a search should be to discover and recover as much of the information types as possible. The Investigator should also obtain information such as the internet service provider that connects suspect’s machine to the internet, the registered name of the account in the ISP. Additional evidence such as if the physical location of the party on the other end of conversation is retrievable with the co-operation of the ISP. The instant messenger service provider is not usually compelled to keep a log of the IP address and activity for the user’s account. However the messenger provider generally keeps the record of the messenger account owner. Information such as name, gender, physical address, contact phone number, age, interest, associated email address and other personal information could be found in the record. However the information is not necessarily accurate. A warrant or letter from the court is generally required for the ISP or messenger provider to expose such information.

Later messenger has provided extra functions such as voice chat, video chat, file transfer, drawing board, party chat that involve multiple chat clients and links that connect to other services such as chat room or games. There is a possibility that the evidence or hint that lead to the discovery of evidence could lie within any of these functions. Investigator will need to determine if an on-site or off-site search is required depends on the characteristics of the case. Very often the activity of an active messenger might be observable from the computer screen and photos should be taken from the screen recording the content of the chat windows and other related materials such as the friend list in the messenger. Valuable information could be recovered from the live memory. For such a situation, investigator should bring along forensic tools that are required for capturing data from random access memory.

There are other situations where the system hosting the messenger service is associated with other important activities and the storage is not allowed to be removed from the system to prevent interruption on the service that the system delivers. In such situation, an on-site investigation has to be carried out unless otherwise stated by the search warrant. An Investigator should also decide whether or not it is appropriate to disconnect the network connecting to the device hosting the messenger. In some situation where leaving the messenger login and running could open up the possibility to acquire additional evidence for the case, however it also enable hacker to alter the integrity of files that contains key evidence to the case.

Some equipment that could aid an on-site search for instant messenger includes:

Password cracker – The messenger might be logged out and a password cracker can possibly allow the investigator to login the messenger to collect an extensive amount of evidence.

Messenger investigation software – Allow the investigator to quickly locate the files which might contain key evidence left behind by instant messenger.

Recovery software - Enable investigator to recover deleted or hidden data on site.

Locking tool – To ensure data integrity on the target files, protect them from intentional corruption over the network or accidental alteration from any investigation tools.

In most cases, off-site searching allows a more comprehensive search on the seized storage devices and the investigator often has a more relax time frame. However for an investigation that involves instant messenger, much evidence is not retrievable once the machine is removed from site. For example a volatile type messenger often leaves an investigator less information for an off-site search. Legal issues may arise while moving any related devices from the site to the lab. It is important for the investigator to consider carefully before removing any item or power down the machine as any mistake could result in permanent loss of evidence. Equal consideration must also be given to the processes of Seizing, Processing, and Reporting.

2.5 TRADITIONAL IM INVESTIGATION

According to the forensic guide, it has mentioned that instant messaging communication may involve text, voice, video and file transfer (Hagy, 2007b). The guide has also provide a basic introduction on how IM services work, the account creation procedure and a basic introduction of how the instant messenger interface look like based on an older version of AOL instant messenger. According to the forensic guide Investigation involving internet and computer network published by United State department of Justice in 2007 (Hagy, 2007a), the following information may be useful to an investigation:

- The computer being used to receive the communication
- The screen or user name (victim and suspect)
- The owner of the Internet Service Provider (ISP) account being used.
- The IM service being used and version of the software
- The content (witness account of contact or activity)
- The date and time the message was received/viewed
- The dates and times of previous contacts
- Any logging or printouts of communications saved by the victim
- Applicable passwords
- Potential suspects
- Whether an Order of Protection/restraining order was in effect
- Witnesses that may have observed the communication
- Whether security software was in use that may have captured additional information

The forensic guide has given instruction to collect information from a seized computer system when the chat window was still opened and it has mentioned that a chat log may be saved but evidence might be lost one the computer has powered off. However the guide did not describe any further instruction or approach to acquire evidence from instant messenger.

If the forensic examiner follows the instruction provided by the forensic guide, the examiner can only capture the current state of the computer system and only under the condition when the chat window was still opened. However any historical data cannot be retrieved if a chat history was not saved which was suggested to be the reality in most cases (Hagy, 2007a).

2.6 ISSUES AND PROBLEMS

A review of the sections above suggests that there are many issues and problems with doing professional digital forensic work on IMs. In this section a short summary is to be made so those in chapter 3 a relevant problem may be selected for research.

A key area was the incomplete nature of instant messenger investigation processes presented in the forensic guide. In the handbook 'Investigation involving the internet and computer networks' published by U.S. Department of Justice, chapter 5 provides information on investigations involving instant message services were detailed. The key points of the processes to collect digital evidence involving instant messenger were summarized. The section was informative to a certain extent and is intended to be used as a basic guide for enforcement agencies. However some of the later methods and technologies were not covered. The author of the chapter himself has also realized the incompleteness and therefore put in a statement at the beginning of the chapter: "The section does not encompass a complete discussion of all the issues surrounding the use of instant messenger communications in an investigation and additional expertise may be needed for a more detailed investigation."

Based on the forensic guides, the following topics were discussed to extend the knowledge in some area of the investigation process: Files stored on a hard drive by the application, file stored on a hard drive by the system, information stored in the memory and information available from the network. Although in theory Digital evidence can be collected over the network, it will be very difficult to perform in reality due to numerous technical and non-technical difficulties.

Difficulties start with connectivity. It is known that authenticity and reliability are the main issue when collecting network evidence from an untrusted network, i.e. the internet (Nikkel, 2006). Generally an IP (Internet Protocol) address and a MAC (Media Access Control) address are used to locate the physical address of a source. However there are many techniques to fake the logical address over the network such as proxy server, web anonymizers, onion routing, Mixmaster/cypherpunk remailers (Nikkel, 2006). Some of the techniques can alter the protocol header information and even then content of the packet can be fictitious (Nikkel, 2006). A summary of issues is as follows:

Proxy Server – It is a very common network technique that serves many IT purpose. The concept is to use a third or even a forth computers in another physical location to redirect the network packets to the destiny. By re-routing the packet, it increases the difficulty to locate the original data source by adding layers of IP addresses to investigate within the network routes.

Web anonymizers (http://www.livinginternet.com/i/is_anon_work.htm) – Using the idea of proxy, web anonymizers allow a user to access website on the internet anonymously by connecting through website that proxies specifically HTTP request. The client can simply send the webpage request to the anonymizer server and the anonymizer server will request the information from the web server and resend the information from the web server to client’s machine. Only the anonymizer holds the information of the client.

Onion routing (http://www.onion-router.net/) – A technique used to cloak network traffic by frequently encrypt message and sent through multiple network nodes over the network. Each node decrypts a layer of encryption to uncover the routing instruction.

Mixmaster/ cypherpunk remailers (http://anonymous.to/tutorials/anonymous-remailers/) – Specially encrypt message with PGP (Pretty Good Privacy or GPG (GNU Privacy Guard) which remove the sending’s information from the header when the message being forward. The method can be used to route a message from numerous of remailers to increase the complexity to determine who the sender is. The Mixmaster remailers can split big cypherpunk messages into several Mixmaster packets while being transmit to the next remailer to further increase the complexity by reducing the chance of capturing the whole message.

All the above techniques can be challenging and time consuming for investigator to locate the source of the in a network evidence acquisition (Nikkel, 2006). The trace can be even more complex if the techniques are carried out over various physical locations across countries boundary, which is fairly common as internet is boundary less in most cases. Due to such reason, it is recommended to collection network information as close to the target as possible, the distance meaning both the physical (geometrical) and logical (network hops) distance from the collector and the target (Nikkel, 2006). Generally as distance increases, the potential error rate and latency will also increase (Nikkel, 2006).

If a router or restricted web interface of a database is in place between the target node and the collector's node or the capturing device is placed in one or more hops away on a redundant network, part of the packets might route through other network path bypassing the collector, some information could be lost and there is a high chance that traffic could be blocked (Nikkel, 2006). In summary, the closer the network evidence collector is to the target node, the more competence the network acquisition can be (Nikkel, 2006).

2.7 CONCLUSION

Through literature research, I have realised that there are different techniques and tools designed to assist evidence acquisition from instant messenger but they were never mentioned in the digital forensic guide published by United States Department of Justice. The reviews have clearly shown that forensic examiners are using techniques that were not mentioned in the guide to extract information from instant messenger. Therefore the issues and problems raised in section 2.5 are relevant and require further research. In particular an examination of the effectiveness of the techniques and tools that were not mentioned in the forensic guide would be useful. In chapter 3 further explorations will be undertaken to establish a methodology to for researching the problem.

Chapter Three

RESEARCH METHODOLOGY

3.0 INTRODUCTION

Chapter 2 reviewed the literature relating to IM systems, the professional literature and a summary of the outstanding issues and problems was made. This chapter 3 will report an exploration to identify an appropriate methodology for investigating the scope of IM evidence extraction methods. The aim is to critique the adequacy of current professional guidance. Hence the problem is re-specified and the relevant research questions and hypothesis derived. The specification for data collection, processing and analysis will also be given.

The chapter is organized to communicate the progressive development of a methodology and to show the research journey I went through to arrive at appropriate methods. In Section 3.1 an exploratory interview with an expert IM software developer is reported. This interview helped to shape my understanding of IM scope. I then reviewed a set of readings on scientific methods. From these sources and section 2.6 summary I can then specify the problem and relevant research questions. Hence, the methodology chapter is firstly organized into the review of explorations (Section 3.1); the research design, research question and hypotheses (Section 3.2); and the data requirements such as how data is to be collected, processed, analyzed and presented (Section 3.3). Then, the limitations and expected outcomes of the research (Section 3.4) will be followed by the conclusion (Section 3.5).

3.1 DISCUSSION WITH EXPERT

An interview with the software developer as an expert was carried out to explore limitations, identify different ways of researching IT artifacts and to further discuss the IM design and development scenarios for evidence extraction. AUT ethics approval was not required for a consultation with an expert. The discussion is reported here and then analyzed for help in designing a research methodology. Chat Sniper is an evidence extraction tool used with IMs.

Barry: Does your application perform any hash check to verify the integrity of the original chat log and the copied chat log?

Alex: Not yet, but that's a good idea. Right now Chat Sniper simply copies the logs from one location to another using the same method as Windows copy/paste.

Barry: The chat sniper can search for chat logs from several messengers, display account usernames, generate buddy lists and retrieve images sent and received through photo-share sessions. According to the user manual, these functions will not work if any file containing the record has been deleted. Is there any plan to enhance the chat sniper to search for deleted files?

Alex: I would like to add the ability to search through free space for deleted files. This would greatly expand Chat Sniper's usefulness. Unfortunately, at this time I have no idea how to program that function.

Barry: In to your application user manual, it reads: *"If you're analyzing a seized drive, connect the drive to your analysis computer and make sure that Windows assigns it a drive letter. After this, run Chat Sniper and select the appropriate drive from the dropdown box."*
What we usually do is to image a seized drive and analyse the image. Can your application function with an image directly?

Alex: Chat Sniper cannot view images directly. Again, that's a feature I'd like to add at some point.

Barry: With the increase popularity of web-based instant messengers, do you have any plan to improve your chat sniper to function with them? Do you think it will be a difficult task since generally a web-based instant messenger won't leave obvious evidence such as a chat log on the storage device?

Alex: I've researched web-based messengers a bit and thus far I haven't found a way to extract any logs or chat artifacts. I think records left by the use of web messengers would be just as useful as records left by traditional messengers, but so far I haven't found a way to get to them yet.

Barry: According to my research, referring to a paper *Forensic analysis of volatile instant messaging*. Presented at the IFIP International Federation for Information Processing, Boston. They suggested that if some files have been deleted or overwritten, some useful forensic information from an instant messenger could also be found in drive free space and file slack. Do you think it is possible to equip the chat sniper with function to search for evidence in the drive free space, file slack and maybe also the RAM?

Alex: See number 2.

Barry: Do you think it is possible to improve your chat sniper to capture evidence from instant messenger over the network?

Alex: That would require active monitoring or some sort of client-side software on the target machine. That's dangerously close to spyware, so I hadn't planned on adding a feature like that.

Barry: Do you think there is currently a lack of standard procedure in capturing evidence from instant messenger and web-based instant messenger?

Alex: I'm not sure if I'd call it a lack of standard procedure, more like a lack of knowledge and training. I think police officers are generally unaware of where to look and what to expect when it comes to chat artifact retrieval, so it's up to tools like mine to fill that knowledge gap.

My comment:

The application is simple to use without needing any forensic knowledge, easy to deploy, economy and able speed up the process of evidence acquisition. However, the application was designed to be used directly with the evidence source for evidence acquisition. It does not provide any function to verify on file integrity from the source. This could lead to invalid evidence in a courtroom environment. Additional procedure and applications are required to ensure the integrity of file. The chat sniper can only function on a limited number of IM, which highly limited the scope of application area. Also it is not known that which version of IM has been tested for validation.

This tool is too simple for its purpose. It offers only the very basic functions in the process of evidence acquisition from IM. Heaps of evidence could have left out if the source file that contains the evidence was deleted or renamed. Forensic experts may not rely on this tool as the only option. The role of this application should be a tier1 acquisition tool aimed to aid the first level enforcement agency (i.e. police officer) in collecting evidence from IM. However the application itself does not provide any protection to the integrity of the chat log collected from the source. Files and system information on the target computer could be altered if the chat sniper is plugged in or installed onto the machine which cause serious consequence and could ruin the reliability of the evidence source. Therefore it should not be used in any serious circumstances. There is still plenty of room for this application to improve.

Hence in conclusion I found the discussion with an expert both helpful and confirming of concerns I had about standardization and consistency in IM evidence extraction tools. I was also surprised at the honesty of the expert and the range of problems he raised. IM evidence extract capabilities appear immature and open to research. Also the lack of clarity in many areas for requirements suggests that an exploratory and experimental method may best for this research.

3.2 CASE STUDIES OF RESEARCH

Case 1 is an example of AOL instant messenger and trace evidence. A case study was published in the Digital Investigation Journal by Jassica Reust (2006). The case was studied because part of the investigation process involved information extraction from instant messenger. In the article, the name of all involved parties, date and location of the criminal case were concealed but other information such as the intention of the case, the process and the finding of the digital investigation were clearly described. The investigation was initiated because the defendant has been accused of raping. However the defendant claimed that the sex was consensual. And to support his argument, the defendant claims that there was a conversation occurred between him and the complainant over AOL instant messenger shortly before he encountered the complainant at the crime scene, the defendant claimed that the complainant has invited him to her place.

The complainant provided another story and claimed that she had little or no contact with the defendant prior to the encounter, which the defendant disagreed and claimed that they had occasional conversation via AOL instant messenger. The tasks of the forensic examiner in the investigation was to examine the computer system of both the defendant and the complainant and attempt to extract digital evidence that conversation has occurred between the screen name of defendant and complainant on the night of the alleged rape.

There were a number of challenges for the forensic examiner in this case. After the alleged rape, both the computers used by complainant and the defendant were used for over a week before being seized by law enforcement. Under normal circumstance, if the chat window is closed and user did not enable the option to save the conversation history, then the evidence extraction for the chat history can become increasingly complicated and difficult. In the case, forensic examiners have attempted to extract evidence from the unallocated disk space and page file, a technique that has been described in chapter 2. However for this case, the computer examiners were unsuccessful to retrieve any chat history. Technique such as memory dump could also be used to recover chat history of a newly closed chat window from random access memory (RAM), however it was not applicable for this case since it was very likely that the RAM have been occupied by other service ran on the computer before the computers were seized.

From this case, it is observed that the forensic examiner and the enforcement agency were interest in:

The **Screen name** of both the defendant and the complainant;

The **Friend list** or also known as the **Contact list or Buddy list**. New screen name has to apply for approval from a user to be added to their friend list. Generally only screen names listed in the friend list were allowed to communicate with the owner of the friend list;

The **Personalized away message**, a common feature of instant messenger allows user to set their online status to normal, busy, away, and invisible. The status can be viewed by other screen names listed in the friend list. Upon activating the away status, the user is often allowed to leave a message to inform other party on the reason that he/she is away from their screen. The trigger on the activation and deactivation of away status varies from different instant messenger, some instant messenger are allowed to customise the behavior of their away status. The change in status might leave a trace in the computer system;

Indication that a conversation has occurred, the case shows that AOL instant messenger is capable to provide the 10 previous Screen names that have communication with the user; and,

Indication that a conversation have occurred (From Random Access Memory), in the case, forensic examiner were not able to find evidence that the 10 previous screen names that have communication with the user due to the fact that both the defendant and complainant’s computer have been used for another 10 days before being sized. Communications with other screen names that took place in the 10 days have pushed out the old record from the list. However forensic examiners were able to perform analysis on the Random Access Memory (RAM) seized from the computer of defendant. The analysis found evidence that there were communication between the screen names of defendant and complainant.

Forensic examiners in the case were able to recover evidence to prove that both defendant and complainant had used instant messenger, screen name of both parties and communication using instant messenger. However the chat history, date of conversation and chat log were not found. Interestingly, evidence that 'a conversation had occurred between screen name of defendant and complainant' was only found on the computer of defendant. Based on the information provided in the article, it is possible that a third party holds the access to the screen name of complainant and had conversation with defendant using the screen name of complainant. However the article did not mention any investigation was done towards that possibility.

There could be a chance that the chat history was saved on the AOL instant messaging server and the server might also provide information such as time of conversation and IP address of the screen names involved in the conversation. Furthermore, if there is doubt in the identity of person accessing the screen name, a method such as Authorship Attribution can be used to perform analysis on the chat log and provide reference on the identity of the person in the conversation. The detail of the method was illustrated in the techniques section of the paper.

Sample cases were also quoted and provide contexts for IM evidence extraction research:

> **Case 1:** The child seduction case mentioned above will be used (Grossman, 2006). Type of messenger, Screen name and the intention of chat are known, therefore the case can be simulated. A forensic copy of the original storage device that contains the chat log will be applied or else this case will be replaced by a similar case where original forensic resource is available. The objective for this case is to attempt to retrieve additional information with the new techniques.
>
> **Case 2:** Other case such as soliciting children for sex with the use of voice chat and video chat function (Dubord, 2008) can be useful to analysis. It is challenging to attempt to recover the voice chat and video if they are not saved or has been deleted from the storage device. A simulation to use voice chat and video chat will be carried out and

technique such as live memory search, unallocated space search will be conducted to attempt to locate and recover the multimedia conversation.

Case 3: A Rape case with evidence stored in AOL messenger (Reust, 2006) was detailed in an article, slight alteration could be done to replace AOL messenger with the newer volatile based AOL messenger and examine the effect of volatile based messenger to the evidence collection process. Live memory search, unallocated space search and network packet capture

3.3 SUMMARY OF PREVIOUS APPROACHES

This section reviews scientific approaches to research in IT. Schneier (2000) states that technology changes constantly but humans are less inclined to do so, and the result is all types of traditional crime can be perform through new technologies. For any crime that involves multiple parties, communication is always involved. Instant messenger as a tool to conduct communication over the network, therefore in theory it can be abusively used in the process of a cybercrime. During the process of any cybercrime that involves the use of instant messenger as a communication tool, a footprint can be left over by a criminal. The duty of digital forensic expert should be to retrieve the footprint that contains evidence of the crime.

The aim of the Schneier (2000) work was to review new techniques and tools designed to collect evidence from instant messenger. The objective of the new forensic tools was argued to be based on the following facts:

To provide additional yet practical evidence to the enforcement agency;

To shorten the time required for an investigation process;

To reduce the difficulties to collect evidence; and,

To reduce the cost to carry out a forensic task.

The research question was to answer how the new techniques and tools can assist the investigator to retrieve evidence from instant messenger in compare to the traditional approach. In order to answer the stated research question, a research methodology was established in order to provide an expandable, structural process to design and carry out experiments and generate a scientifically acceptable result to justify the answer for the research question. Scientific Methodology in Computing was developed by reviewing the usefulness of the selection of techniques and tools developed based on empirical methods and comparison methods (Santos, Dias, Silva, Ferreira, & Madeira, 2009). Empirical methods are increasingly important to any computer research (Santos et al., 2009). Practically, empirical methods aim to answer a question by a set of experiments or measurements and by analysis the collected data (Braught, Miller, & Reed, 2004).

Many questions faced by computer scientists are empirical in nature (Braught et al., 2004). Questions such as how to optimize an enterprise server, assess a new software development methodology, very often such questions can be solved by empirical method (Braught et al., 2004). The data collected from experiment can be used for analysis and to back up a theory or assumption and finally to derive a conclusion in the research (Braught et al., 2004). However, in the article 'Computer' published in 1998 (Tichy, 1998), it has stated Fred Brooks, a well-known software engineer and computer scientist has questioned the effectiveness of experimentation in computer science related topic (Tichy, 1998). It was suggested that testing theories by experiments would be misplaced because computer science is not a science but a synthetic, an engineering discipline (Tichy, 1998). It is somewhat true because from the view of a mathematicians, very often they claim that experiment does not prove anything, it is correct to an extend due to no experiment can proof with absolute certainty (Tichy, 1998).

Applying Scientific Methodology in the research gives rise to a question regarding how the new instant messenger forensic tools and techniques perform compare to the legacy method in revealing evidence from instant messenger. Therefore it is preferred to apply the chosen forensic tools and techniques to a real case or a simulated case in the experiment. The certainty of the experimental result can be significantly increased. Based on the above discussion in research methodology, the following procedures were used as an example to conduct a reliable evaluation on the forensic techniques and tools.

<u>Step 1 - Case Selection:</u>

Cases were selected base by criteria:

- Availability of the Resources

In order to simulate a forensic case, it requires having as much detail from the original case as possible. Ideally the best result can be achieved if the original copy of evidence is available for analysis. Where the original copy is not possible, detail description of the original evidence will be required to produce a quality simulation. Source must be reliable and does not require any ethics approval.

-Situation and Specialty

Ideally each case should be different with their own characteristics. They should be able to outline the testing of the new techniques, the case must also offer insufficient or very limited evidence after processed with traditional methods in order to give a potential for the new techniques a possibility to reveal any mystery left behind the case.

Step 2 - Simulation:

Equipment, network and software should be setup to closely match the detail provided by the case. The setup will follow a similar manner to the evidence tracing trial for AOL instant messenger done by Jessica Reust in 2006 (Reust, 2006). In the case the defendant was accused of raping and was later acquitted of the rape charge, the key evidence including screen name, a portion of the chat log's content, the nature of the case, IM and its version, keyword, buddy lists, user profile and other details of the cases were known (Reust, 2006). A setup that closely matches with this case can be simulated.

Step 3 – Experiment Design:

Follow by case simulation; new techniques will be applied in place depends on the case and attempt to retrieve additional evidence. For example, evidence can be found in deleted files, memory, network as the following example demonstrate. A detailed illusion of possible places where evidence can be found is provided in chapter 2. Searching unallocated space with EnCase may reveal deleted files, chat log and IE internet records, cookies, browsing history and cache records (Chen, Luo, Gao, Qian, & Wu, 2009). This technique is especially useful when the forensic examiner believe that any evidence that has been purposely deleted from the system or extra information required in analysis of volatile based instant messenger.

Additionally, live memory could be saved a copy of contact list, IM account information, display name and content of the chat (Gao & Cao, 2010) or other sensitive information that has been performed by process done on the predator's machine. The content in live memory can be browsed with application such as Ulink or WinHex. Unencrypted IM network packets can be captured with Wireshark and content such as screen name, chat content and file being sent between the two IM users may also be captured (Ho, Chen, & Hsieh, 2009). The method can also capture the IP address of the two IM users and may use as an evidence to prove the physical location of the predators.

Step 4 - Analysis

Data collected from the simulation will be compared to the evidence extracted from the original cases and all the new techniques will be comment based on the additional evidence they can collect (if any) and the effect to the evidence collection process. The results of the experiments will conclude on whether or not the new forensic techniques have the ability to reveal useful evidence that has been missed out in previous cases that were analysed with the traditional forensic process. And if there is, then what kind of evidence could be provided to benefit the cases.

The testing is not necessary the end of research but to locate the strength and weakness of each evidence collection techniques and to analyze the effect of these techniques to the evidence collection process. The outcome of this research can be used for both enhancing the design of an evidence collection system for instant messenger and assist any further development in evidence extraction tools or techniques for instant messenger (Chen et al., 2009; Kiley, Dankner, & Rogers, 2008; Law, Chow, Kwan, & Lai, 2007; Mrdovic, Huseinovic, & Zajko, 2009; Savoldi & Gubian, 2008). The limitation of the experiment is the lack of actual information and data from a case that involves evidence extraction from instant messenger. Therefore experiments can only be done in a simplified yet similar environment.

3.4 THE RESEARCH DESIGN

In the previous Sections 3.1-3.3, the interview and review of cases reviews of similar works have been identified and analysed in order to develop the options for this research. In particular section 3.3 reviewed systematic approaches to doing IM research. It was suggested four steps (case selection, simulation, experiment, and analysis) should be followed for investigation. However the cases and interviews suggest that there are many more problems than solutions in IM research. This section is organised to acknowledge the guidance developed in sections 1-3, to review the problems specified in section 2.6, to develop researchable questions, give a phase model to follow and to specify the data requirements.

3.4.1 The Research Problem

The review of the sections in chapter 2 made in sections 2.6 suggests that there are many issues and problems with doing professional digital forensic work on IMs. A key area was the incomplete nature of instant messenger investigation processes presented in the forensic guides. In the handbook 'Investigation involving the internet and computer networks' published by U.S. Department of Justice, chapter 5 provided information on investigations involving instant message services were detailed. The key points of the processes to collect digital evidence involving instant messenger were summarized. The section was informative to a certain extent and is intended to be used as a basic guide for enforcement agencies. However some methods and technologies were not specified. The author acknowledged that: "The section does not encompass a complete discussion of all the issues surrounding the use of instant messenger communications in an investigation and additional expertise may be needed for a more detailed investigation." Hence a key problem was identified, that of incompleteness. The problem has implications for technical problem solving and readiness for investigators to do IM research.

3.4.2 The Research Question

The review and identification of the research problem in chapter 2.6, leads to the development of a research question that is feasible for a proposed project such as this. There are many more questions that could be logically asked but the selection of a question must consider the time and resource limitations in proposing wide scope and long time frame options. Consequently the research question is stated as:

Can later forensic tool and technique add value to the traditional approach in evidence acquisition from instant messaging?

A working hypothesis for the primary research question can also be asserted:

Techniques and tools designed for instant messaging forensic examination are able to provide additional value to an investigation.

And the sub-questions can be stated as:

Are the current computer forensic tools adequate in evidence acquisition from instant messenger?
&
Was the selected forensic tool able to recover information from Microsoft live messenger as advertise?

And working hypothesis for the sub-questions can also be asserted:

A large portion of information can be recovered from instant messenger with the current forensic tools and techniques designed for that purpose.
&
The selected forensic tool was able to carry out the functions it has advertised and was able to deliver the promised evidence from Microsoft live messenger.

3.4.3 Planned Research Overview

The research involves four different phases that have come from the literature review and guidance gained from the reviews in sections 3.1-3.3. First a scenario / case should be chosen to encapsulate the project. The choice of extraction scenario was made for a scenario where an IM has enabled the function to save chat history and the chat program has been shut down before an enforcement agency can seize the computer system containing the instant messenger.

The phases were then defined as (see figure 3.4):

A Pilot Study – where the integration and tool performances could be tested;

The Pilot Analysis – where the environment could be stabilized;

A Formal Extraction – where a IM evidence extraction could be demonstrated; and,

The Analysis of findings – where reports can be made.

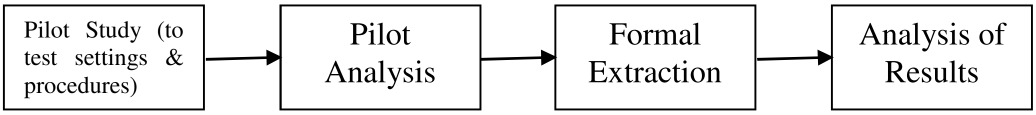


Figure 3.4: Research Phases

3.5 DATA REQUIREMENTS

The data requirements for the research project include several different sources. Some data will come from trial and error testing of configurations and extraction software. Some data will come from the pilot study and other data from the formal extraction. There will also be theoretical data generated by the analysis and comparative study of findings and the guides reported in chapter 2 and 3. Data can therefore be presented as tables, figures, screenshots and in descriptive forms.

The analysis of the tools can also provide data to inform best practice guidance. For example the issues raised with FTK Imager. Through discussion with Belkasoft technical support, there is a chance that the FTK Imager might affect the integrity of the data on a seized drive. When running FTK Imager to collect data dump from the seized computer system, FTK Imager consumes only a small portion of RAM in modern computer system and the chance of affection cannot be prevented. It was selected because the application was free and it was highly recommend by the Belkasoft technical support.

Similarly the Belkasoft Evidence Center has issues for consideration. Belkasoft Evidence Center was designed to perform instant messenger forensic examination for instant messaging. The evidence might be retrieve from hard drive and RAM. However the software does not offer the function to capture an image from a seized drive and it is unable to capture live memory data. Therefore FTK Imager was selected to assist Evidence Centre in capturing hard drive image and performed the live memory dump from the virtual machine image. Despite the fact that there are many different forensic methodologies can be found in literature, every phase of any methodology must be performed correctly by the forensic investigator. Otherwise, the results of the investigation as evidences may not be possibly accepted by the court (Fowler, 2009).

3.6 LIMITATIONS AND EXPECTED OUTCOMES

This study is designed to demonstrate one successful extraction of evidence from IM under two scenarios. As such it is a case study and it may not be transferred to other environments or contexts. The depth of literature research completed and the testing of the software tool environment in the pilot study should provide reliability so that generalisations can be made. To answer the research question the addition of any knowledge to the current forensic extraction guide published by U.S department of Justice will show the limitation of such guidance. It is expected that more than one contribution can be made and fresh guidance provided.

3.7 CONCLUSION

In this methodology chapter 3, the comprehensive review of the background to the experimental method was made. A research methodology was derived from diverse sources and designed to fit a pragmatic approach to testing digital evidence extraction from IM. Some of the detail is yet to be developed as the Pilot Study is undertaken. In chapter 4 the Pilot Study is reported and further detail of the software environment and configurations is given. Chapter 4 will now report the findings of the test case.

Chapter Four

RESEARCH FINDINGS

4.0 INTRODUCTION

In the previous chapter (Chapter 3), the research methodology was decided by interviewing an expert, looking at what other people had done and also looking directly at the IT artefact, the Instant Messenger (IM). The artefact itself and the guidance from digital forensic investigation literature suggested that a direct approach to the artefact through extraction tool software would provide the best insight into the problem of evidence extraction from IM. The case of volatile IM was chosen as it is a more difficult and a contemporary development for IM.

The procedures outlined in Chapter 3 were designed to run a pilot study first so that the potential to apply systematic and standardised forensic extraction methods could be explored. In his chapter 4 the results of the pilot study and research results (a successful extraction) are reported. In section 4.1 the experimental method and its development are reported. In section 4.2 the pilot study, the issues and problems; and, the subsequent decisions that were made to structure the formal extraction are reported. In section 4.3 the results of the formal extraction are reported.

4.1 EXPERIMENTAL PREPARATION AND SETUP

The simulation testing on extraction scenarios was carried out for a scenario where an IM has enabled the function to save chat history and the chat program has been shut down before an enforcement agency can seize the computer system containing the instant messenger. In this section, the trial and error analysis and trials are presented in order to evaluate the assumptions made regarding potential digital evidence extraction. The MSN live messenger environment is used and the Belkasoft Evidence Center forensic tool selected for the tests. Many of the reports simply demonstrate the performance of the tool under particular conditions and server to guide the use and the settings for the formal extraction.

From the previous literature review in chapter 2 a list of information that was potentially important to forensic examiner during an instant messaging examination was summarised. The information included:

Screen name;
Friend list/Contact list/Buddy list;
Personalized away messages;
Indication that a conversation have occurred;
Chat history (Content of conversation);
Date and time of the conversation;
Email address of screen name;
Indication that picture sharing has occurred;
The content of picture shared or received via instant messenger;
Indication that video call has occurred;
The content of video call received or sent via instant messenger;
Indication of voice message has been sent or received; and,
The content of the voice message.

The literature also indicated that a trace of the information listed above could potentially be found in the following areas in the computer system:

The historical log of messenger;
Allocated disk space;
Unallocated disk space;
Random access memory (RAM);
Pagefile;
Hibernation file; and,
System Registry.

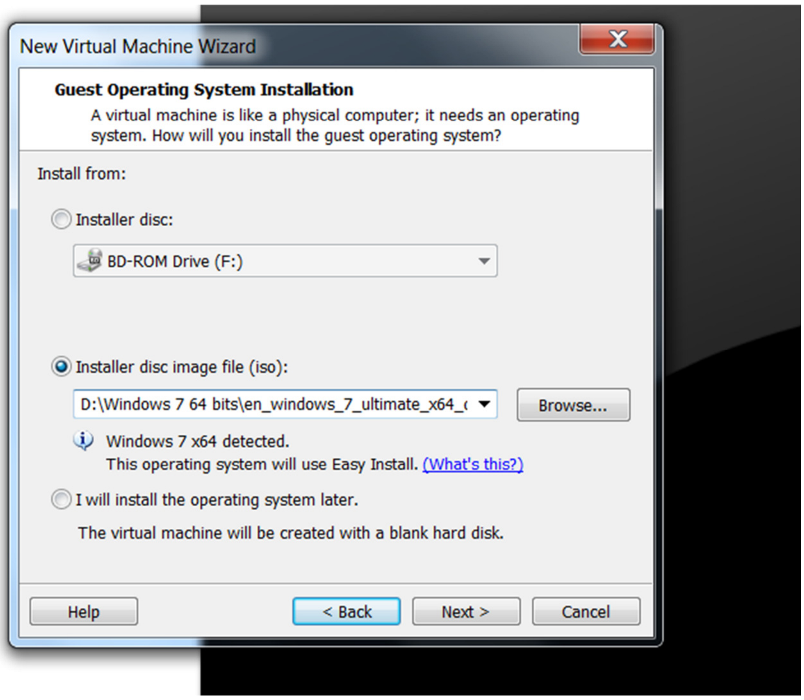
In order to compare what information could be potentially important and what can actually be recovered from the selected forensic tool, a table had been constructed (Figure 4.1.1). The items in the table were selected based on the case study and literature research in previous chapters 2 and 3. The empty box was marked with an ‘O’ if the information was able to be retrieved in that area of a computer system. Otherwise the box was marked with ‘X’. All the testing was conducted using VMware Workstation 8.0.2 build-591240 and the benefits of using virtualisation technology are outlined in section 4.2. Much time was spent setting the test environment up and manipulating the variables so that a stable, consistent and reliable platform was available for the formal testing requirements.

List of Evidence	Messenger history profile	Allocated disk space	Unallocated disk space	RAM	Pagefile	Hibernation file	System Registry
Screen Name							
Friend list/Contact list/Buddy list							
Personalized away messages							
Online status							
Indication that a conversation have occurred							
Chat history							
Date and time of the conversation							
Email address of screen name							
Indication of file transferred							
File name of file transferred							
Location of file							
Indication of picture share							
Picture Shared							
Indication of video call							
Content of video call							
Indication of voice call							
Content of voice call							
Indication of voice message							
Content of voice message							

Figure 4.1.1: Matrix for examining the capability of ideal IM forensic tool

In order to setup the virtual environment, the first step was to create the virtual image using the new virtual machine wizard as shown in figure 4.1.2. The testing was conducted using Microsoft Window 7 Ultimate 64bits operating system and an Installer Disc Image file (.iso) for the platform.

The wizard has created a virtual image with Microsoft Window 7. Initially the virtual machine was assigned with 1GB of RAM, network access and 60GB of hard disk space in NTFS format as shown in figure 4.1.3. Most of the settings can be changed after the image was setup and some settings such as adjusting the amount of random access memory required the virtual machine to be restarted. Figure 4.1.4 provided a screenshot on how the VMware setup page looked like.


New Virtual Machine Wizard

Guest Operating System Installation

A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

○ Installer disc:

BD-ROM Drive (F:)

● Installer disc image file (iso):

D:\Windows 7 64 bits\en_windows_7_ultimate_x64_(

Windows 7 x64 detected.
This operating system will use Easy Install. (What's this?)

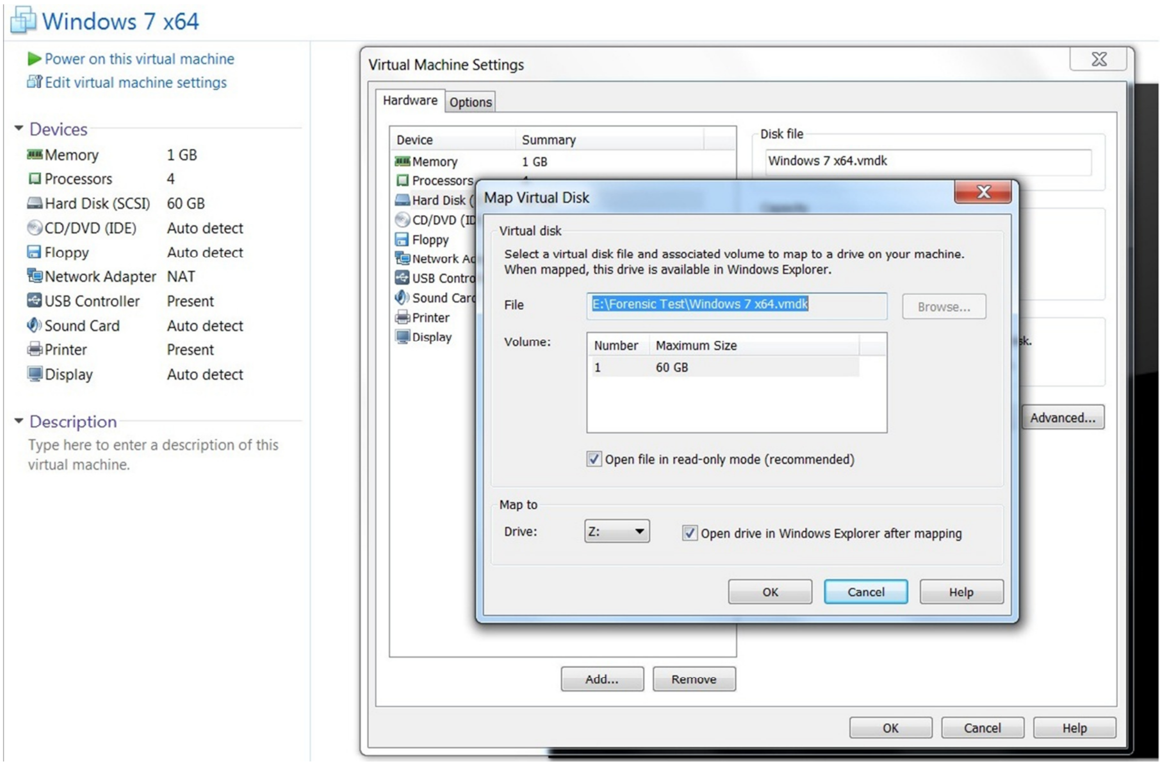
○ I will install the operating system later.

The virtual machine will be created with a blank hard disk.

Figure 4.1.2: The setup page of the new virtual machine wizard, it provides the option to install an OS on the image when it was created.

The initial image was built on a brand new 720GB IDE SATA hard drive. A backup of the image was copied to another hard drive for pilot testing.

The 60GB disk space initially assigned to the disk image was not pre-allocated, which means the virtual disk space was only allocated in advance. The space allocated for the virtual disk begins small and grow larger later to consume additional physical disk space as needed (VMware, 2012). Through pilot testing, the feature has proven to affect the accuracy of the experiment result. This is because unallocated disk space never existed in a virtual image created with this feature enabled. And according to the literature read, evidence might be retrieved from unallocated disk space.



Devices	
Memory	1 GB
Processors	4
Hard Disk (SCSI)	60 GB
CD/DVD (IDE)	Auto detect
Floppy	Auto detect
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Type here to enter a description of this virtual machine.

Disk file: Windows 7 x64.vmdk

Virtual disk

Select a virtual disk file and associated volume to map to a drive on your machine. When mapped, this drive is available in Windows Explorer.

File: E:\Forensic Test\Windows 7 x64.vmdk

Volume:

Number	Maximum Size
1	60 GB

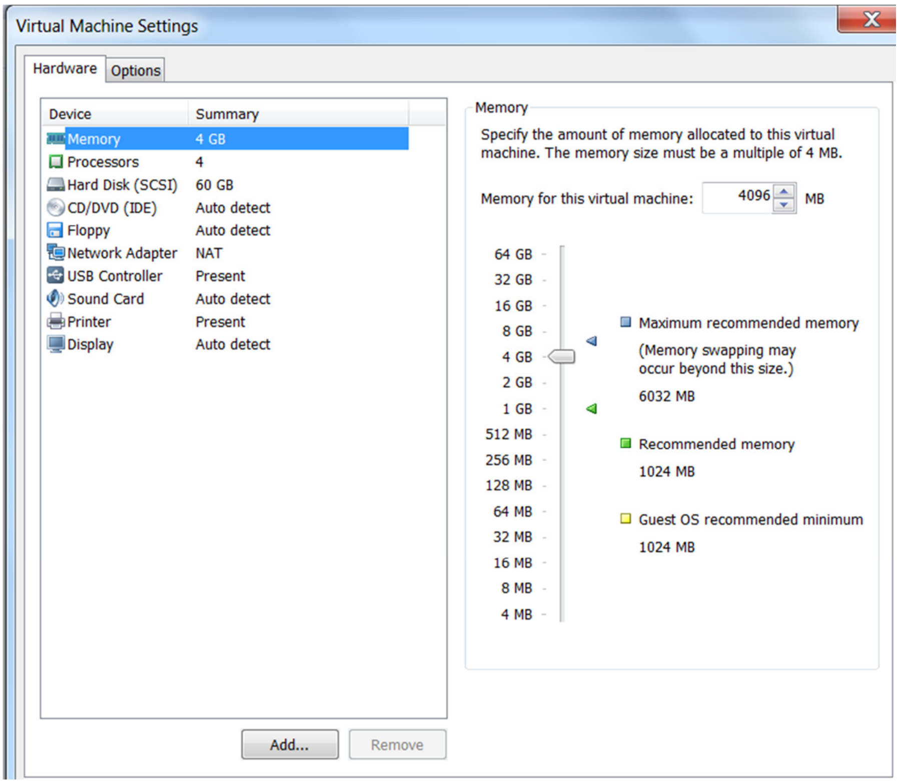
☑ Open file in read-only mode (recommended)

Map to

Drive: Z: ☑ Open drive in Windows Explorer after mapping

Figure 4.1.3: 60GB disk space was assigned to the virtual image and named Windows_7_x64.vmdk.

Therefore another technique has been used to convert the disk image into a 60GB pre-allocated disk image which created an unallocated disk space on the virtual image. The detail of the technique is described in the pilot testing section 4.2.



Device	Summary
Memory	4 GB
Processors	4
Hard Disk (SCSI)	60 GB
CD/DVD (IDE)	Auto detect
Floppy	Auto detect
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Memory

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

Memory for this virtual machine: 4096 MB

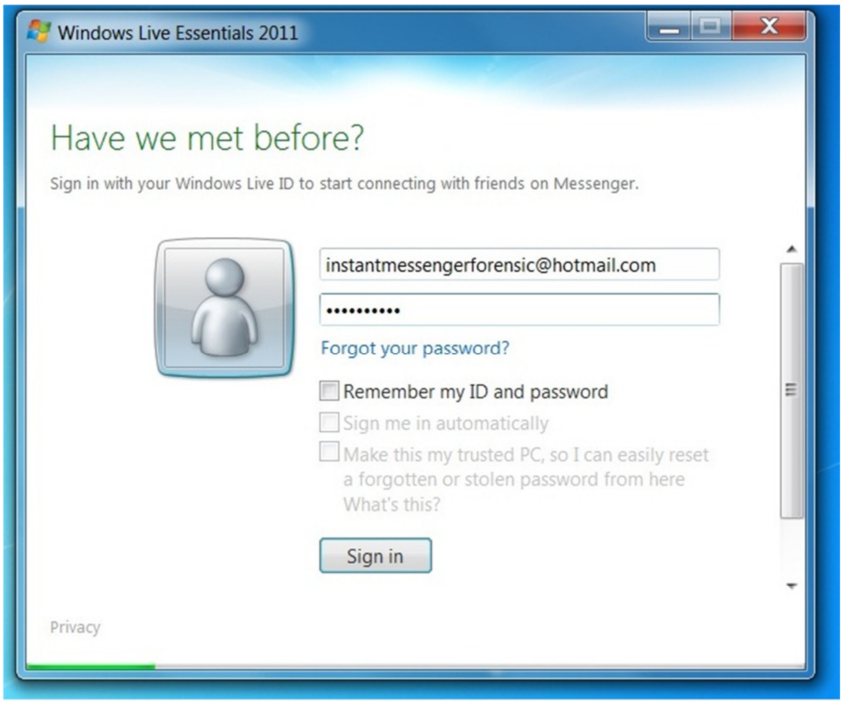
🟦 Maximum recommended memory
(Memory swapping may occur beyond this size.)
6032 MB

🟩 Recommended memory
1024 MB

🟨 Guest OS recommended minimum
1024 MB

Figure 4.1.4: Memory of the virtual machine can be adjusted after the installation but requires the restart of the virtual machine.

After the image has been setup, Microsoft Window Live Messenger 2011 (build 15.4.3538.513) was installed on the virtual machine and another test machine across the internet. Two Live messenger accounts instantmessengerforensic@hotmail.com and forensictester1@hotmail.com were also created for the experiment. The Windows live messenger launched in the virtual machine was login with account instantmessengerforensic@hotmail.com account as shown in figure 4.1.5 and will be called Machine-A in the experiment. The other account forensictester1@hotmail.com was used to login from another machine and will be called Machine-B. Machine-B was controlled by my assistance throughout the experiment.


Windows Live Essentials 2011

Have we met before?

Sign in with your Windows Live ID to start connecting with friends on Messenger.

instantmessengerforensic@hotmail.com

••••••••••

Forgot your password?

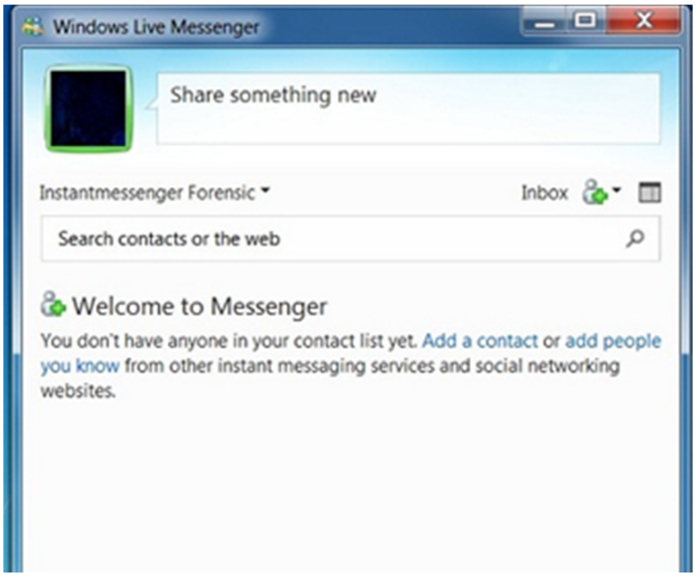
□ Remember my ID and password

□ Sign me in automatically

□ Make this my trusted PC, so I can easily reset a forgotten or stolen password from here What's this?

Figure 4.1.5: Initial login screen of Window live messenger 2011.

After the login information has been verified with the Microsoft live messenger server, the user was allowed to access the main Window live messenger operation interface as shown in figure 4.1.6. The main operation area contains a dialogue box located at the top of the interface and initially it contains the message 'Share something new'.


Windows Live Messenger

Share something new

Instantmessenger Forensic

Welcome to Messenger

You don't have anyone in your contact list yet. Add a contact or add people you know from other instant messaging services and social networking websites.

Figure 4.1.6: The main operation screen of Window live messenger 2011.

The primary function of the dialogue box was to allow the user to share a personalised message that can be viewed by any other parties in the user's contact list. Previous case studies show that the personalised message may provide useful evidence. Therefore the personalised message was in the scope of the experiment. The user was also allowed to share their online status with other users in their contact list. There were four different status allowed in Window live messenger 2011 as shown in figure 4.1.7. Users were allowed to choose between 'Available', 'Busy', 'Away' and 'Appear offline'.

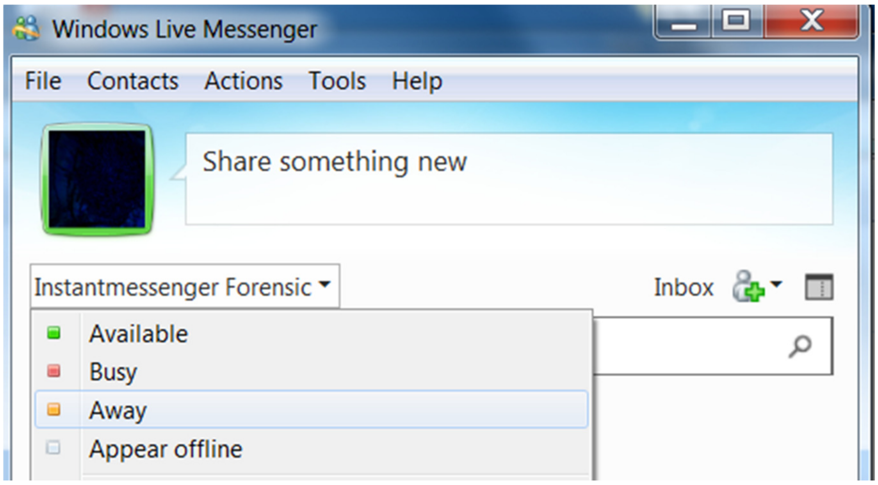
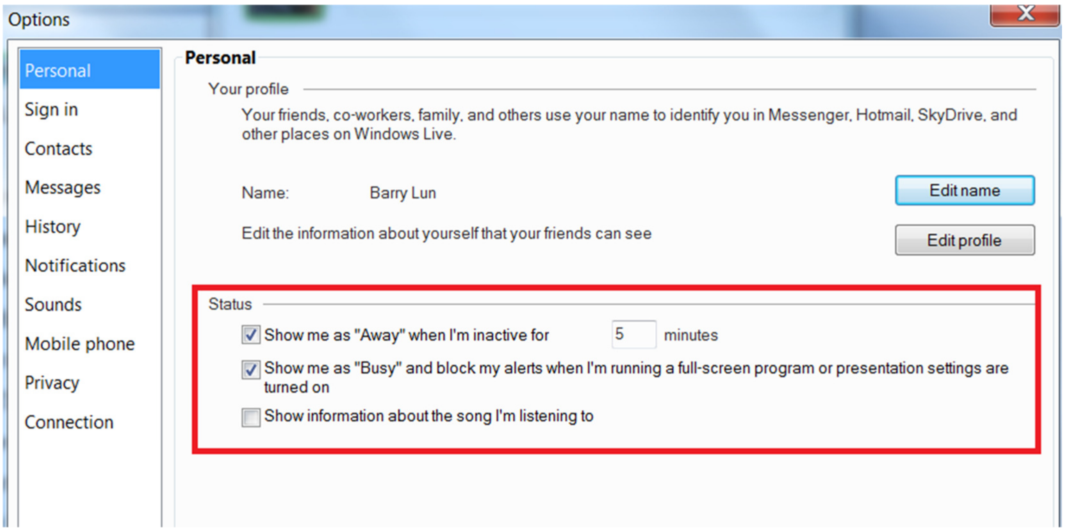


Figure 4.1.7: Users were allowed to choose between four online statuses from the drop down menu.

From previous case studies, a messenger might keep a record of time when the online status has been changed. The information might be used as an evidence to show when the user has returned to the keyboard from away status. Figure 4.1.8 shows the default online status setting for Microsoft live messenger 2011. By default, the online status will automatically change to 'Away' if the user has been inactive for five minutes. Through testing, any keyboard or mouse movement would reset the counter. The next step is to change the option on how conversation history was recorded. By default, the messenger was not keeping any conversation history itself. In order the test the function of Belkasoft Evidence Centre, I have enabled the option to keep a conversation history by ticking the checkbox next to 'Automatically save my conversation' which allows the messenger to save the conversation history in the default location as shown in figure 4.1.9.



Personal

Your profile

Your friends, co-workers, family, and others use your name to identify you in Messenger, Hotmail, SkyDrive, and other places on Windows Live.

Name: Barry Lun

Edit the information about yourself that your friends can see

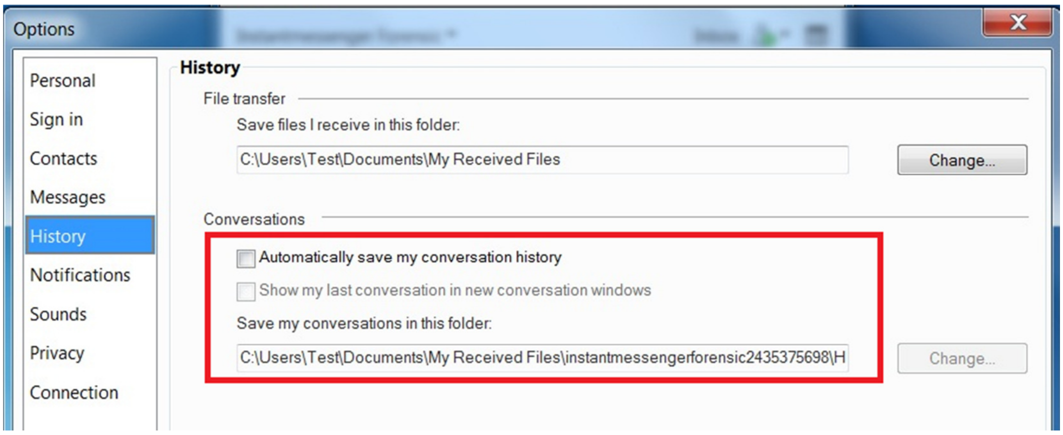
Status

☑ Show me as "Away" when I'm inactive for 5 minutes

☑ Show me as "Busy" and block my alerts when I'm running a full-screen program or presentation settings are turned on

□ Show information about the song I'm listening to

Figure 4.1.8: The red box in the screenshot highlighted the default setting to the online status of Microsoft live messenger 2011.



History

File transfer

Save files I receive in this folder:

C:\Users\Test\Documents\My Received Files

Conversations

□ Automatically save my conversation history

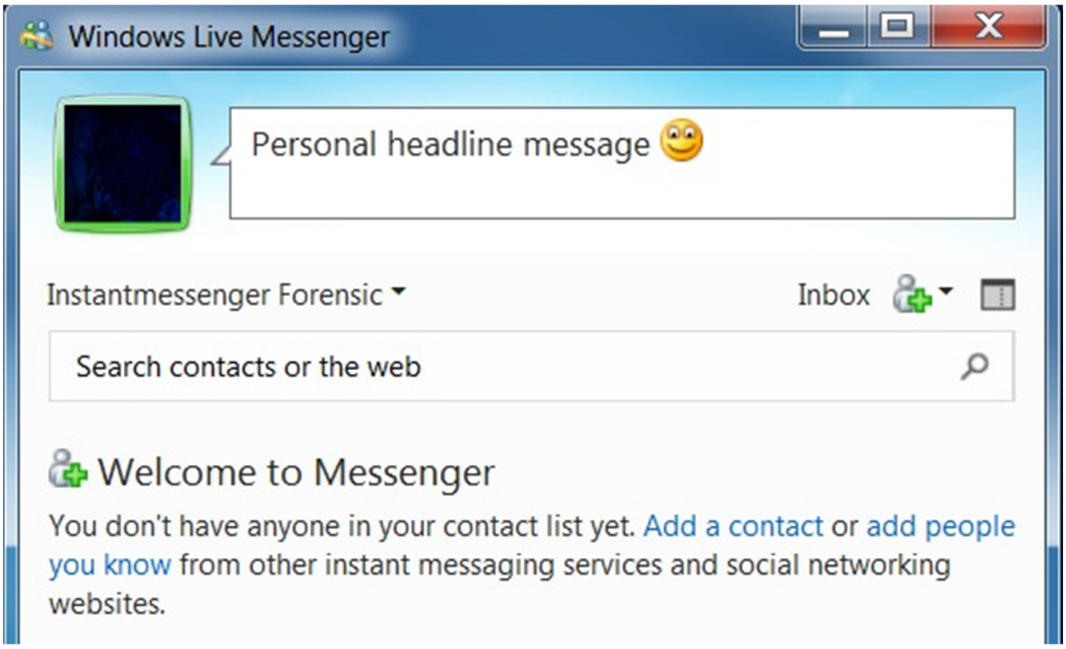
□ Show my last conversation in new conversation windows

Save my conversations in this folder:

C:\Users\Test\Documents\My Received Files\instantmessengerforensic2435375698\H

Figure 4.1.9: The red box in screenshot indicated the option to allow the messenger to save conversation history automatically.

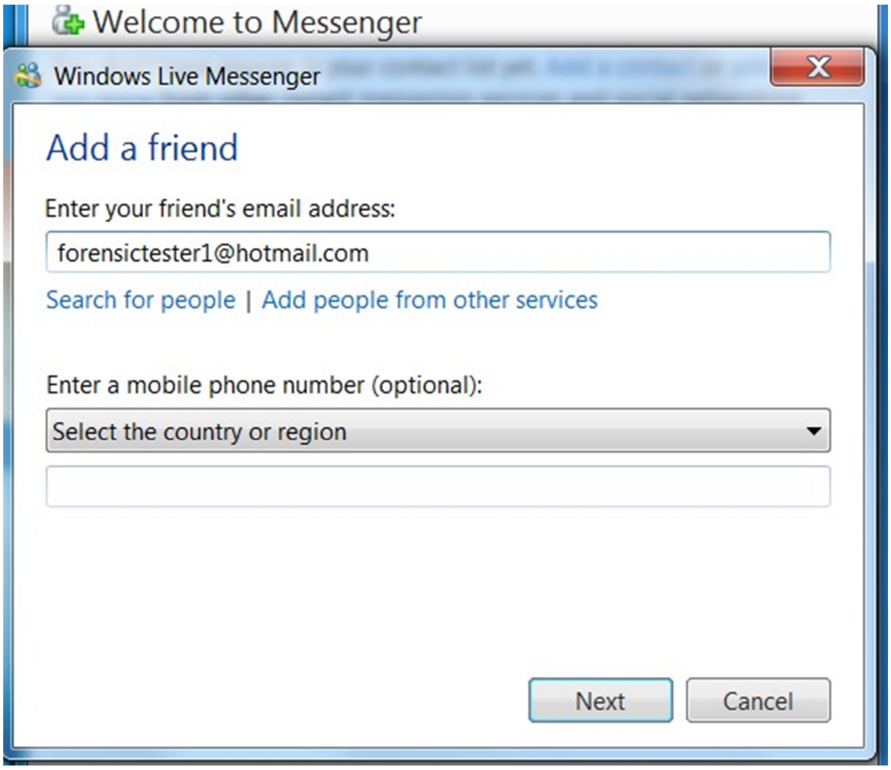
The simulation testing process was shown in between figure 4.1.10 to 4.1.15. The first step was changing the personalised message from ‘Share something new’ into ‘Personal headline message ☺’ in Machine-A as shown in figure 4.1.10. Then I have sent a friend request to Machine-B and requested my assistance to accept the request. After the screen name of Machine-B was added to the friend list of Machine-A, I have initiated a conversation from Machine-A through to Machine-B over a chat window as shown in figure 4.1.12.


Windows Live Messenger
Personal headline message
Instantmessenger Forensic
Inbox
Search contacts or the web
Welcome to Messenger

You don't have anyone in your contact list yet. Add a contact or add people you know from other instant messaging services and social networking websites.

Figure 4.1.10: Manually changing the personalised messenger.

Followed by the conversation, other functions of the Windows live messenger 2011 have been tested, a text file sample.txt was created and sent from Machine-A then received by Machine-B. A video call has been initiated from Machine-A for a duration of 5 seconds and was hung up by Machine-A itself (See figure 4.1.13).



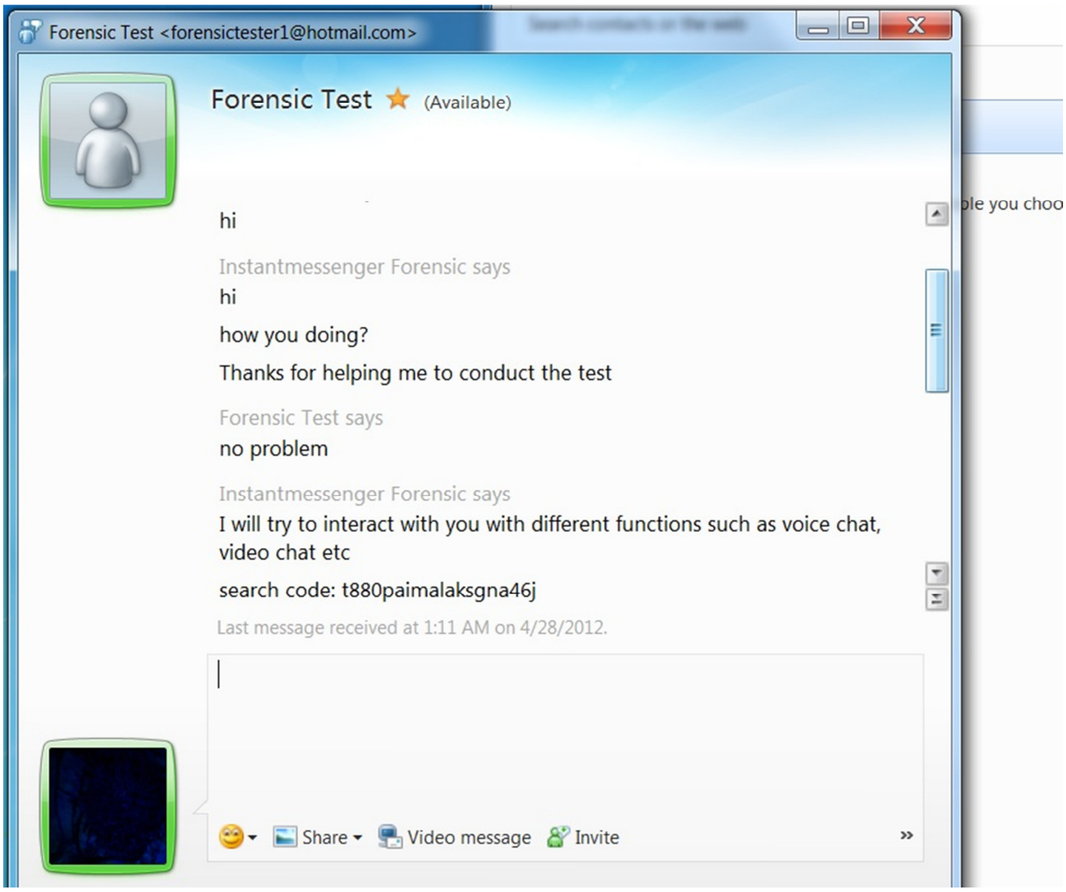
Enter your friend's email address:

forensictester1@hotmail.com

Enter a mobile phone number (optional):

Select the country or region

Figure 4.1.11: Friend request was about to be sent to the other testing account.



Forensic Test <forensictester1@hotmail.com>

Forensic Test ★ (Available)

hi

Instantmessenger Forensic says

hi

how you doing?

Thanks for helping me to conduct the test

Forensic Test says

no problem

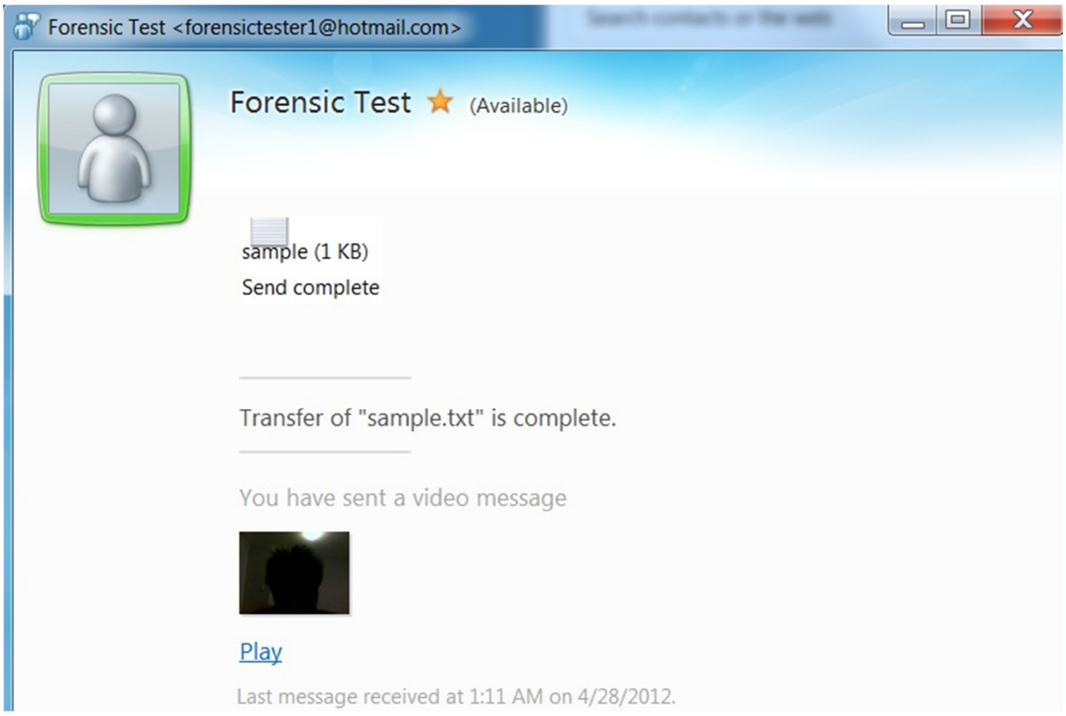
Instantmessenger Forensic says

I will try to interact with you with different functions such as voice chat, video chat etc

search code: t880paimalaksgna46j

Last message received at 1:11 AM on 4/28/2012.

Figure 4.1.12: Conversation between the two test parties



Forensic Test <forensictester1@hotmail.com>

Forensic Test ★ (Available)

sample (1 KB)

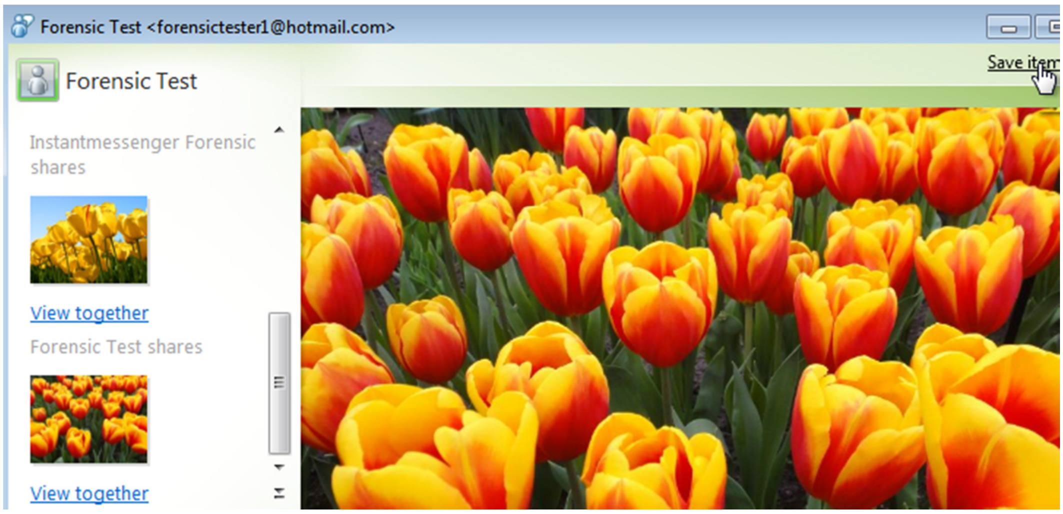
Send complete

Transfer of "sample.txt" is complete.

You have sent a video message

Last message received at 1:11 AM on 4/28/2012.

Figure 4.1.13: Simulation of file transfer and video call.


Forensic Test <forensictester1@hotmail.com>

Forensic Test

Instantmessenger Forensic shares

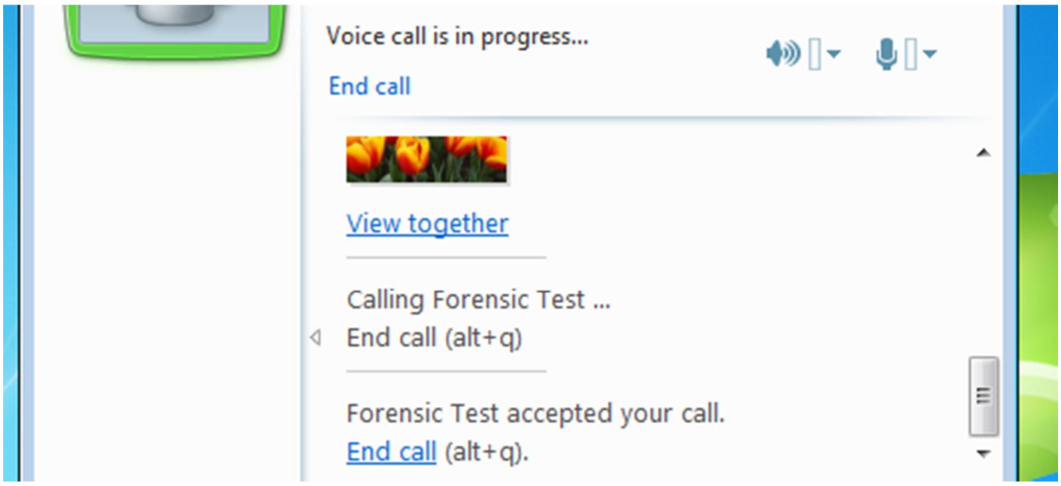
View together

Forensic Test shares

View together

Figure 4.1.14: Picture sent from Machine-B was saved into the system drive of Machine-A.

The personalised message has been changed to ‘I am away’ and a picture was shared from Machine-A to Machine-B but Machine-B did not require saving the picture to the machine. After that, I have requested my assistance to send a picture from Machine-B to Machine-A and I have saved the picture into the Windows Picture folder located in the system drive of the virtual image. The picture has been given a file name of ‘forensicpicture’ and was saved in .jpg format. A voice call was initiated from Machine-A and the call was accepted by Machine-B for a short period of time.


Voice call is in progress...

End call

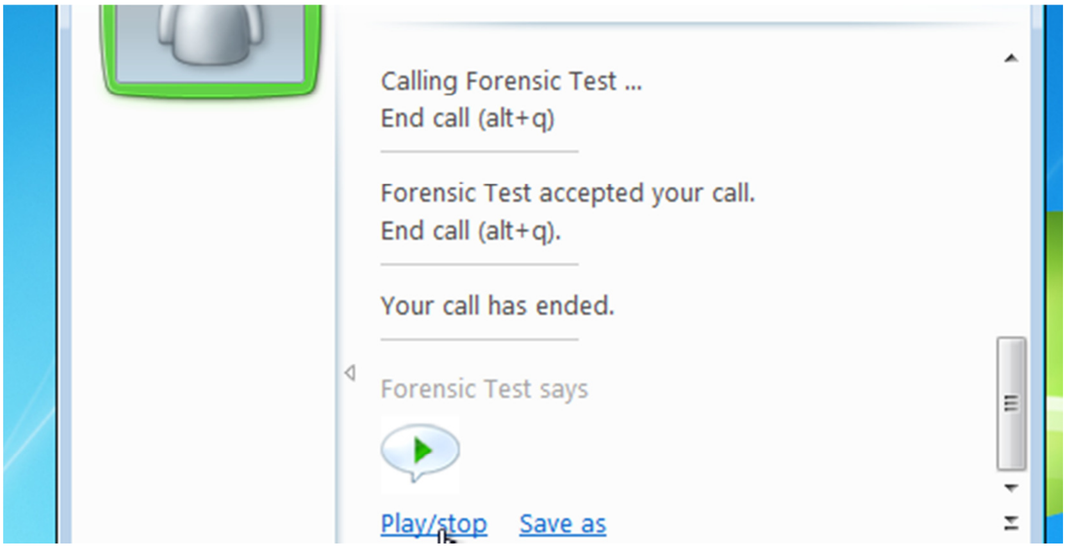
View together

Calling Forensic Test ...
End call (alt+q)

Forensic Test accepted your call.
End call (alt+q).

Figure 4.1.15: Voice call from Machine-A to Machine-B.

The last function tested was the voice message. I have requested my assistance to record a short voice message and send to Machine-A. The voice message has been received, played and saved into the system drive.



Calling Forensic Test ...
End call (alt+q)

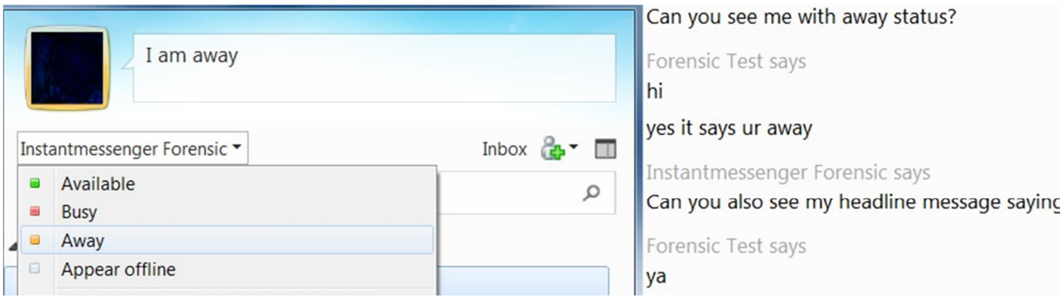
Forensic Test accepted your call.
End call (alt+q).

Your call has ended.

Forensic Test says

Figure 4.1.16: Voice message from Machine-A to Machine-B.

After testing the common functions of Window live messenger 2011, the online status of Machine-A was left ideal for 5 minutes and the online status automatically set to ‘Away’. The experiment shows that the Window live messenger will return the online status to ‘Available’ once any keyboard or mouse movement has been detected. Some conversation between the two test machines took place after the change in status as shown in figure 4.1.17.



I am away

Instantmessenger Forensic

Can you see me with away status?

Forensic Test says
hi
yes it says ur away

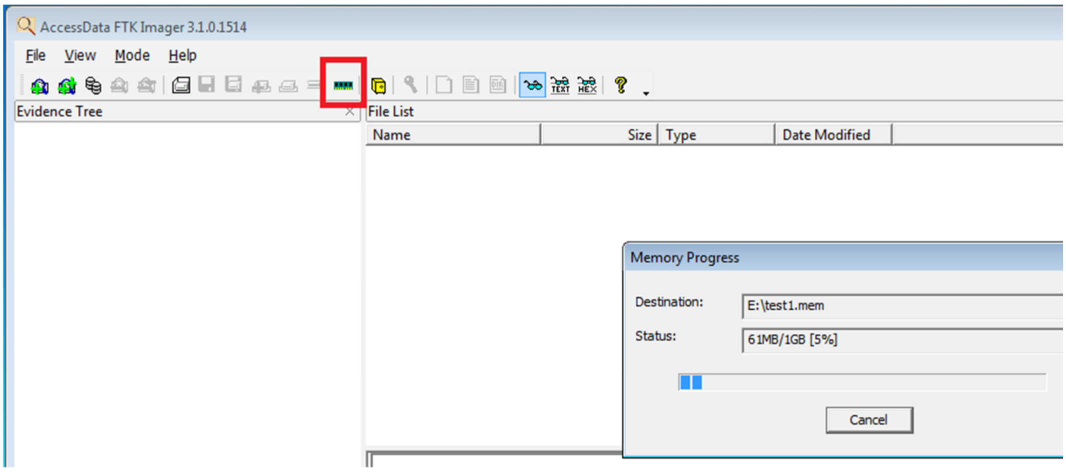
Instantmessenger Forensic says
Can you also see my headline message saying

Forensic Test says
ya

Figure 4.1.17: Change of online status

The chat windows and the messenger were closed on Machine-A and the next step is to collect information from the random access memory.

Previously FTK Imager was installed into a flash drive. The drive was plugged into the USB and connected to Machine-A. The FTK Imager interface was shown in figure 4.1.18. The memory dump can be done by simply clicking the icon inside the red square marked in the figure 4.1.18 and the data stored in the random access memory was written onto the test1.mem file stored in the flash drive. It is important to ensure that the flash drive have sufficient storage space to capture the data from the RAM. Through testing, 1GB of RAM will generate a memory file of exactly the same size on the flash drive.



Destination: E:\test1.mem

Status: 61MB/1GB [5%]

Figure 4.1.18: Interface of FTK Imager.

After the data from the RAM was fully dumped onto the flash drive, Machine-A has been turned into hibernate mode before shut down completely. Through information from the previous literature research (chapter 2), there is a chance that information from instant messenger could be stored in the hibernation file if the machine has been hibernated.

The next step was to create a forensic copy of the virtual image using FTK Imager file as shown in figure 4.1.19. The image was called named ‘test.dd’ and was created directly from the virtual image of Machine-A. The fragment size was set to 0 to ensure FTK did not divide the forensic drive into multiple fragments which simplified the simulation and the compression was set to 0 to reduce time to create the forensic copy of Machine-A. Generally a write blocker is required to be used to create the forensic copy from a seized drive. The purpose was to ensure the integrity of the seized drive. However a write-blocker is not required for the simulation testing because the function of FTK

Imager here was only to convert the VMware image into a forensic image that can be recognised by the Belkasoft Evidence Centre. Figure 4.1.20 shows that the process to create the forensic copy took around 24minutes to complete.

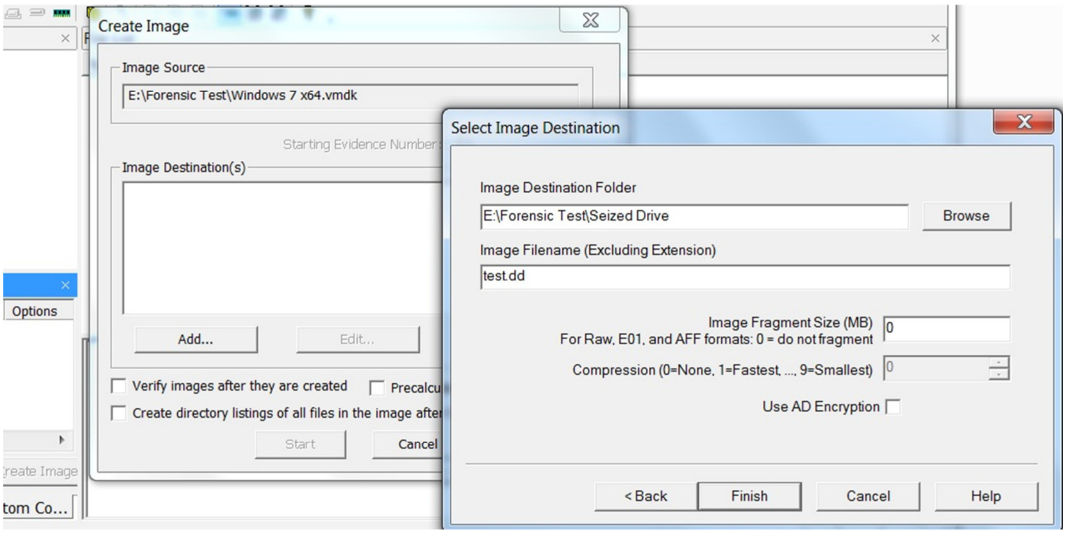


Image Source: E:\Forensic Test\Windows 7 x64.vmdk

Starting Evidence Number

Image Destination(s)

□ Verify images after they are created □ Precalcu

□ Create directory listings of all files in the image after

Image Destination Folder: E:\Forensic Test\Seized Drive

Image Filename (Excluding Extension): test.dd

Image Fragment Size (MB) For Raw, E01, and AFF formats: 0 = do not fragment: 0

Compression (0=None, 1=Fastest, ..., 9=Smallest): 0

Use AD Encryption □

Figure 4.1.19: Simulate the process to create a forensic copy from Machine-A using FTK Imager.

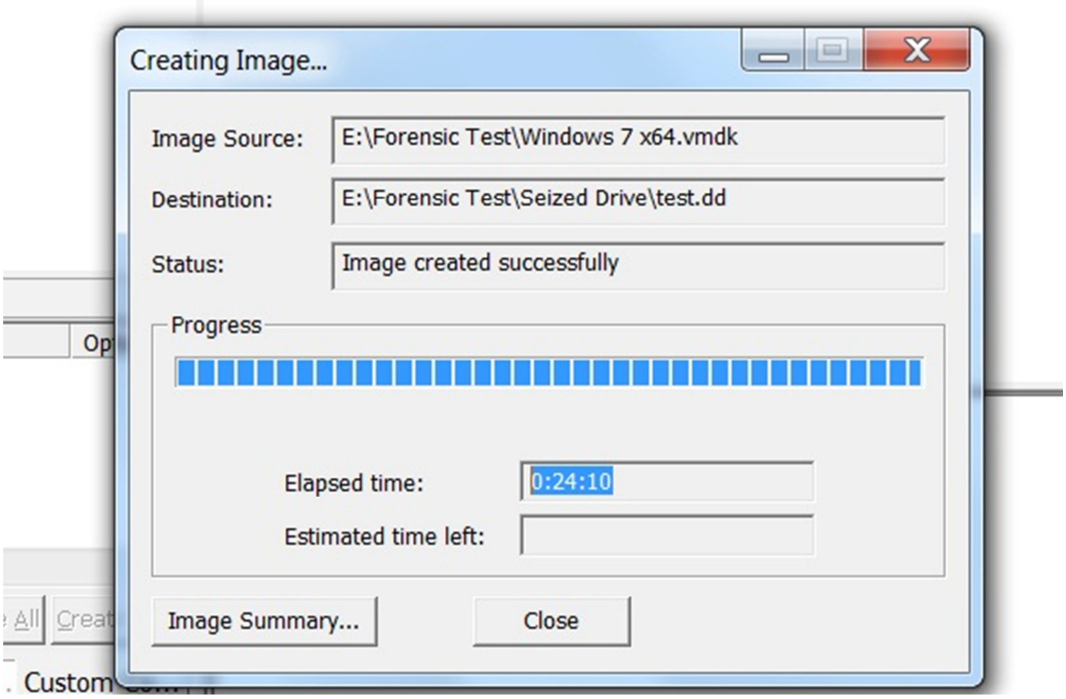


Image Source: E:\Forensic Test\Windows 7 x64.vmdk

Destination: E:\Forensic Test\Seized Drive\test.dd

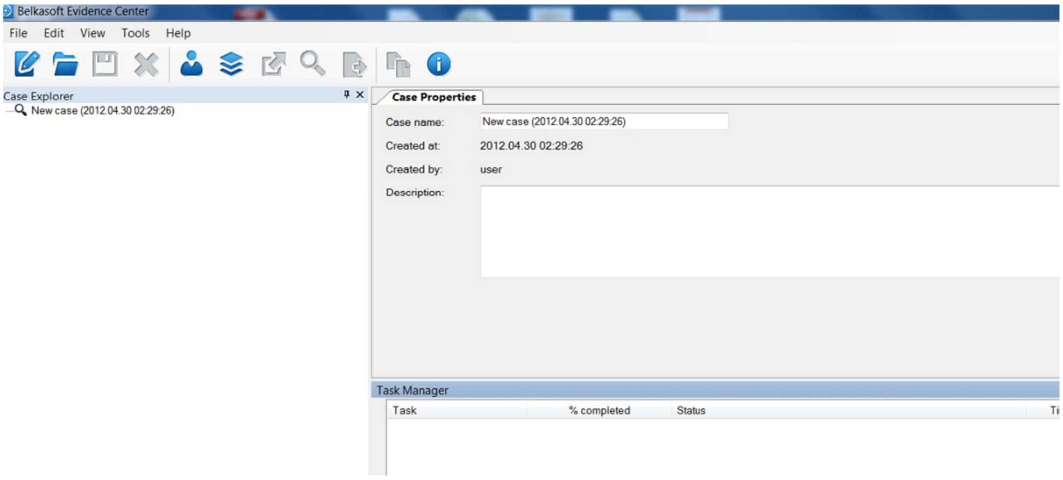
Status: Image created successfully

Elapsed time: 0:24:10

Estimated time left:

Figure 4.1.20: Process to create the forensic copy of a 60GB drive requires 24 minutes to complete.

Belkasoft Evidence Center version 3.8 build 336 was installed onto the system drive of my laptop. Figure 4.1.21 shows the interface of the application.



Case name: New case (2012.04.30 02:29:26)
Created at: 2012.04.30 02:29:26
Created by: user
Description:

Figure 4.1.21: Primary interface of the Belkasoft Evidence Center 3.8

After the testing was done, the copy of the virtual image prepared at the beginning was used to carry out testing on the scenario where the messenger did not enable the option to save the conversation history. The copied image was at the state when Windows 7 was installed initially and it did not contain any previous usage of instant messaging. The testing was carried out in exactly the same manner as shown above from Figure 4.1.5 to Figure 4.1.20 except the option in Figure 4.1.9 where the box to enable the option to save the conversation history was remained un-ticked. The scenario where a conversation history was not saved was described as the scenario of most cases in reality.

4.2 PILOT RUN

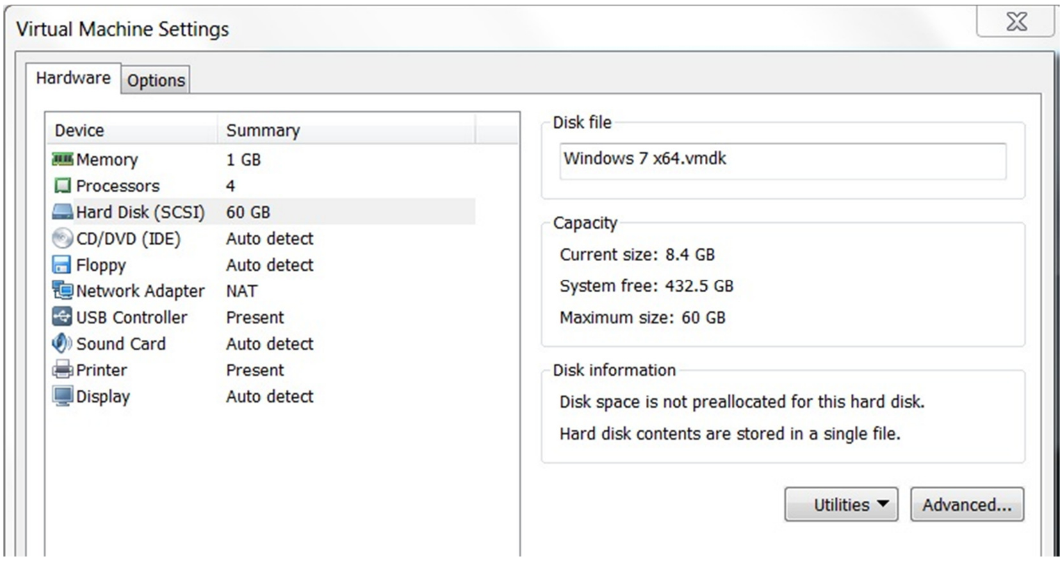
A series of pilot testing runs were carried out before the actual experiment was conducted. The pilot testing consisted of testing different vitalisation tools such as Microsoft Virtual PC, VMware Player 4.0 and VMware Workstation 4.0.2. The following issues were encountered during the pilot runs and several changes were made to the experiment setup and preparation to resolve the issues.

Issues with the Physical Workstation: The initial plan was to carry out the simulation using a physical laptop computer instead of virtual images. During the pilot run with a physical machine, I have found an excessive amount of noise (un-related data) due to previous usage of the laptop. In order to maintain the integrity of the data from the experiment, ideally the experiment should be carried out using a freshly built workstation. Alternative, the workstation has to be rebuilt as it is difficult to ensure data written on the hard drive has been completely removed. As stated in the security guide written by Canada Communications Security Establishment in 2006, some methods were able to ensure previous data cannot be retrieved, such as overwriting the entire hard disk with multiple layers of data or using equipment such as degaussing machinery (VMware, 2012). However the time required for conducting the experiment would be greatly increased.

Therefore the experiment was conducted by manipulating virtualisation technology. With the use of virtualisation, I was able to have duplicated copies of a fresh Window image on a previously unused hard drive for multiple trials of the experiment. The forensic examinations on each image were bounded only to the disk space allocated to each image which ensures the testing done on a virtual image will not affect the examination result from another virtual image.

Issue with VMware Player 4.0: Initially, VMware Player 4.0 was chosen to mount the virtual Window image for the experiment. However VMware Workstation 8.0 was found to be a better choice because VM Player does not offer the function to convert virtual image into pre-allocated disk from a dynamic disk (Artman), which was essential for the simulation to perform the task of searching evidence from unallocated disk space. Secondly, VM Workstation provided the function to capture video from the screen (Huhtinen, 2008, January 17) of the virtual environment, the function could be manipulated to review the experiment.

Issue with dynamic virtual disk space: The virtual image built for the experiment was assigned 60GB when it was being created. However the image file was found to have a size of 8.4GB. After some investigation, the problem was due to a feature of VMware where the virtual disk space was allocated in advance. The initial assigned disk space to the virtual image was shown in figure 4.2.0. Disk space was dynamically allocated to the image only when required (VMware, 2012).



Device	Summary
Memory	1 GB
Processors	4
Hard Disk (SCSI)	60 GB
CD/DVD (IDE)	Auto detect
Floppy	Auto detect
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Disk file

Windows 7 x64.vmdk

Capacity

Current size: 8.4 GB

System free: 432.5 GB

Maximum size: 60 GB

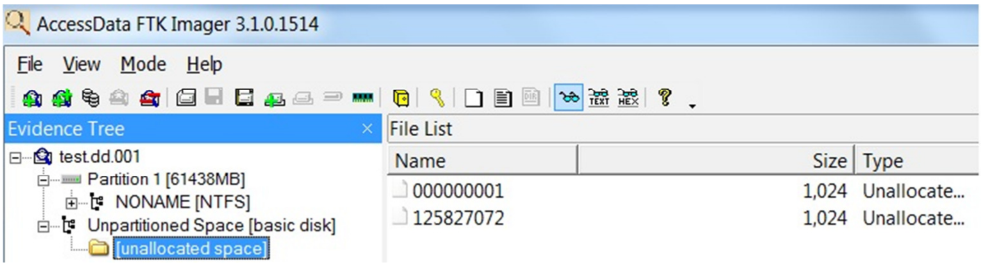
Disk information

Disk space is not preallocated for this hard disk.

Hard disk contents are stored in a single file.

Figure 4.2.0: Dynamic VMware hard disk image had an initial size of 8.4GB but was allocated to expand to up to 60GB

The image was mounted into FTK Imager as shown in figure 4.2.1 and found to have a 2MB unallocated disk space. The image was also mounted into Belkasoft Evidence Center but was unable to properly carry out a search on the unallocated disk space. The symptoms indicated the test result on unallocated disk space analysis might not be affected.



test.dd.001

Partition 1 [61438MB]

NONAME [NTFS]

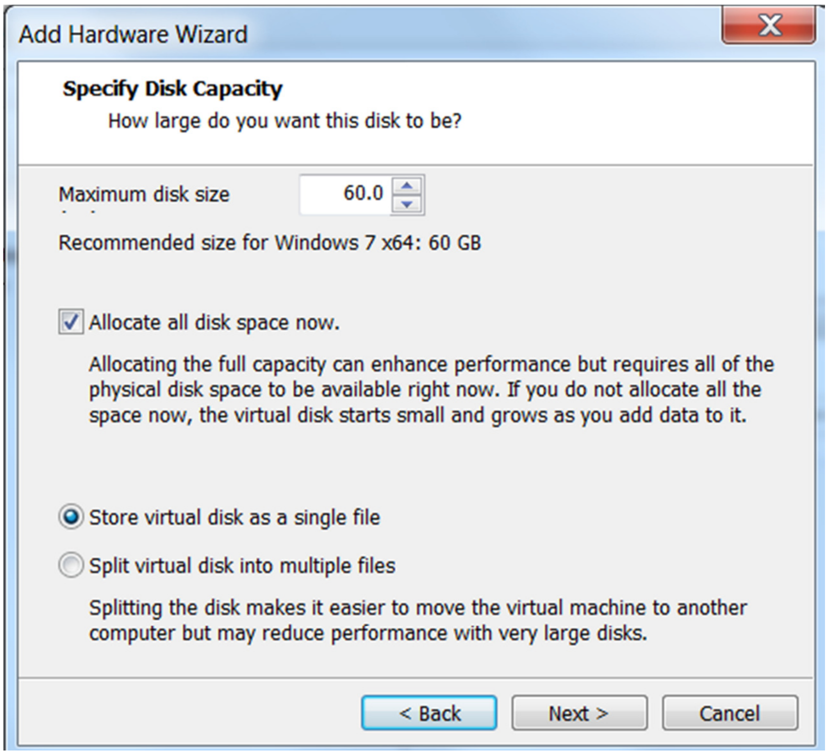
Unpartitioned Space [basic disk]

[unallocated space]

Name	Size	Type
000000001	1,024	Unallocate...
125827072	1,024	Unallocate...

Figure 4.2.1: Due to an early misconfiguration, the unallocated disk space only has a capacity of 2MB.

To ensure the disk space is pre-allocated, the option ‘Allocate all disk space now’ must be enabled when creating the virtual hard disk as shown in figure 4.2.2.



Add Hardware Wizard

Specify Disk Capacity

How large do you want this disk to be?

Maximum disk size 60.0

Recommended size for Windows 7 x64: 60 GB

☑ Allocate all disk space now.

Allocating the full capacity can enhance performance but requires all of the physical disk space to be available right now. If you do not allocate all the space now, the virtual disk starts small and grows as you add data to it.

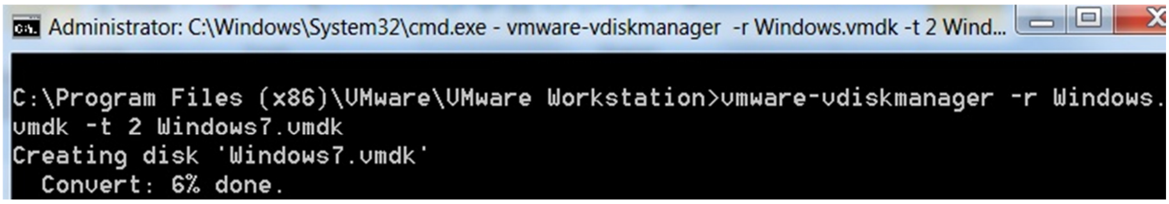
● Store virtual disk as a single file

○ Split virtual disk into multiple files

Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

Figure 4.2.2: Option to ensure the disk space is pre-allocated in VM

There is no option in VMware interface to convert an expandable virtual hard disk into one with pre-allocated disk space on an image. A more complicated procedure was required for the conversion. The procedure was to enter cmd (window command processor) in admin mode, then using the command as shown in Figure 4.2.3 to convert the image into one with pre-allocated disk space.



Administrator: C:\Windows\System32\cmd.exe - vmware-vdiskmanager -r Windows.vmdk -t 2 Wind...

```
C:\Program Files (x86)\VMware\VMware Workstation>vmware-vdiskmanager -r Windows.
vmdk -t 2 Windows7.vmdk
Creating disk 'Windows7.vmdk'
  Convert: 6% done.
```

Figure 4.2.3: Command to convert test image from dynamic disk space into one with pre-allocated disk space.

Issue with Window Crash Dump: Initially the method to manually initiate a Windows crash dump has been considered to collect data stored from the random access memory. A crash dump was a function of Windows that was designed to collect the information stored in the random access memory in the event of a system failure. The data collected from the crash dump will be saved to a file for analysis. In order to manually crash the window system and initiate the crash dump, some modification in the Windows registry was required. However through testing, Windows built on VMware virtual image did not appear to support the method to manually crash the system. The method was also considered not ideal to used for my simulation after a discussion with Belkasoft support engineer, the reason was due to the method can easily affect the integrity of the data stored in the computer system in a real life scenario and the crash dump will consume a portion of unallocated space in the system drive when creating the data dump file. Therefore FTK Imager is suggested to be used in the experiment to perform a memory dump from the test machine.

4.3 EXPERIMENTAL RESULTS

The first test was to examine if Belkasoft Evidence Center was able to retrieve information stored in Window live messenger by default such as a saved conversation history. The test was necessary as each default had to be set and tested before the tool was run each time. This was done by opening a new case in the application and select 'MSN/Live Messenger' as shown in figure 4.3.0.

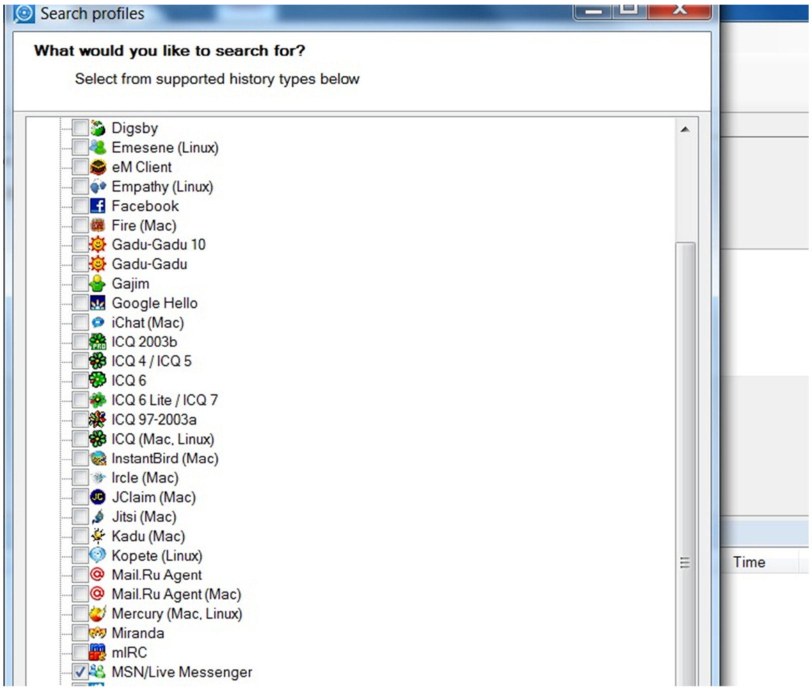
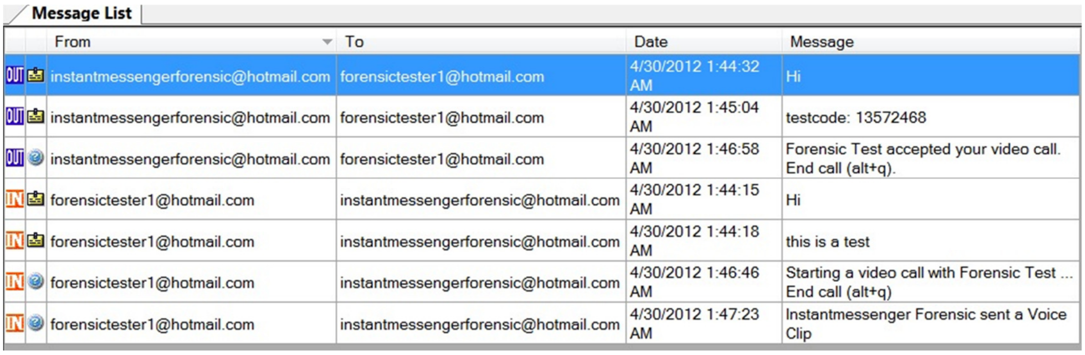


Figure 4.3.1: Selecting MSN/Live Messenger from the menu.

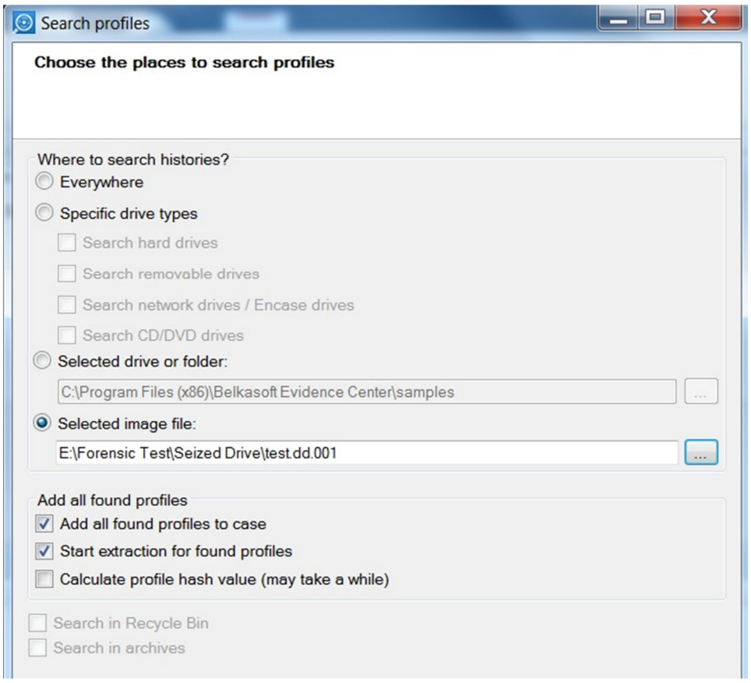
The next screen was shown in figure 4.3.1, the application allowed users to search for evidence from different devices. Here I have selected the forensic copy created earlier by FTK Imager. I did not enable the option to calculate hash value in order to save time as it was not required for the experiment. Figure 4.3.2 presented the search result from the basic search function. The screenshot showed that the tool was able to provide information such as the date and time when the message was sent or received. There was a clear 'OUT' and 'IN' icon to indicate if the message was received or sent out by the messenger. The MSN account (email address) of the message sender and receiver was shown, the content of the conversation has been achieved and there was indications that when a video call was initiated and ended. The list also provided information on when a voice clip was sent.



Message List

	From	To	Date	Message
OUT	instantmessengerforensic@hotmail.com	forensictester1@hotmail.com	4/30/2012 1:44:32 AM	Hi
OUT	instantmessengerforensic@hotmail.com	forensictester1@hotmail.com	4/30/2012 1:45:04 AM	testcode: 13572468
OUT	instantmessengerforensic@hotmail.com	forensictester1@hotmail.com	4/30/2012 1:46:58 AM	Forensic Test accepted your video call. End call (alt+q).
IN	forensictester1@hotmail.com	instantmessengerforensic@hotmail.com	4/30/2012 1:44:15 AM	Hi
IN	forensictester1@hotmail.com	instantmessengerforensic@hotmail.com	4/30/2012 1:44:18 AM	this is a test
IN	forensictester1@hotmail.com	instantmessengerforensic@hotmail.com	4/30/2012 1:46:46 AM	Starting a video call with Forensic Test ... End call (alt+q)
IN	forensictester1@hotmail.com	instantmessengerforensic@hotmail.com	4/30/2012 1:47:23 AM	Instantmessenger Forensic sent a Voice Clip

Figure 4.3.2: Search result via the basic search function.



Search profiles

Choose the places to search profiles

Where to search histories?

○ Everywhere

○ Specific drive types

□ Search hard drives

□ Search removable drives

□ Search network drives / Encase drives

□ Search CD/DVD drives

○ Selected drive or folder:

C:\Program Files (x86)\Belkasoft Evidence Center\samples

● Selected image file:

E:\Forensic Test\Seized Drive\test.dd.001

Add all found profiles

☑ Add all found profiles to case

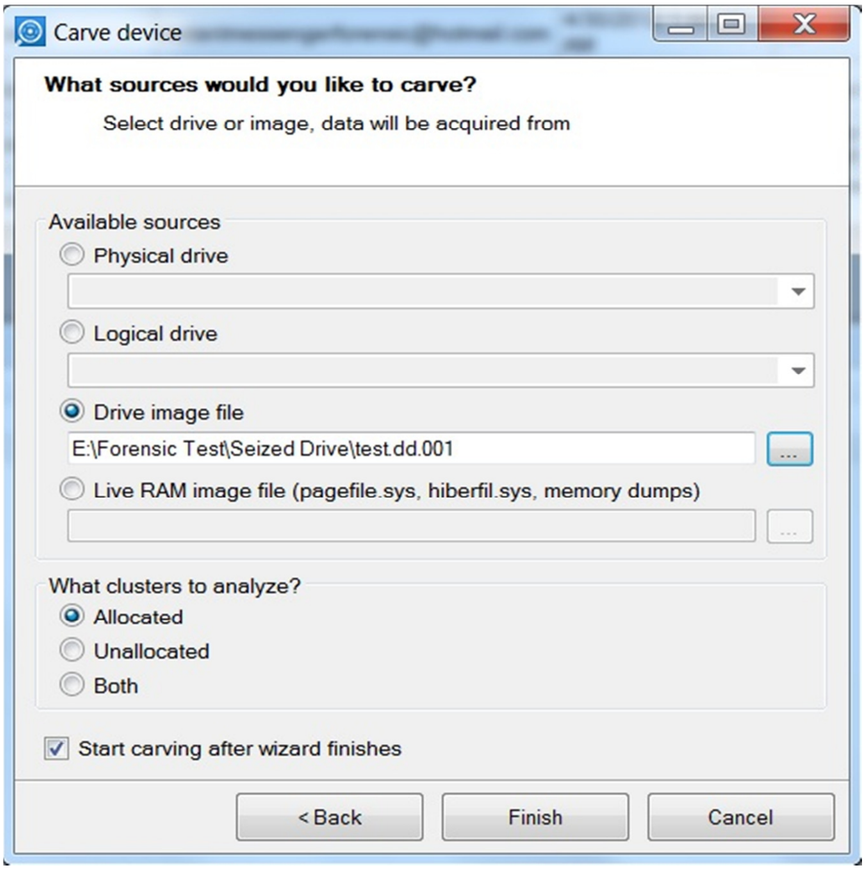
☑ Start extraction for found profiles

□ Calculate profile hash value (may take a while)

□ Search in Recycle Bin

□ Search in archives

Figure 4.3.3: Belkasoft Evidence Center saved information by default



Carve device [redacted]

What sources would you like to carve?

Select drive or image, data will be acquired from

Available sources

○ Physical drive

○ Logical drive

● Drive image file

E:\Forensic Test\Seized Drive\test.dd.001

○ Live RAM image file (pagefile.sys, hiberfil.sys, memory dumps)

What clusters to analyze?

● Allocated

○ Unallocated

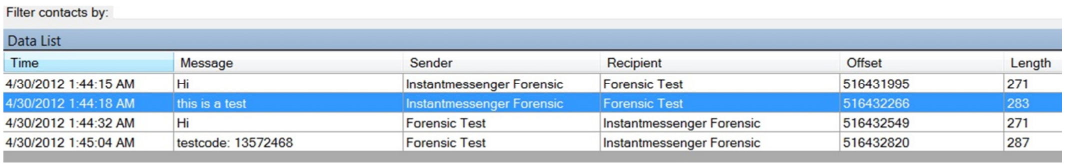
○ Both

☑ Start carving after wizard finishes

Figure 4.3.4: Using Carve device function to search for information from the allocated disk space.

The next step was to search for information from the allocated drive. It was done by using the 'Carve device' function as shown in figure 4.3.4. I have only targeted the search on the allocated space in order to distinguish results between information retrieved from allocated space and unallocated space.

The search result of allocated disk space was shown in figure 4.3.5, I was able to retrieve date and time of conversation, content of message, screen name of sender and recipient of message, the offset and length of the message stored on the allocated disk.



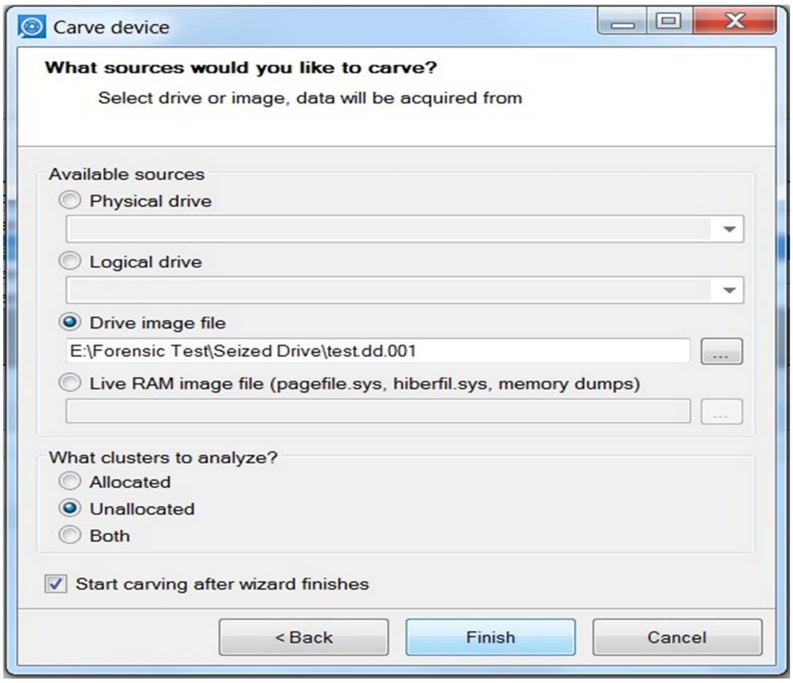
Filter contacts by:

Data List

Time	Message	Sender	Recipient	Offset	Length
4/30/2012 1:44:15 AM	Hi	Instantmessenger Forensic	Forensic Test	516431995	271
4/30/2012 1:44:18 AM	this is a test	Instantmessenger Forensic	Forensic Test	516432266	283
4/30/2012 1:44:32 AM	Hi	Forensic Test	Instantmessenger Forensic	516432549	271
4/30/2012 1:45:04 AM	testcode: 13572468	Forensic Test	Instantmessenger Forensic	516432820	287

Figure 4.3.5: Search result from the allocated disk space.

The search on unallocated disk space was done in a similar procedure as the allocated disk space search. Carve device function was selected but the option on ‘What clusters to analyze?’ was changed to ‘Unallocated’ as shown in figure 4.3.6.



Carve device

What sources would you like to carve?

Select drive or image, data will be acquired from

Available sources

○ Physical drive

○ Logical drive

● Drive image file

E:\Forensic Test\Seized Drive\test.dd.001

○ Live RAM image file (pagefile.sys, hiberfil.sys, memory dumps)

What clusters to analyze?

○ Allocated

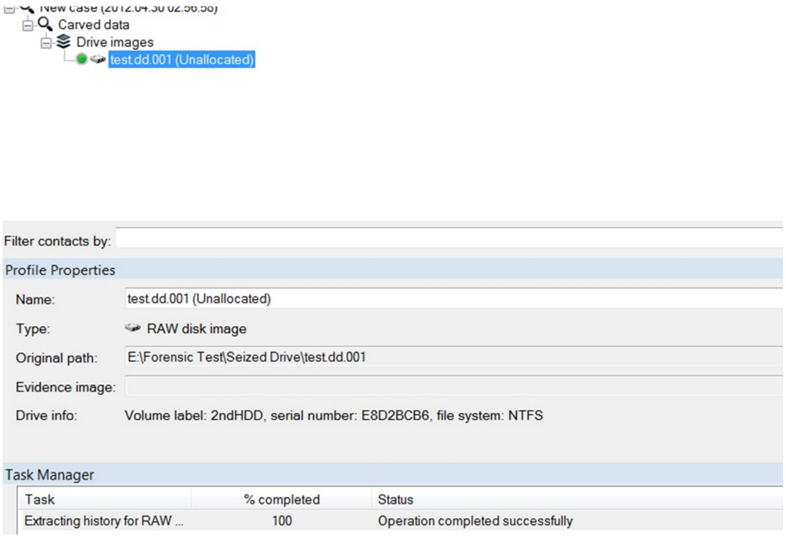
● Unallocated

○ Both

☑ Start carving after wizard finishes

Figure 4.3.6: Using Carve device function to search for information from the unallocated disk space.

The search result on the unallocated disk space is presented in figure 4.3.7. The result indicated that nothing was found from the unallocated disk space.



New case (2012.04.30 02.56.58)
Carved data
Drive images
test.dd.001 (Unallocated)

Filter contacts by:

Profile Properties

Name: test.dd.001 (Unallocated)

Type: RAW disk image

Original path: E:\Forensic Test\Seized Drive\test.dd.001

Evidence image:

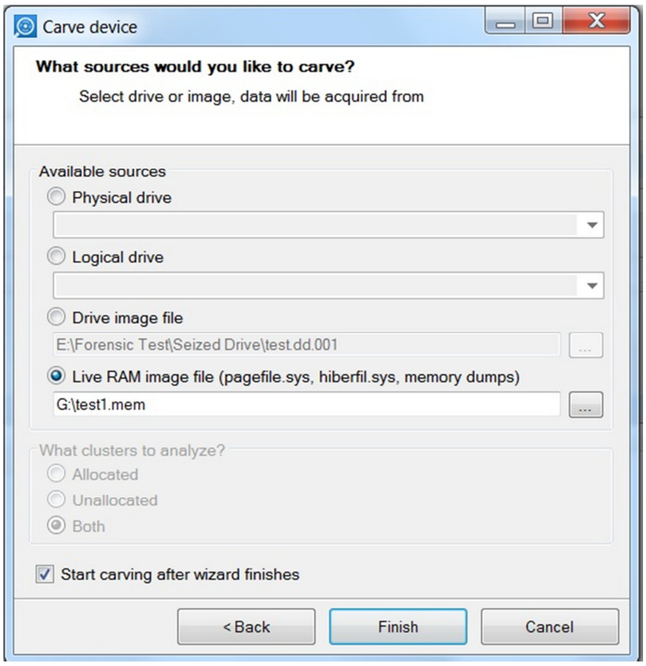
Drive info: Volume label: 2ndHDD, serial number: E8D2BCB6, file system: NTFS

Task Manager

Task	% completed	Status
Extracting history for RAW ...	100	Operation completed successfully

Figure 4.3.7: Search result from unallocated disk space.

The next area to search was the RAM image generated from memory dump using FTK Imager. With the carve device function, I was able to direct the Evidence Center to locate the memory data file test1.mem stored in G: (flash drive) as shown in figure 4.3.8.



Carve device

What sources would you like to carve?

Select drive or image, data will be acquired from

Available sources

○ Physical drive

○ Logical drive

○ Drive image file

E:\Forensic Test\Seized Drive\test.dd.001

● Live RAM image file (pagefile.sys, hiberfil.sys, memory dumps)

G:\test1.mem

What clusters to analyze?

○ Allocated

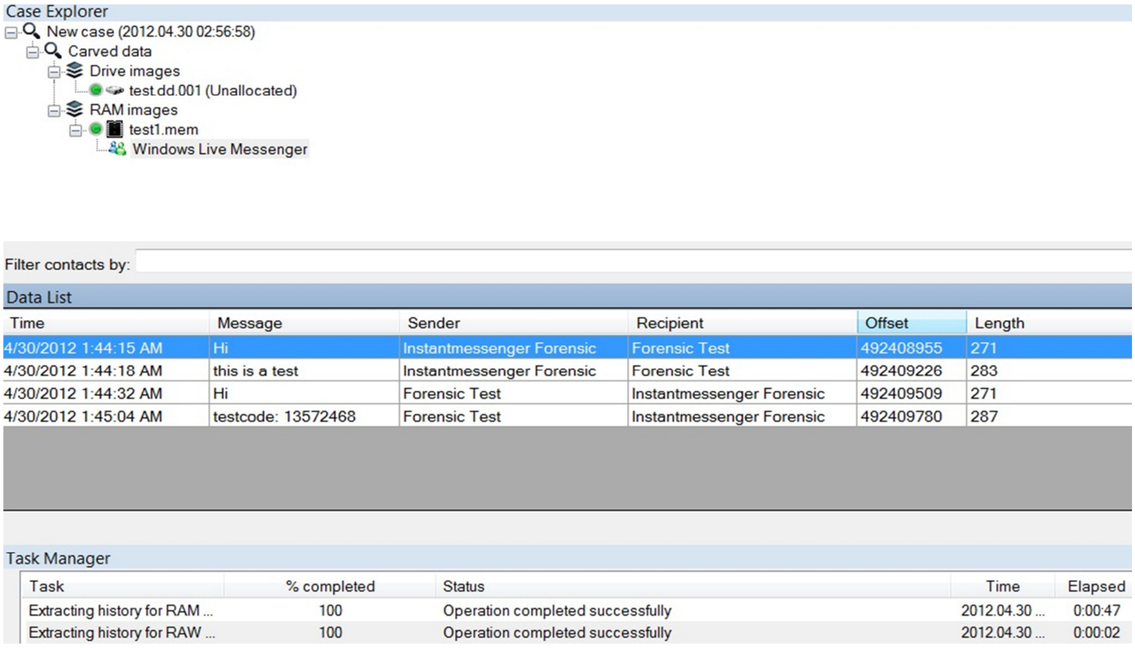
○ Unallocated

● Both

☑ Start carving after wizard finishes

Figure 4.3.8: Search for information from the RAM image.

The search result from the memory dump file was shown in figure 4.3.9. The result indicated that the Evidence Center have retrieved some information from the RAM of Machine-A. The information included the data and time of the message, the content of the message, the screen name of the sender and receipent, the offset and length the offset and length of the message. The evidence found was exactly the same as the finding from the search in allocated disk space.



Case Explorer

- New case (2012.04.30 02:56:58)
  - Carved data
    - Drive images
      - test.dd.001 (Unallocated)
    - RAM images
      - test1.mem
        - Windows Live Messenger

Filter contacts by:

Data List

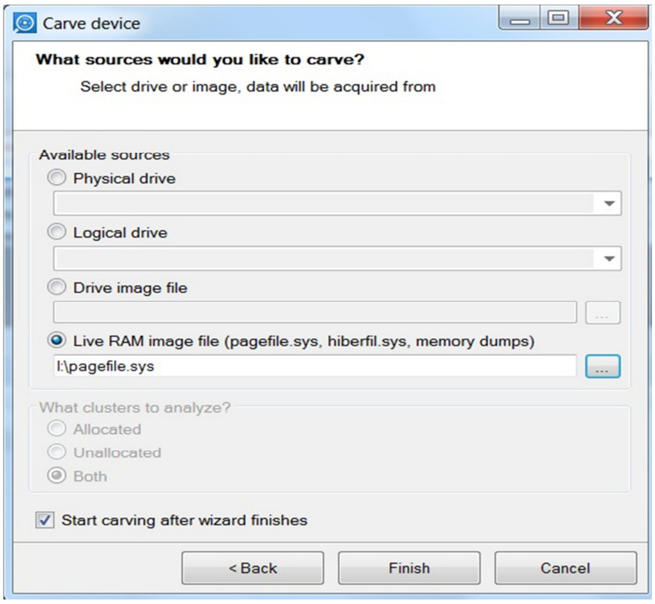
Time	Message	Sender	Recipient	Offset	Length
4/30/2012 1:44:15 AM	Hi	Instantmessenger Forensic	Forensic Test	492408955	271
4/30/2012 1:44:18 AM	this is a test	Instantmessenger Forensic	Forensic Test	492409226	283
4/30/2012 1:44:32 AM	Hi	Forensic Test	Instantmessenger Forensic	492409509	271
4/30/2012 1:45:04 AM	testcode: 13572468	Forensic Test	Instantmessenger Forensic	492409780	287

Task Manager

Task	% completed	Status	Time	Elapsed
Extracting history for RAM ...	100	Operation completed successfully	2012.04.30 ...	0:00:47
Extracting history for RAW ...	100	Operation completed successfully	2012.04.30 ...	0:00:02

Figure 4.3.9: Search result from RAM image.

The search on pagefile was done using the Carve device function as shown in figure 4.3.10.



Carve device

What sources would you like to carve?

Select drive or image, data will be acquired from

Available sources

○ Physical drive

○ Logical drive

○ Drive image file

● Live RAM image file (pagefile.sys, hiberfil.sys, memory dumps)

I:\pagefile.sys

What clusters to analyze?

○ Allocated

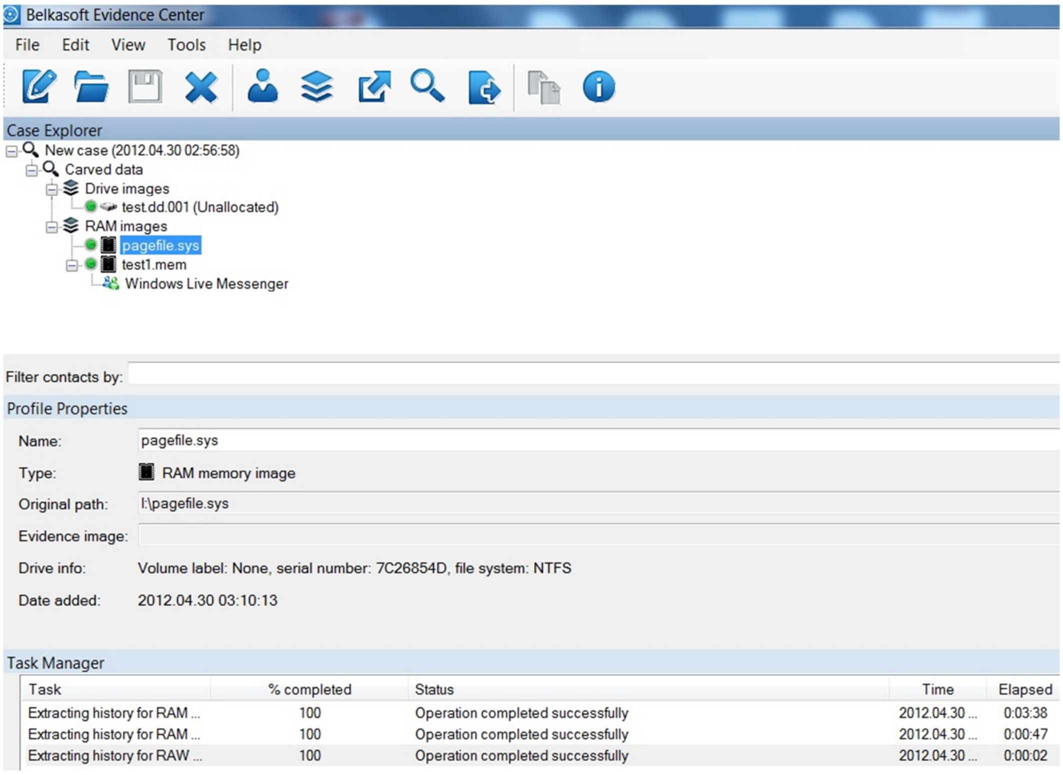
○ Unallocated

● Both

☑ Start carving after wizard finishes

Figure 4.3.10: Attempt to search for information from pagefile.

The result in figure 4.3.11 has shown that Evidence Center found nothing from the pagefile. The same function was used to search on the hibernation file retrieved from Machine-A and the chat history, screen name, time stamp, message offset and length were retrieved from the hibernation file as shown in figure 4.3.12.



New case (2012.04.30 02:56:58)
Carved data
Drive images
test.dd.001 (Unallocated)
RAM images
pagefile.sys
test1.mem
Windows Live Messenger

Filter contacts by:

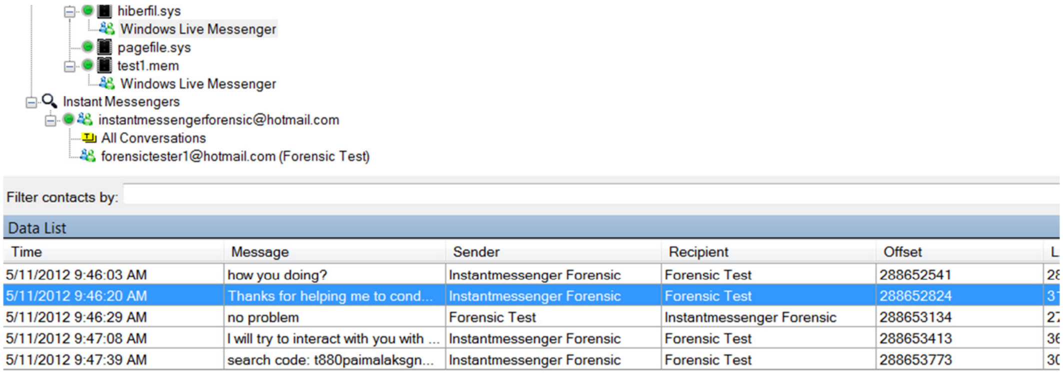
Profile Properties

Name:	pagefile.sys
Type:	RAM memory image
Original path:	I:\pagefile.sys
Evidence image:	
Drive info:	Volume label: None, serial number: 7C26854D, file system: NTFS
Date added:	2012.04.30 03:10:13

Task Manager

Task	% completed	Status	Time	Elapsed
Extracting history for RAM ...	100	Operation completed successfully	2012.04.30 ...	0:03:38
Extracting history for RAM ...	100	Operation completed successfully	2012.04.30 ...	0:00:47
Extracting history for RAW ...	100	Operation completed successfully	2012.04.30 ...	0:00:02

Figure 4.3.11: Attempt to search for information from pagefile.

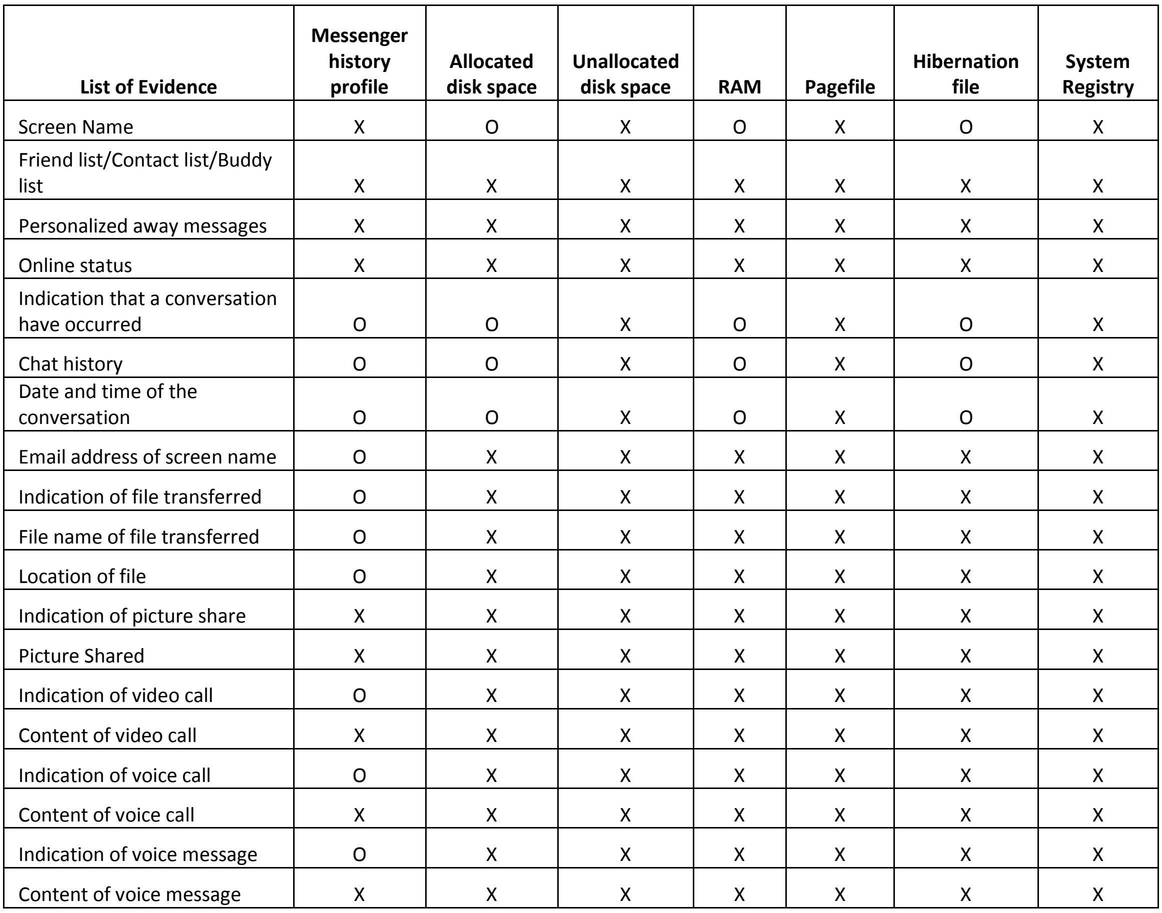

hiberfil.sys
Windows Live Messenger
pagefile.sys
test1.mem
Windows Live Messenger
Instant Messengers
instantmessengerforensic@hotmail.com
All Conversations
forensictester1@hotmail.com (Forensic Test)

Filter contacts by:

Data List

Time	Message	Sender	Recipient	Offset	L
5/11/2012 9:46:03 AM	how you doing?	Instantmessenger Forensic	Forensic Test	288652541	28
5/11/2012 9:46:20 AM	Thanks for helping me to cond...	Instantmessenger Forensic	Forensic Test	288652824	3
5/11/2012 9:46:29 AM	no problem	Forensic Test	Instantmessenger Forensic	288653134	27
5/11/2012 9:47:08 AM	I will try to interact with you with ...	Instantmessenger Forensic	Forensic Test	288653413	36
5/11/2012 9:47:39 AM	search code: t880paimalaksgn...	Instantmessenger Forensic	Forensic Test	288653773	30

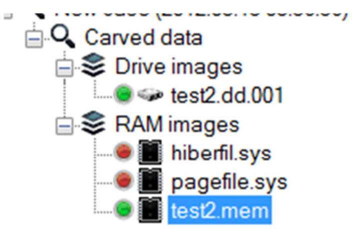
Figure 4.3.12: Search result from hibernation files.



List of Evidence	Messenger history profile	Allocated disk space	Unallocated disk space	RAM	Pagefile	Hibernation file	System Registry
Screen Name	X	O	X	O	X	O	X
Friend list/Contact list/Buddy list	X	X	X	X	X	X	X
Personalized away messages	X	X	X	X	X	X	X
Online status	X	X	X	X	X	X	X
Indication that a conversation have occurred	O	O	X	O	X	O	X
Chat history	O	O	X	O	X	O	X
Date and time of the conversation	O	O	X	O	X	O	X
Email address of screen name	O	X	X	X	X	X	X
Indication of file transferred	O	X	X	X	X	X	X
File name of file transferred	O	X	X	X	X	X	X
Location of file	O	X	X	X	X	X	X
Indication of picture share	X	X	X	X	X	X	X
Picture Shared	X	X	X	X	X	X	X
Indication of video call	O	X	X	X	X	X	X
Content of video call	X	X	X	X	X	X	X
Indication of voice call	O	X	X	X	X	X	X
Content of voice call	X	X	X	X	X	X	X
Indication of voice message	O	X	X	X	X	X	X
Content of voice message	X	X	X	X	X	X	X

Figure 4.3.13: Information recovered by Belkasoft Evidence Center from Machine-A and it has indicated which area the information was retrieved from.

The experiment result indicated that the forensic analysis using Belkasoft Evidence Center 8.3 was able to retrieve some information from different areas of Machine-A and the findings was summarised in the matrix as shown in figure 4.3.13 under the condition when the chat history was saved by the messenger. The second scenario has no historical conversation history saved by default. The testing result was shown in Figure 4.3.14



Carved data
Drive images
test2.dd.001
RAM images
hiberfil.sys
pagefile.sys
test2.mem

Figure 4.3.14: Information was not found from ram, hibernation file and page file when a conversation history was not saved by the instant messenger.

The result has indicated that nothing can be recovered by the forensic tool if the conversation is not saved.

4.4 CONCLUSION

This chapter 4 has reported the actual setting up of the evidence extraction environment, the alterations to designs and configurations made during the pilot phase and the findings from the formal extraction. It is evident that evidence extraction from IM is complex and challenging. The procedures advocated in guidance handbooks only tell the bare basics of what is expected and no information on how to do an extraction is usually given. In the report in this chapter 4 I have shown a set of procedural steps for doing an extraction. The extraction itself is a case and raises a number of issues. In chapter 5 the research question is to be answered and the issues and problems discussed.

Chapter Five

RESEARCH DISCUSSION

5.0 INTRODUCTION

In Chapter 4, the findings from the research experiment were reported. The changes made on the proposed data requirements (see Chapter 3), referred to as variations encountered, during the experiment were described in Section 4.1. After performing a number of pilot tests on different phase of the research (for instance; see pilot experiment section), the final experiment was conducted in order to answer the selected research questions according to the research methodology developed in Chapter 3.

The significant findings from the research experiment conducted that evidence acquisition from instant messaging using techniques and tools could be made easier, faster and more comprehensive in compare with the knowledge and technique listed in the forensic handbook published by United State department of Justice.

The purpose of a research methodology and then conducting the forensic investigation was to investigate what benefit can an out of the shelf forensic tool designed for evidence acquisition from instant messaging provide to the forensic examiner. The findings after the forensic examination were able to prove the forensic tool was able to provide additional benefit to a forensic examiner in an investigation over in compare to the traditional method listed in the forensic guide.

Therefore, Chapter 5 will discuss the findings of the research (Section 4.1) in order to evaluate the importance of the results. The finding results evaluation will be discussed in association with the discipline area. In addition, the developed research questions stated in Chapter 3 will be answered and discussed in relation to the asserted hypotheses in Section 5.1. The discussion summaries will be described according to the evidential arguments made, for and against. Subsequently, the discussion of the findings of the research experiment will be presented in Section 5.2 in order to comprehensively evaluate the reported outcomes. Then the recommendations (Section 5.3) will be drawn according to the knowledge acquired from the research report, followed by the conclusion of the chapter in Section 5.4.

5.1 DISCUSSION OF RESEARCH QUESTION

According to the literature review in Chapter 2 and the review of similar published work in Chapter 3, the research question was developed.

In this section, the research questions will be answered by extracting the evidence from the chapter 4 experiment finding and using a table format for evaluation. Each table format will include the question asked along with the asserted hypothesis, in which the knowledge acquired from the review of the literature will be briefly explained. Evidence will be tabulated for and against the hypotheses and then a judgement made. The outcome can be accept, reject, or insufficient evidence.

The discussion in the table will be a comparison of the knowledge gained from literature and the findings of the research experiment phases (Chapter 4). The *arguments* for the hypotheses will be presented in order to prove or refute the asserted hypotheses. To validate the report of the arguments presented the references of specific findings will be used. In conclusion of each table discussion, a brief summary of the research question and tested hypothesis will be made based on the research findings achieved in Chapter 4.

5.1.1 The Research Question and Associated Hypotheses

The main research question was derived in research methodology (Chapter 3) in order to provide a specific objective for phases of research experiment concerning digital forensic investigation. The afore-mentioned main research question was:

Can later forensic tool and technique add value to the traditional approach in evidence acquisition from instant messaging?

The forensic tool and technique is able to provide additional information from instant messenger in compare with traditional approach listed in the forensic guide published by United State department of Justice.

To answer the research question proposed in Section 3, a number of phases of research experiments were planned and conducted. The instant messaging testing environment was shaped after performing pilot tests within the laboratory to simulate evidence acquisition from instant messenger with the use of forensic technique and tool that was not described in the forensic guide (see Chapter 2). Hence, the main research question, the associated hypotheses, arguments, and a brief summary of the tested hypotheses will be presented in Tables 5.1 - 5.3.

5.1.2 Secondary Research Question and Associated Hypotheses

As stated in Chapter 3, a total of 2 secondary research questions were derived in order to inquire into related areas of concern and hence provide greater depth when answering the main research question and the following secondary research question will be discussed and answered before answering the main research question.

Are the current computer forensic tools adequate in evidence acquisition from instant messenger?

Was the selected forensic tool able to recover information from Microsoft live messenger as advertise?

The following tables (Table 5.1, Table 5.2, and Table 5.3) present the discussions of the answers to the sub-question or secondary questions. All tables contain the research question itself, the test hypothesis of the research questions, an argument section to detail the discussion in the reason of delivering the answer to the research question and a summary to conclude the answer to the research question and their hypothesis. A statement of accepting, rejecting or considering the hypothesis indeterminate will be expressed for each question based on a summary of evidence and the significant research outcome of each question.

Table 5.1: Secondary Research Question 3 and Tested Hypothesis 3

Primary Question 3: *Was the selected forensic tool able to recover information from Microsoft live messenger as advertise?*

Hypothesis 3: Hypothesis: The selected forensic tool was able to carry out the functions it has advertised and was able to deliver the promised evidence from Microsoft live messenger.

ARGUMENT:

Based on the literature research in Chapter 2, the selected forensic tool Belkasoft Evidence Center has advertised to deliver the information from MSN/live messenger as listed in Figure 5.1.1.

List of Evidence	Messenger history profile	Carving	RAM
Chat history	O	O	O
Invitation	O	X	X
Invitation Response	O	X	X
Participants	O	O	O
Date and time of the conversation	O	X	X

Table 5.1.1: Information that Belkasoft Evidence Center advertised to deliver. *note that carving function included search in allocated, unallocated disk space, pagefile, hibernation file.

The result from the experiment was indicated in Table 5.1.2.

List of Evidence	Messenger history profile	Carving	RAM
Chat history	O	O	O
Invitation	-	-	-
Invitation Response	-	-	-
Participants	O	O	O
Date and time of the conversation	O	O	O

Table 5.1.2: Information that Belkasoft Evidence Center was recovered during the experiment detailed in Chapter 5.

After comparing Table 5.1.1 and 5.1.2, Belkasoft Evidence Center has proven to be capable in recovering chat history in all areas promised. This included messenger history profile, carving function and live memory. The recovery of invitation and invitation response was not tested, therefore the function was uncertain. The history of participants and Date/time when the conversation took place were also recovered as advertised in the messenger history profile, carving and RAM.

There was no description on how the Belkasoft Evidence Center would perform under different condition. In condition such as a history profile was not found on the seized computer system which a more common scenario, test result indicated the Belkasoft Evidence Center could not recover any evidence from the computer system. As stated in Chapter 2, literature researches showed that evidence might still be recovered in RAM, unallocated disk space, pagefile or hibernation file under such scenario.

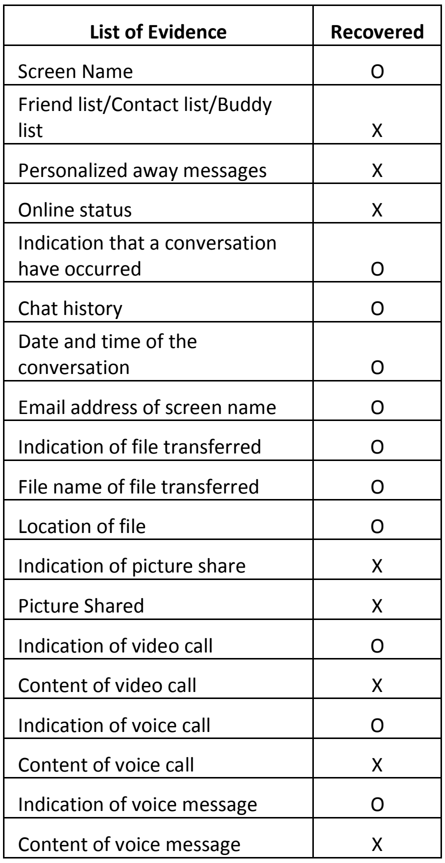
SUMMARY:

The selected forensic tool was tested in a forensically sound manner in a simulation to recover evidence from an instant messenger it advertised as supported. As stated in chapter 4, the test result indicated that although there are some limitations as stated in the above mentioned argument section. The argument has provided evidence that hypothesis 3 is to be accepted in this research experiment. Hence the selected forensic tool was able to carry out the functions it has advertised and was able to deliver the promised evidence from Microsoft live messenger.

Table 5.2: Secondary Research Question 2 and Tested Hypothesis 2

Secondary Question: *Are the current computer forensic tools adequate in instant messenger evidence acquisition?*
Hypothesis 2: A large portion of information can be recovered from instant messenger with the current forensic tools and techniques designed for that purpose.
ARGUMENT: As stated in Chapter 2 and 4, the list of possible instant messenger activities could include but not limited to text, video, voice, file transfer, photo sharing. Due to the different nature of every investigation, there was never a general indication on what type of information is defined as essential for forensic examiner and what not. Therefore when performing forensic examination on instant messenger, ideally the forensic examiner should be able to recover any evidence hidden beneath instant messaging from difficult circumstance and area in the computer system. As stated in literature research in Chapter 2, there could be different scenario such as the messenger did not enable the option to a save message log or during the time when the chat windows was closed when the computer system was seized or even after the power of the computer has been shut down. According the literature research in Chapter 2 and simulation done in Chapter 5, a little change in the circumstance could be critical in delivering a truthful forensic investigation result that may provide evidence to support the hypothesis of an investigation. In the research experiment in Chapter 4. The examination was done targeting evidence acquisition from Microsoft live messenger. There were a wide range of functions provided by the messenger for users to interact with each other's over internet. The function was The forensic examiner should be able to tell what functions of instant messaging has been used, for example Microsoft live messenger 2010 provide offer functions such as text chat, change in online status, away message, voice chat, file transfer, video chat and voice message. All these functions were a portal to communicate with other parties over the internet therefore they all presented a potential in carrying trace that lead to succeed of a forensic investigation. In Chapter 4, the result of the simulation has proven that the selected forensic tool and techniques were able to recover some information but a large portion of information remained unable to recover in both tested scenario. The first phase of simulation in chapter 4 has indicated that under the condition when

Microsoft live messenger 2011 has its chat window closed and the message log enabled, information listed in Figure 5.2.1 could be recovered.



List of Evidence	Recovered
Screen Name	O
Friend list/Contact list/Buddy list	X
Personalized away messages	X
Online status	X
Indication that a conversation have occurred	O
Chat history	O
Date and time of the conversation	O
Email address of screen name	O
Indication of file transferred	O
File name of file transferred	O
Location of file	O
Indication of picture share	X
Picture Shared	X
Indication of video call	O
Content of video call	X
Indication of voice call	O
Content of voice call	X
Indication of voice message	O
Content of voice message	X

Table 5.2.1: Information that the selected tools and techniques were able to recover from the experiment conducted in Chapter 4

Table 5.2.1 was constructed based on experiment result conducted in Chapter 4, the result from experiment has indicated that information including screen name, indication that a conversation have occurred, chat history, date and time of the conversation, email address of screen name, indication of file transferred, file name of file transferred, location of file, indication of video call, indication of voice call and indication of voice message were recovered by the selected forensic tool. However a portion of activities and content of the activities were unable to recover via the selected forensic tool. The list of evidence unable to recover included friend list/contact list/buddy list, personalized away messages, online status, indication of picture share, picture Shared, content of video call, content of voice call and content of voice message. Which indicated that only 72% of the evidence listed in the chart can be recovered.

The second phase of experiment was conducted while the history profile of the messenger was not saved. The experiment result indicated that the selected tool was unable to recover any evidence from this scenario.

List of Evidence	Recovered
Screen Name	X
Friend list/Contact list/Buddy list	X
Personalized away messages	X
Online status	X
Indication that a conversation have occurred	X
Chat history	X
Date and time of the conversation	X
Email address of screen name	X
Indication of file transferred	X
File name of file transferred	X
Location of file	X
Indication of picture share	X
Picture Shared	X
Indication of video call	X
Content of video call	X
Indication of voice call	X
Content of voice call	X
Indication of voice message	X
Content of voice message	X

Table 5.2.2: No information can be recovered from the selected forensic tool if the messenger did not keep the chat history.

According to literature researches and case study in Chapter 2, it is possible to recover evidence listed in Table 5.2.1 and 5.2.2 through different techniques. It is possible even in complicate situation such as no history profile is saved, evidence has been purposely deleted, chat window is closed and seized machine has been turned off. The tool should be act as a media to manipulate the techniques to simplify the process when attempt to recover evidence from instant messenger.

The selected forensic tool to conduct the experiment was officially described with the capability to recover evidence from instant messenger through different techniques. It supported many popular instant messengers and the tool has been widely accepted by numerous popular forensic organisations across. However one tool may not be adequate to represent the functionality of all and the tool selected does not equip with all available forensic technique to conduct forensic examiner on instant messaging. Chapter 2 stated that technique such as searching the Windows registry and network evidence acquisition could be used to recover some evidence from instant messaging but the selected tool was not equipped with those techniques yet.

SUMMARY:

As discussed in the argument section, it is hard to measure and define what is adequate and what not, because there are unique characteristics in every investigation which lies unlimited possibilities on what evidence could be useful to the forensic examiner. Hence, we can only put in a best effort to collect a list of evidence that may be useful in an investigation based on literature researches and case studies.

The experiment conducted in Chapter 4 has tested the ability of the chosen forensic tool designed to recover evidence from instant messaging. The tool has manipulated several but not all forensic techniques described in Chapter 2.

The experiment result shows that the tool appeared to be inadequate in evidence acquisition from instant messaging because a good portion of activities and evidence hidden beneath instant messenger could not be recovered.

Although the tool that was used to conduct the experiment in Chapter 4 was considered one of the more comprehensive forensic tools designed for instant messaging examination. But yet its functionality appears to be very conditional and deficient. Through literature research, no forensic tool was found to have equipped with all techniques developed for instant messaging examination.

The argument has provided evidence that hypothesis 2 is to be rejected in this research experiment. Hence a large portion of information was not recovered from instant messenger with the current forensic tools designed for that purpose.

Table 5.3: Primary Research Question and Tested Hypothesis 1

Primary Question: *Can later forensic tool and technique add value to the traditional approach in evidence acquisition from instant messaging?*
Hypothesis 1: Techniques and tools designed for instant messaging forensic examination are able to provide additional value to an investigation.
ARGUMENT: According to the literature researches in Chapter 2. The traditional approach was stated in the forensic guides published by United State Department of Justice in 2007. The traditional approach was able to deliver information that heavily relies on chat windows that remain opened when the computer system was seized by enforcement agencies. The guide did not describe any further approach that may recover evidence from instant messenger during scenario where chat window was closed or computer system was not powered on. The traditional approach described enforcement agency should take photos from the screen when an instant messenger was observed. That only captures the evidence from instant messenger at the state when it was seized. If function such as voice chat and video chat has been has been initiated, photo from the screen may only prove the function has been initiated and the time when it was initiated but the content of the voice and video chat could not be recovered from the photo of a screenshot. Through literature researches, network forensic technique may be used to capture some evidence if the instant messenger session was still active when it was seized. Although other techniques might appears to be situational, literature researches in Chapter 2 has proven that live memory acquisition may restore evidence from a closed chat Windows and other items previously stored in the RAM. If the computer system has been hibernated or if the data from instant messenger has been written to the pagefile, it was possible to retrieve evidence from those areas. The unallocated space search offer the option to search for temporary or deleted data generated from the instant messenger. Although the techniques appears to be situational, they offer enforcement agency more options to achieve evidence in different situations and increase the success rate to locate key evidence from instant messenger in compare to the traditional approach stated in the forensic guides. The experiment result stated in Chapter 4 has tested the ability of the selected forensic

tool. Research question 3 has been answered there is evidence to show that the selected forensic tool was able to deliver the evidence from Microsoft live messenger as advertised. However the constraint was limited to a saved messenger history profile. The test result shows that under condition where the messenger history profile was not saved, the tool was unable to reveal more information than the traditional approach.

Chapter 2 has described that the forensic techniques can be situational and the experiment might not have the required elements to replicate the scenario to trigger the situation to test out the forensic techniques.

SUMMARY:

Through argument, the research question has been discussed. The experiment result from Chapter 4 stated that in terms of competency of evidence retrieval, the forensic tool does not offer anything more than the traditional approach stated in the forensic guides.

It is arguable that additional evidence could be achieved in unique circumstances as stated in literature researches in Chapter 2.

Regardless of the retrievable from instant messenger, the tool offers simplicity to search for evidence from a wide range of messengers. The tool was also equipped with functions including keyword search for key evidence from the extracted messenger history profile. Although not essential, these functions were able to increase the efficiency of an investigation in terms of speed and simplicity when compare to the traditional approach.

Therefore the argument has provided evidence that hypothesis 1 is to be accepted in this research experiment. Hence techniques and tools designed for instant messaging forensic examination are able to provide additional value to an investigation.

5.2 DISCUSSION OF FINDINGS

The findings of the research were detailed, analysed and reported in the previous chapter (Chapter 4). This section will now discuss the significance of the results related to instant messaging forensic examination. Hence, the discussions will include the phases of research, the evaluation of the tools and techniques used in research.

5.2.1 Discussion of Conducted Research Phases

The research experiment was composed of two different phases (see Chapter 3) and each phase shared a common goal but under different constraints on the circumstance. To identify and emphasize the significant findings (Chapter 4), the discussion of research testing phases will involve case scenario when history profile was saved and when history profile was not saved. However, the testing on network forensic technique and Windows registry search will not be covered in this section as it was conducting research and analysing of the previous similar published works stated in Chapter 2 in order to derive the methodology for research conducted (Chapter 3).

5.2.2 Discussion of First Testing Scenario

The first phase of the research experiment, testing environment has been setup under the condition where the history profile was saved by default, chat windows was closed and machine was powered down after switched to hibernation mode. After conducting a few pilot tests, the problems were encountered during the pilot testing phases of setting up a stabilized system listed as stated in the pilot testing section in chapter 4. For instances, the problems such as compatibility issue with virtual environment were encountered which lead to some changes from the original experiment design. Even though, a steadied virtual environment was set up to fit a laboratory simulation.

5.2.3 Discussion of Second Testing Scenario

Likewise, the second phase of the research experiment has been setup under the condition where a message history profile was not saved. The proposed scenario was believed to be more common in a real world investigation as stated in the studies of forensic guides in Chapter 2, therefore a second scenario where the messenger history profile was not saved. The testing environment has been setup under a similar condition as the first phase. However, the simulated system design appears to be inefficient to replicate the special condition required to trigger an accurate testing of the proposed scenario.

5.2.4 Discussions of Identification, Acquisition and Extraction

The identification, acquisition and extraction processes of evidential data, in the both phase of the research experiment were performed by using an out of shelf forensic tools introduced in Chapter 2. The primary concern was to select a tool that was accepted by a wide range of enterprises and it has to be designed for the purpose of instant messaging forensic examination. Techniques that can be manipulated in evidence acquisition from instant messaging were introduced in Chapter 2 and they were to be tested through the use of the selected forensic tool. Hence, Belkasoft Evidence Center was selected to be the tool used in the simulation for identification, acquisition and extraction. Other candidates did not fall into the desire criteria.

The identification of evidence in the simulation was simple because the scope has been set through pervious case studies and literature researches in Chapter 2. Also the laboratory context had no business processes or policies to obstruct the access to evidence. As a consequence a clear objective has been delivered to each scenario of the simulation.

The challenge was to follow the correct process in extraction and acquisition that is very similar to a real life scenario.

5.3 DISCUSSION OF RECOMMENDATIONS: BEST PRACTICES

The previously discussed sections and the findings of the research experiment (Chapter 4) has guided the forensic investigators and forensic tool developer in such a way in which the knowledge of the digital forensic tool and technique for instant messaging evidence acquisition need to be improved. Especially, the digital forensic tool designed for acquisition or extraction can be equipped with additional techniques and coverage of different scenario has to be broadened. Hence, the knowledge acquired during the research experiment has been shared and discussed with the forensic tool developer. As a result, recommendation has been accepted and improvement to the tool has been scheduled to be developed in the upcoming versions.

5.4 CONCLUSION

In this chapter, the discussion of findings from the research experiment presented in Chapter 4 was made. The answers to the proposed research questions from the methodology in chapter 3 were discussed in relation to the asserted hypotheses and a conclusion was reached with regard to the validity of the anticipated hypotheses. Likewise, the findings after the investigation on the effectiveness on the later tool and technique designed for instant messaging evidence acquisition were also discussed and evaluated. Furthermore, the issues related to the investigation were stated.

The main research question was a focal point to discuss the effectiveness of later tool and technique and the phases of research model stated in Chapter 3 were established based on the primary research question. The tested system design was also set up based on the main research question. The findings in Chapter 4 after a complete forensic examination were able to prove that instant messenger evidence acquisition can be benefit by later forensic tool and technique in compare to the traditional approach.

The secondary research questions were also answered by the tested system. The findings in Chapter 4 were able to prove that the selected tool was only capable to assist the instant messaging forensic examination to some extend but was inadequate to carry out a comprehensive investigation. The finding suggested that several improvements could be done on the selected tool to extend its current limitation.

In the following chapter, the thesis research project will be concluded. A summary of the research conducted and the significant answers to the research questions will be outlined in that conclusion chapter (Chapter 6). Furthermore, the areas for future research will be explained and followed by the conclusion.

Chapter Six

CONCLUSION

6.0 INTRODUCTION

The significant gap in the digital forensics research relating to IM business system tools and professional procedures was noted in chapter 1. The relevant literature was reviewed in Chapter 2, including an introduction to the IM system (Section 2.1), a selection of current IM evidence extraction tools (Section 2.2) and techniques (Section 2.3), the IM investigation procedures (Section 2.4) and the traditional investigation. A summary was made of the relevant issues and problems (2.7), notably that the literature research has suggested many issues and problem presented in digital forensic work for IM. The concerns including the incompetency of forensic guide published by U.S Department of Justice in terms of forensic procedure, technique and knowledge. In chapter 3 a researchable problem and question were identified (3.4.2) and a plausible research methodology specified (3.4, 3.5).

In order to answer the research questions, the scope of the research has been specified through literature research and interview with forensic tool developer. Subsequently, four different research phases has been set out based on literature research and guidance obtained from the review in Section 3.1-3.3 and two scenarios were chosen for the research experiment to increase the reliability of the research findings. The choices of extraction scenario were selected based on the literature researches (2.5, 2.6). First scenario was decided to simulate the scenario where an IM has enabled the function to save chat history and the chat program has been shut down before an enforcement agency can seize the computer system containing the instant messenger, and the second scenario was decided to simulate a scenario similar to the first scenario but with the function to save chat history disabled. A series of pilot testing has been carried out before the actual testing to oversee and overcome difficulties that might encounter in the actual experiment testing. The detail of the pilot testing and problem arisen was specified in Section 4.2.

Subsequently, Forensic tool and technique were applied to each scenario following the IM investigation procedure (2.4). The entire experiment testing setup and activities was captured in Section 4.1. Hence, data was collected from the experiment and the result was sorted and preserved in matrix format (4.3). Likewise, the other scenario was tested and recorded in the same manner. The evidential search was performed in each of the entities by using Evidence Center developed by Belkasoft. Hence, the findings of the research were presented, analysed and discussed in Chapter 4 and Chapter 5 respectively.

In order to conclude the research project, the following sections are organized. Section 6.1 is a summary of findings from the completed research and Section 6.2 summarises the answers to the research question. Then, future research opportunities arising are outlined in Section 6.3 followed by the conclusion (Section 6.4).

6.1 SUMMARY OF FINDINGS

Thus, the research presents different techniques that might apply for extracting evidence from volatile instant messenger and the result can add to the knowledge base for the instant messenger forensic investigations and provide additional knowledge for forensic investigator when attempt to acquire evidence from a volatile instant messenger.

Based on the result of my experiment, an off the shelf forensic tool Belkasoft Evidence Center was used to extract evidence from a volatile IM. It was able to simplify the processes in digital evidence extraction for the areas of:

- Saved chat log
- Allocated disk space
- Unallocated disk space
- RAM

It could potentially retrieve digital evidence from Pagefile and Hibernation file however nothing was found in those areas during my experiment. It is due to the usage of pagefile and hibernation file that were subjective. Generally the computer system will only store information in pagefile and when RAM is insufficient, data will only be written to hibernation file when the computer is switched to the hibernation mode. The experiment was not designed to trigger those elements.

The current version of Belkasoft Evidence Center was able to store the digital evidence extracted from instant messenger in a database for further analysis and it was able to provide useful function such as keyword search to aid an investigation. Based on the literature research, an instant messenger could leave a trace in Window Registry, however the tool did not provide the function to capture information from the registry. Another off the shelf application was required to capture the image of the hard drive and perform memory dump from the RAM before Belkasoft Evidence Center could analyse the data.

The experiment showed that the tool did not provide the function to extract the following type of digital evidence:

- Indication of picture sharing
- Content of the picture shared
- Content of video call
- Content of voice message

The finding indicated that the forensic tool in the experiment was able to aid the forensic examiner to extract digital evidence from instant messenger but it was not comprehensive enough at its current form. Forensic examiners could not rely on one tool during an investigation.

The tool had proven to greatly simplify the processes of evidence extraction. However there are many variables that lie in the process of instant messenger forensic examination. Therefore a comprehensive knowledge of forensic techniques was still essential in order to carry out an investigation. The tool was not powerful enough to allow general enforcement agents to extract digital evidence from instant messenger without the supervision from an expert.

6.2 ANSWER TO THE RESEARCH QUESTIONS

The primary research question is stated as:

Can later forensic tool and technique add value to the traditional approach in evidence acquisition from instant messaging?

> With the hypothesis:
>
> *Techniques and tools designed for instant messaging forensic examination are able to provide additional value to an investigation.*
>
> > And the answer was:
> >
> > *There was evidence to support that hypothesis 1 is to be accepted in this research experiment. Hence techniques and tools designed for instant messaging forensic examination are able to provide additional value to an investigation.*

The first secondary research questions are stated as:

Are the current computer forensic tools adequate in evidence acquisition from instant messenger?

> With the hypothesis:
>
> *A large portion of information can be recovered from instant messenger with the current forensic tools and techniques designed for that purpose.*
>
> > And the answer was:
> >
> > *There was evidence to support that hypothesis 2 is to be rejected in this research experiment. Hence a large portion of information was not recovered from instant messenger with the current forensic tools designed for that purpose.*

The second secondary research questions are stated as:

Was the selected forensic tool able to recover information from Microsoft live messenger as advertise?

With the hypothesis:

The selected forensic tool was able to carry out the functions it has advertised and was able to deliver the promised evidence from Microsoft live messenger.

And the answer was:

There was evidence to support that hypothesis 3 is to be accepted in this research experiment. Hence the selected forensic tool was able to carry out the functions it has advertised and was able to deliver the promised evidence from Microsoft live messenger.

6.4 FUTURE RESEARCH

The findings of the research have been shared with the forensic tool developers included in the research and there were further discussions around development of the tools.

As a result, technique such as searching IM fingerprint through Window Registry and web browser were agreed to be implemented in a further version of Belkasoft Evidence Centre.

During the process of testing, a bug of Belkasoft Evidence Centre 2012 has been discovered during the testing where conflict were found between two functions, the bug and the work around has been submitted to the developer as a reference to further enhance the stability of the software.

Further research in the subject can be extent by testing the ability of forensic tools developed by other developers, the range of scenario can be broaden to test the veracity of the selected tool. Further research into the IM forensic area can be target on volatile based messenger as they were known to leave minimal trace in the computer system and have been a difficult subject for forensic examiner.

REFERENCES

Artman, J. (2012). How to Change a VMware Disk to Preallocated Retrieved April 26, 2012, from http://www.ehow.com/how_6011473_change-vmware-disk-preallocated.html

Belkasoft. (2012a). Belkasoft customers, from http://forensic.belkasoft.com/en/home/en/customers.asp

Belkasoft. (2012b). Instant Messenger Support, from http://forensic.belkasoft.com/en/bec/en/Instant_Messenger_Support.asp

Braught, G., Miller, G. S., & Reed, D. (2004). Core Empirical Concepts and Skills for Computer Science. *ACM SIGCSE Bulletin, 36*(1), 4.

Carvey, H. (2004). Instant messaging investigations on a live Window XP system. *Digital Investigation, 1*(4), 256-260. doi: 10.1016

Chen, H., Luo, D., Gao, Q., Qian, Z., & Wu, S. (2009). *IE internet information forensics technology in unallocated disk space.* Paper presented at the Computer Network and Multimedia Technology, 2009. CNMT 2009, Wuhan.

Chiu, C.-H., Wu, R.-S., Tut, C.-I., Lin, H.-T., & Yuan, S.-M. (2007). *Next generation notification system integrating instant messengers and web service*. Paper presented at the Convergence Information Technology, 2007., Gyeongju.

von Dongen, W. S. (2007). Forensic artefacts left by Window Live Messenger 8.0. *Digital Investigation 4, 4*(2), 73-87.

Dubord, P. (2008). Investigating cybercrime *Handbook of Digital and Multimedia Forensic Evidence* (pp. 77-89). Totowa: Humana Press.

Gao, Y., & Cao, T. (2010). Memory forensics for QQ from a live system. *Journal of computers, 5*(4), 541-548.

Grossman, A. M. (2006). No, don't IM me - Instant messaging, authentication, and the best evidence rule. *George Mason Law Review, 13*(6), 1309-1339.

Hagy, D. W. (2007a). *Investigative involving the internet and computer networks*. Washington, DC: National Institute of Justice.

Hagy, D. W. (2007b). *Investigative uses of technology: devices, tools, and techniques*. Washington, DC: National Institute of Justice.

Hagy, D. W. (2008). *Electronic crime scene investigation: A guide for first responders, second edition*. Washington, DC: National Institute of Justice.

Ho, J., Chen, W., & Hsieh, R. (2009). *Identifying google talk packets.* Paper presented at the Intelligence and Security Informatics, 2009. ISI '09. IEEE International Conference, Dallas, TX.

Huhtinen, H. (2008, January 17, 2011, October 03). What is the difference between Workstation, Player and Server? Retrieved April 27, 2012, from http://vmfaq.com/entry/5/

Kiley, M., Dankner, S., & Rogers, M. (2008). *Forensic analysis of volatile instant messaging.* Paper presented at the IFIP International Federation for Information Processing, Boston.

Meebo. (2012). Meebo products, from https://www.meebo.com/products/

Law, F. Y. W., Chow, K. P., Kwan, M. Y. K., & Lai, P. K. Y. (2007). *Consistency issue on live systems forensics* Paper presented at the Future Generation Communication and Networking (FGCN 2007), Korea.

Microsoft. (2012). Window Live Messenger Features, from http://windows.microsoft.com/en-US/messenger/features

Mrdovic, S., Huseinovic, A., & Zajko, E. (2009). *Combining static and live digital forensic analysis in virtual environment.* Paper presented at the Information, Communication and Automation Technologies, 2009. ICAT 2009, Bosnia.

Network Dictionary. (2011). Instant Messenging, from http://wiki.networkdictionary.com/index.php/Instant_Messenging

Nikkel, B. J. (2006). Improving evidence acquisition from live network sources. *The International Journal of Digital Forensics and Incident Response, 3*(2), 1-22.

Reust, J. (2006). Case study: AOL instant messenger trace evidence. *Digital Investigation 3, 3*(4), 238-243.

Santos, B. S., Dias, P., Silva, S., Ferreira, C., & Madeira, J. (2009). Introducing students to empirical methods in CG and HCI courses through user studies. *The Eurographics Association*.

Savoldi, A., & Gubian, P. (2008). *Towards the virtual memory space reconstruction for windows live forensic purposes.* Paper presented at the Systematic Approaches to Digital Forensic Engineering, 2008. SADFE '08, Oakland, CA.

Schuster, A. (2006). Searching for processes and threads in Microsoft Windows memory dumps. *Digital Investigation 3S.*

Tichy, W. F. (1998). Should computer scientists experiment more? *Computer, 31*(5), 9.

Turnbull, B., & Slay, J. (2007). *Wireless forensic analysis tools for use in the electronic evidence collection process.* Paper presented at the 40th Hawaii International Conference on System Sciences, Hawai

Vleck, T. V. (2012). Electronic Mail and Text Messaging
in CTSS. *IEEE Annals of the History of Computing, 34*(1), 4-6. doi: 10.1109/MAHC.2012.6

VMware. (2012). Using VMware Virtual Disk Manager, from http://www.vmware.com/support/ws45/doc/disks_vdiskmanager_ws.html