Forensic Analysis of the Windows 7 Registry

Khawla Abdulla Alghafli[1], Andrew Jones [1, 2] and Thomas Anthony Martin [1]
[1] Khalifa University of Science, Technology and Research (KUSTAR)
Sharjah, UAE
khawla.alghafli@kustar.ac.ae

[2] Edith Cowan University
Perth, Western Australia

Abstract
The recovery of digital evidence of crimes from storage media is an increasingly time consuming process as the capacity of the storage media is in a state of constant growth. It is also a difficult and complex task for the forensic investigator to analyse all of the locations in the storage media. These two factors, when combined, may result in a delay in bringing a case to court. The concept of this paper is to start the initial forensic analysis of the storage media in locations that are most likely to contain digital evidence, the Windows Registry. Consequently, the forensic analysis process and the recovery of digital evidence may take less time than would otherwise be required. In this paper, the Registry structure of Windows 7 is discussed together with several elements of information within the Registry of Windows 7 that may be valuable to a forensic investigator. These elements were categorized into five groups which are system, application, networks, attached devices and the history lists. We have discussed the values of identified elements to a forensic investigator. Also, a tool was implemented to perform the function of extracting these elements and presents them in usable form to a forensics investigator.

Keywords
Windows Registry, Computer Forensics, Forensics investigator,

INTRODUCTION

It is generally accepted nowadays that there is an ongoing evolution in technologies (including computers, networks, the internet, smart homes, e-commerce etc.) that are increasingly involved in most aspects of our life. Illegal activities and crimes have also increased with this evolution. A large number of organisations are suffering from these computer crimes and the criminals that perpetrate them have a range of motivations. For example, criminals have terrorism goals or may aim to gain money or seek to destroy the reputation and customer confidence of organisations. Figure 1 shows several types of computer crimes and the percentages of organisations affected by these crimes in the Middle East for the period between 2007 and 2009.

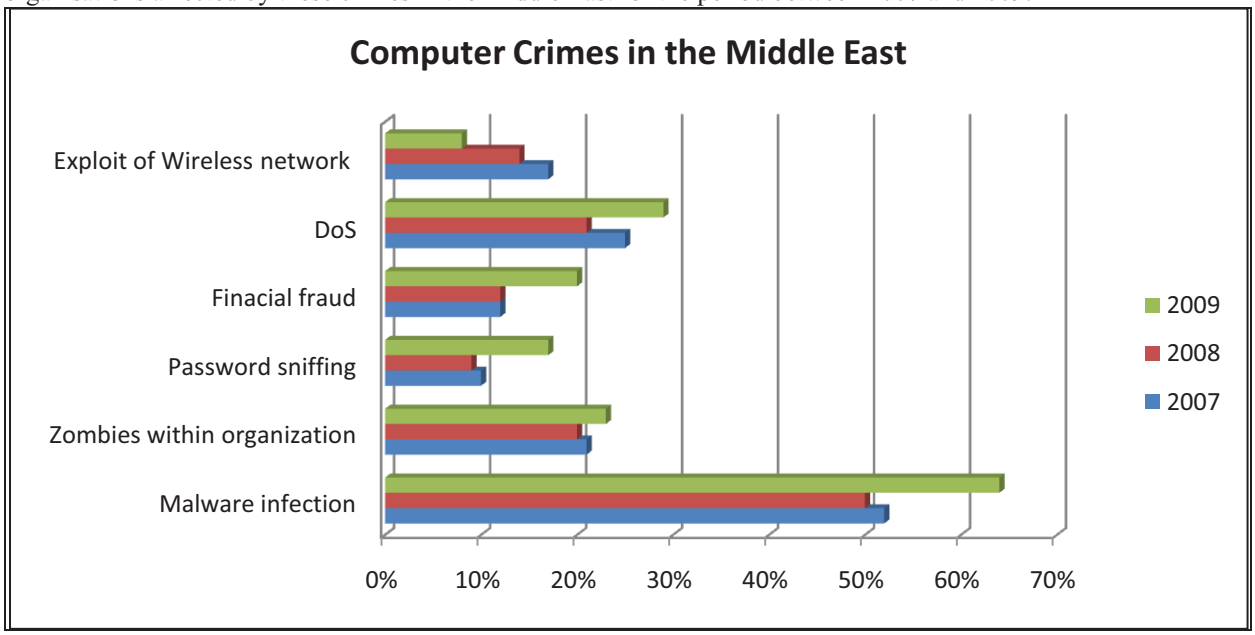

Figure1: Computer crimes in the Middle East
Source of statistics: (Dwyer, 2010)

Since crimes have moved into the computing environment, a new field in forensic investigations has appeared which is called Computer Forensics, but this is now more commonly referred to as digital forensics. There are several definitions for Computer Forensic including the following:

> "Computer forensic is the collection, preservation, analysis, and presentation of computer-related evidence" (Vacca, 2010).

> "Computer investigation and analysis techniques that involve in the identification, preservation, extraction, documentation, and interpretation of computer data to determine potential legal evidence" (Solomon, Barrett, & Broom, 2005).

From these definitions it is clear that the aim of computer forensics is to find digital evidence that is acceptable in the court. It is generally accepted that the capacity of storage media is in a state of constant growth. Consequently, the recovery of digital evidence of crimes from storage media is increasingly time consuming and complex. One way to make the process faster and simpler is to start searching for evidence in the locations that are most likely to contain information that is of value to the forensics investigator. One of the best areas to start such an investigation is in the Windows Registry.

The Windows Registry is one of the essential components of current Microsoft Windows operating systems. The Windows registry performs two critical tasks for the Microsoft Windows operating system. The first is that it is the repository for settings for the Windows operating system and applications that are installed on the system. The second is that it is the database of the configuration of all installed hardware. The Windows Registry is defined as follows:

> "A central hierarchical database used in Microsoft Windows 98, Windows CE, Windows NT, used to store information that is necessary to configure the system for one or more users, applications and hardware devices" (Microsoft Computer Dictionary, 2002).

Note: Since this reference the same approach has been taken with Windows 2000, Windows XP, Windows Vista and Windows 7.

In this paper several elements of the Windows Registry that may be valuable to a forensics investigator are discussed. First the structure of Windows Registry was analysed, then elements within the Windows Registry that may be of evidential value are discussed.

RELATED WORKS

The evolution of computers and internet technology has had an impact on most areas of our lives. Illegal activities and crimes have also increased with this technology evolution. Consequently, a new field of forensic investigation developed to deal with this phenomenon and this was called Computer Forensics. Computer Forensics is defined as "the process of methodically examining computer media (hard disk, diskettes, tapes, etc.) for evidence (Vacca, 2010). The computer forensic process consists of evidence identification, evidence preservation, evidence analysis and evidence presentation (Solomon, Barrett, & Broom, 2005).

The digital forensic investigators' aim is to find evidence of crimes. There are several types of digital crimes in the computing environment. Each electronic crime has several potential digital evidences. For instance, the types of digital evidence associated with identity theft include accounting software, financial records, forged documents and web site transaction records (An on the Scene Reference for First Responders, November 2009).

There are several books that describe the structure of versions of the Window Registry, such as the Microsoft Windows Registry Guide (Honeycutt, 2005) and the Windows XP Registry (Kokoreva, 2002). They described the history, the structure and the purpose of the Windows Registry. The description of the structure consists of a description of the logical and physical structures. The description of the logical structure includes analysis of five basic registry keys as they are viewed in basic windows registry editors. The description of the physical structure includes how and where registry hive files are stored in the physical memory.

Over the years since Microsoft implemented the Windows Registry in their operating systems, it has become clear that it contains valuable information for the forensics investigator (Carvey & Kleiman, 2007). Carvey said that "Knowing where to look within the registry, and how to interpret what you find, will go a long way towards

giving you insight into activity that occurred on the system". He analysed the Registry structure of Windows XP and did an excellent job of the analysis of the registry structure within the hive files in physical memory. He also provided useful information about the signature of hive files in memory. These signatures can be used by a forensics investigator to carve registry keys and their values from the unallocated space of an image or from a dump of the RAM. The value of this book is the registry analysis and the considerable amounts of valuable information that are identified for the forensics investigator within the Windows Registry. For example time zone information, audit policy, wireless SSIDs, locations of auto-start programs, user activities and mounted devices. I believe that this book provides the forensics investigator with a deeper understanding of the forensics elements within the Windows Registry.

Thomas and Marris said that "When a USB flash drive is plugged into a Windows XP computer, a number of registry settings and log files are automatically updated to reflect the use of the USB flash drive" (Thomas & Marris, 2008). The purpose of their work was to understand information that identifies a USB flash drive that has been used in the computer and to identify where the forensics investigator should look to acquire this digital evidence.

WINDOWS REGISTRY STRUCTURE

In the Windows operating system, the Windows Registry is organised logically into a number of root keys and tools such as, the Windows Registry editor can be used to display the logical structure of the Windows Registry. There are five logical root keys in the Windows Registry of Windows 7 which are:

1. HKEY_CLASSES_ROOT.
2. HKEY_CURRENT_USER.
3. HKEY_LOCAL_MACHINE.
4. HKEY_USERS.
5. HKEY_CURRENT_CONFIG.

Figure 2 shows the five root keys of the Registry in Windows 7 as displayed in the Windows Registry Editor.

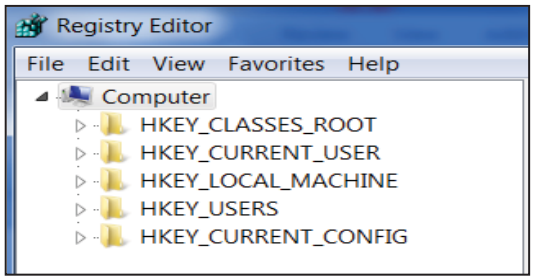

Figure 2: Windows Registry root keys

Actually there are only two root keys which are HKEY_LOCAL_MACHINE and HKEY_USERS. These two root keys are stored on the hard disk of the system and are not volatile data held in main memory. The other root keys are subsets of these of keys. Figure 3 shows the relationship between root keys.

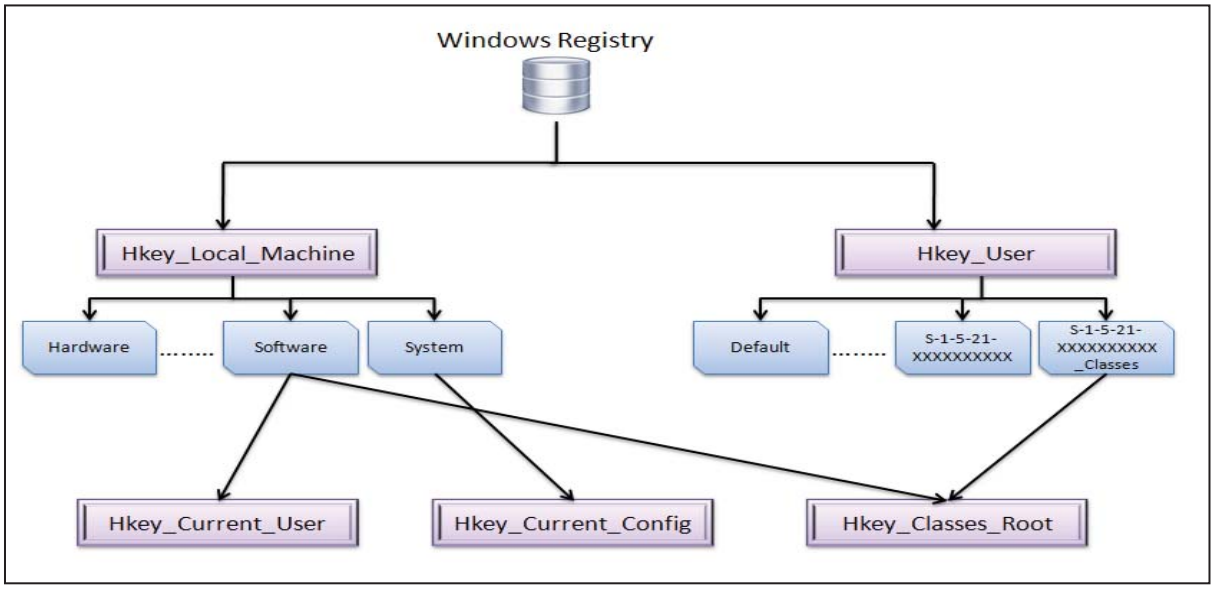

Figure 3: Relation between Windows Registry root keys

The Windows Registry editor displays the logical structure of the Registry. The Windows operating system organises the Registry into a number of hive files. The hive file is a binary file which consists of one or more Registry keys, together with their values. These files have been modified with changes in the Windows operating system. The changes have been made because each new Windows operating system has new functionality. Figure 4 shows the changes in hive files of the Windows Registry in several variants of the Windows operating system.

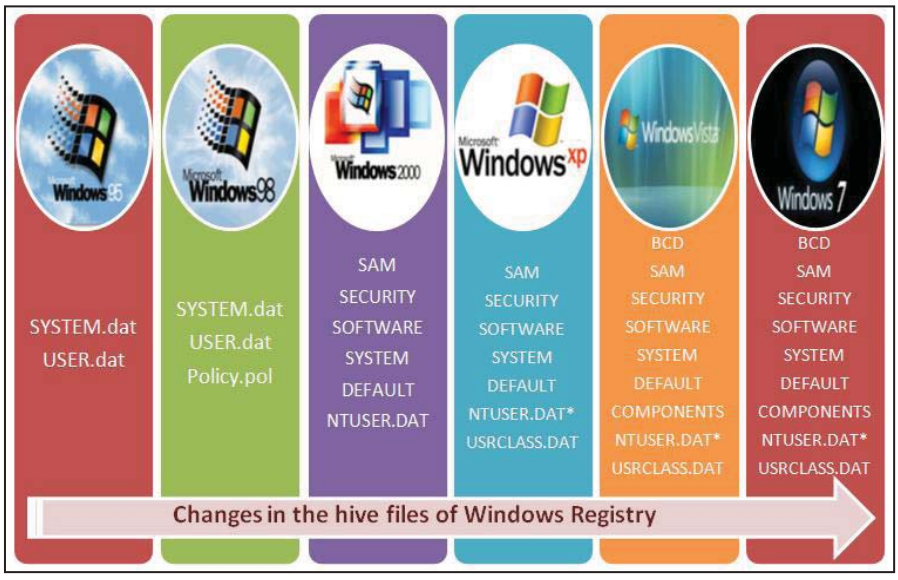

Figure 4: changes in the hive files of Windows operating system

*there are three or more hive files that have the name NTUSER.DAT. The first one is related to network services account, the second one to local services account and the third one to user account (each user account has its NTUSER.DAT hive file).

FORENSICS ANALYSIS OF THE REGISTRY OF WINDOWS 7

System Analysis

The Windows Registry holds a great deal of information about the system such as the settings and configuration of the system. There are a number of these values that would be of the interest to a forensic investigator.

Firstly, the computer name is available in the following Registry sub key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName
The system information Registry sub key has the following path:
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\BIOS
This key holds several values that contain information about the system such as BIOS information and product information. The BIOS information includes the BIOS release date and BIOS version. Information about the BIOS includes the product name of the system and its manufacturer's name. Figure 5 shows the system information Registry sub key.

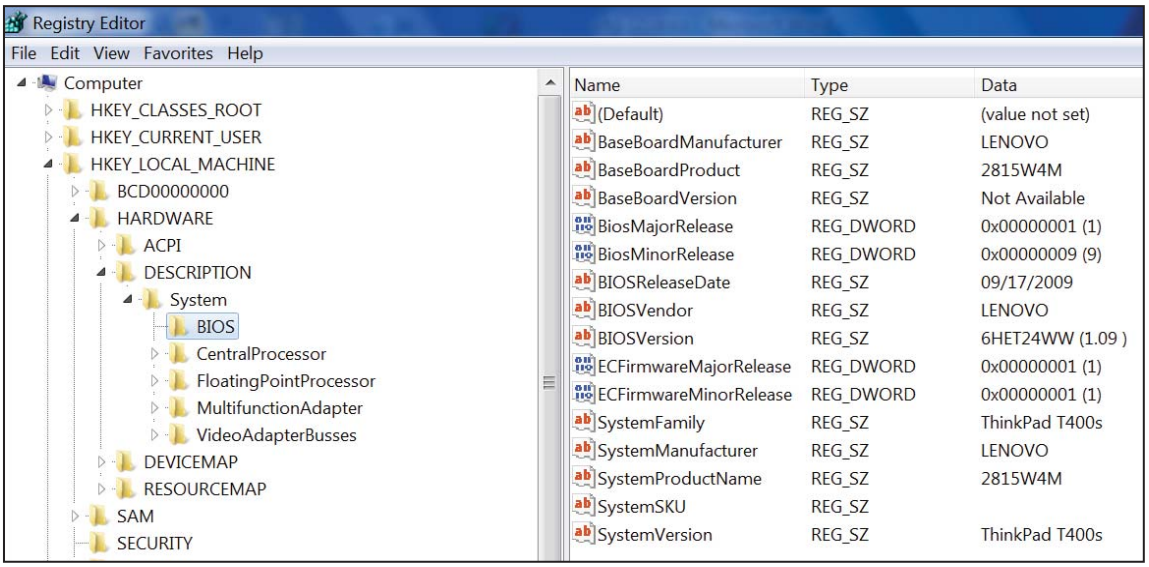

Figure 5: system hardware description within Windows Registry

The information about the processors of the system is stored in the following Windows Registry sub keys:
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\1
This information includes the processor name, its speed and vendor identifier as shown in Figure 6.

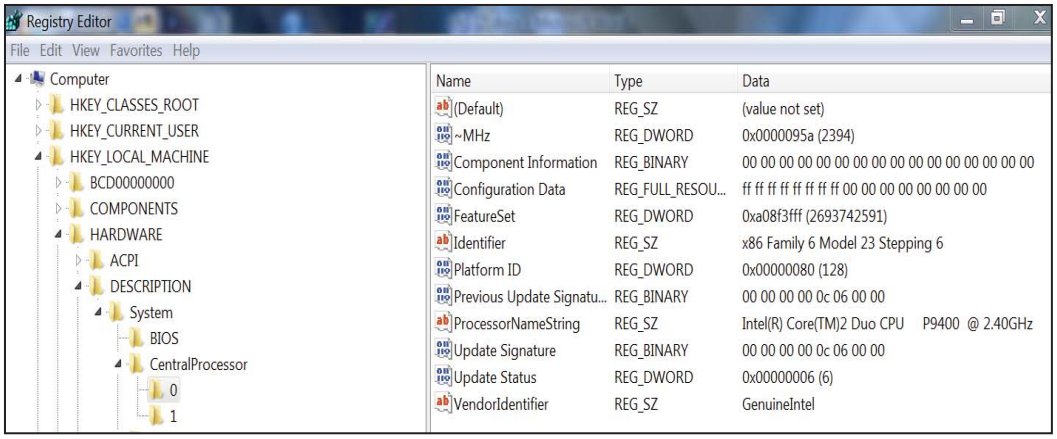

Figure 6: Central Processor description within Windows Registry

There are a number of elements of information about the user account that are stored in the Registry. For example a list of user accounts, last login time of each account, whether it requires a password, whether it is a disabled or enabled account and the method used to hash the password of the user account. All of this information is held in the following Registry key:

HKEY_LOCAL_MACHINE \SAM\Domains\Account\Users

Figure 7 shows details of a user account as it is viewed using the Access Data Windows Registry viewer.

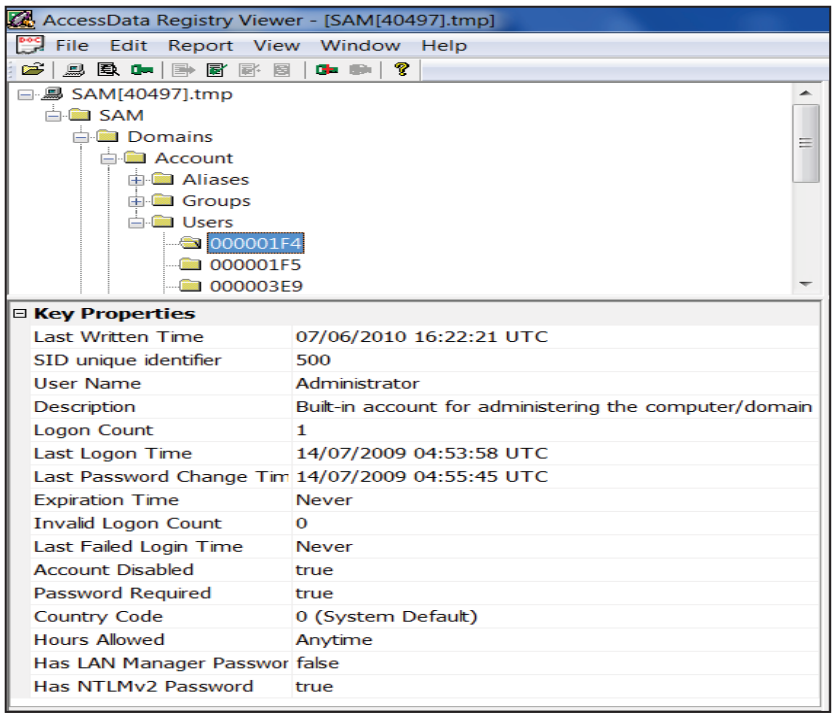

Figure 7: Details of a user account in Access Data Registry Viewer

In addition the user account names are listed in the following Registry key:

HKEY_LOCAL_MACHINE\SAM\Domains\Account\Users\Names

Figure 8 shows the user account names as they viewed using the Access Data Windows Registry viewer.

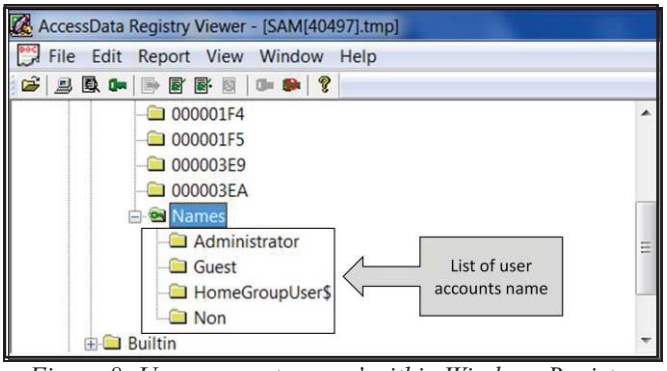

Figure 8: User account names' within Windows Registry

Other valuable information to a forensic investigator is the time of the last shutdown of the system. This information is stored in the ShutdownTime value in the following Windows Registry key:

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Windows

Figure 9 shows the ShutdownTime value as it is viewed using the Access Data Windows Registry viewer with the last written time which is referred to as the last shutdown time.

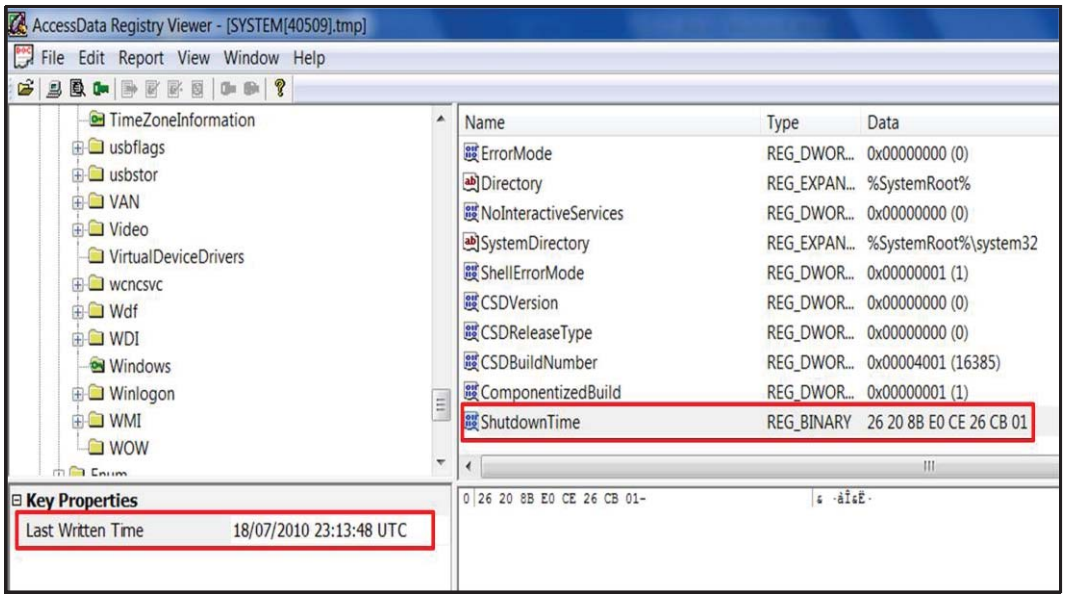

Figure 9: Shut down time value with Windows Registry

Application Analysis

a. Start up programs

The list of startup programs is showed in Figure 10 and listed in the following Windows Register key (Farmer, 2008):

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

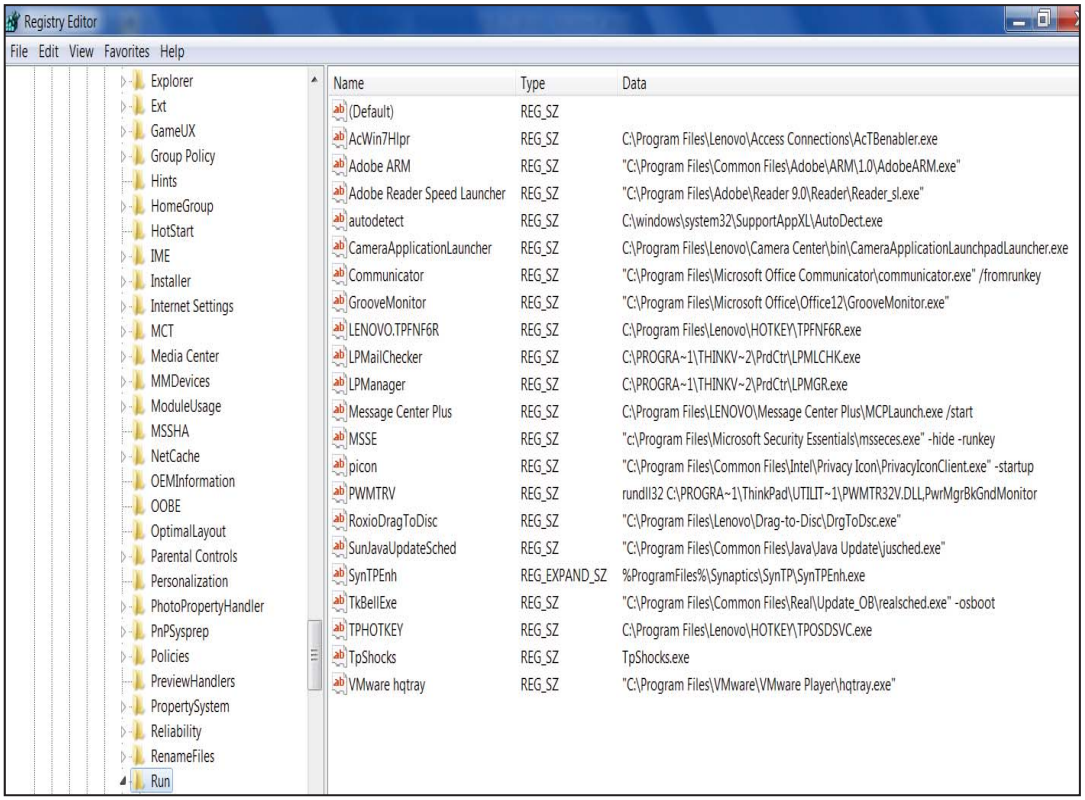

Figure 10: List of startup programs with Windows Registry

b. Registered Application

The list of registered application is showed in Figure 11 and listed in the following Register key:

HKEY_LOCAL_MACHINE\SOFTWARE\RegisteredApplications

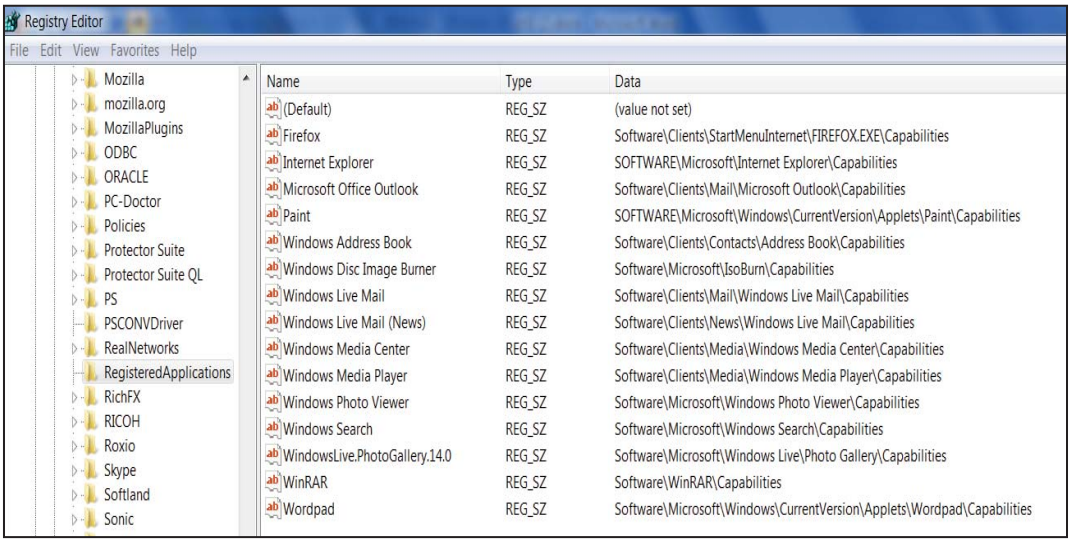

Figure 11: List of Registered application within Windows Registry

Windows Live Messenger analysis

Microsoft Windows Live Messenger is a well known chat application used by a large number of people. There are some elements of information of interest related to the Microsoft Windows Live messenger that are stored within the Registry. In simple terms, an MSN object is used to contain user settings when the application runs such as the background and displayed picture. This information is held in the value called UTL in the following Registry key:

HKEY_USERS\S-1-5-21–[UserIdentifier]\Software\Microsoft\
MSNMessenger\PerPassportSettings\[MSNMessengerAccountIdentifier]

Figure 12 shows the content of the UTL value.

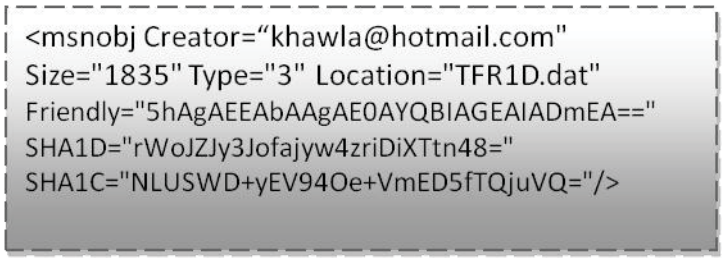

Figure 12: UTL value content

The following is a description of each field of an MSN object (MSN:P2P/Msnobj Description, 2009):

1. Creator: MSN messenger user account.
2. Size: The size of data that the object holds.
3. Type: Several types identifier are shown in Table1.

Table 1: Type field description of MSN object

Type no.	Description
1	Unknown
2	Custom Emoticons
3	Static display picture
4	Shared File
5	Static Backgrounds
6	Unknown
7	Dynamic display pictures
8	Wink
9	Map File
10	Dynamic Backgrounds
11	Voice Clip
12	State
13	Roaming Objects
14	Signature Sound
15	Unknown
16	Scene
17	Web cam Dynamic Display Picture

4. Location: The file name that holds the object.
5. Friendly: Encoded picture name using UTF-16.
6. SHA1D: SHA1 hash digest of the data
7. SHA1C: SHA1 hash digest of all previous fields of the MSN object

Skype analysis

Skype is another well known application that allows a user to make a voice or video call over IP based networks. In other words it is VoIP software. It is important for the forensics investigator to know whether the user of the system has been using this software. Also it is important to know the account name that the user of the system is using. If the Skype application is installed on the system, there will be a sub key in the software key of HKEY_LOCAL_MACHINE and HKEY_USERS\S-1-5-21-[User Identifier]\ for the Skype application. In this sub key the forensics investigator can find the most recent user of this application. The following Registry key holds the recent user value and the country code of the Skype application and it is shown in Figure 13:

HKEY_USERS\S-1-5-21-[User Identifier]\Software\Skype\PluginManager

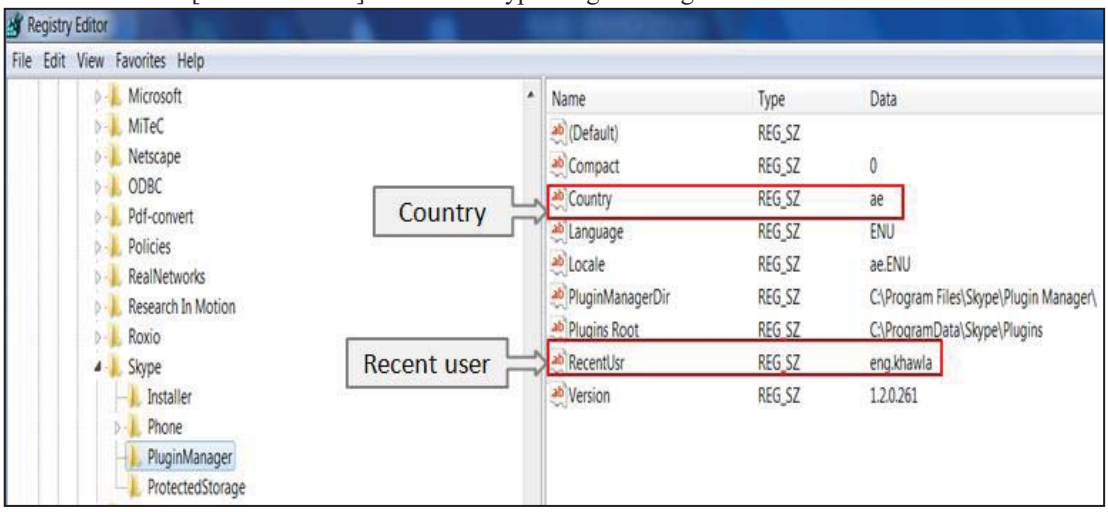

Figure 13: Interested information of Skype application within Windows Registry

Network Analysis

a. Network Cards

The Registry holds a list of all network cards whether the network card is built in or is an external network card. In most laptops there are two type of network card: the Ethernet network card and Wi-Fi network card. The following Registry key holds a list of network card:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkCards

b. Intranet Networks

The list of intranet network that the system has been connected to is stored within the Registry in the following key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Nla\Cache\Intranet

c. Wireless Networks

For any wireless networks that the system was connected to, the identifiers are stored in the following key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\ CurrentVersion\NetworkList\Nla\Wireless

This key is just a list of identifiers for each of the wireless networks that the system has been connected to. More information about each of these wireless networks such as the MAC address of the default gateway, DNS suffix and SSID can also be found within the Registry. This can be done by linking the identifier from the previous key to the following Windows Registry key and is shown in Figure 14. This key holds a great deal of information about the networks in general rather than just about wireless networks.

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged

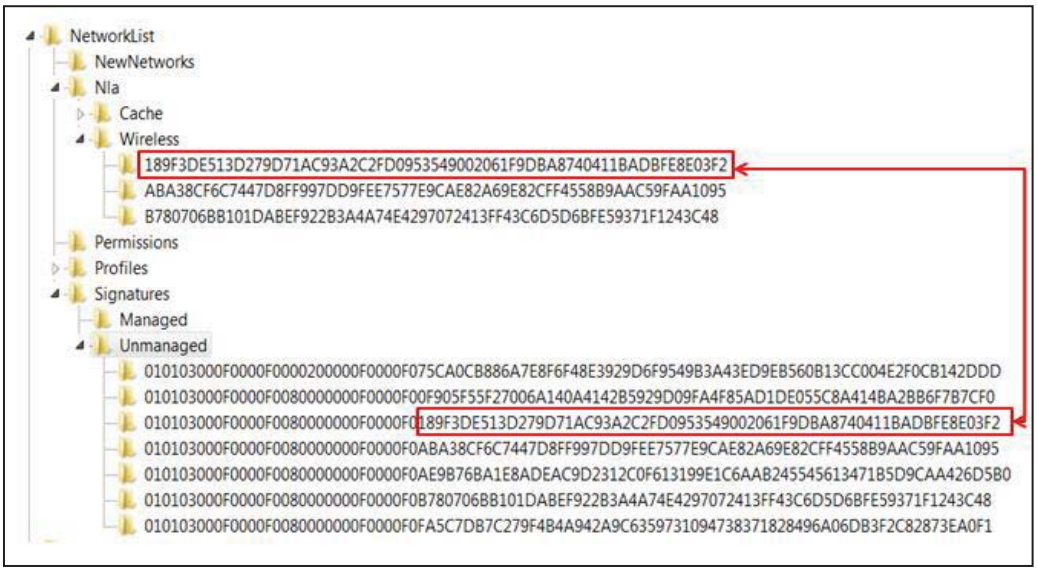

Figure 14: Matching Wireless network identifier within Windows Registry

In addition, the Windows Registry holds important information for the forensic investigator about Wireless networks. This information includes the created date and last connected date. They are stored in the following Registry sub key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{Wireless - Identifier}

The value DateCreated holds the created date of a specific wireless network and the value DateLastConnected holds the last date that the computer was connected to this wireless network as shown in Figure 15.

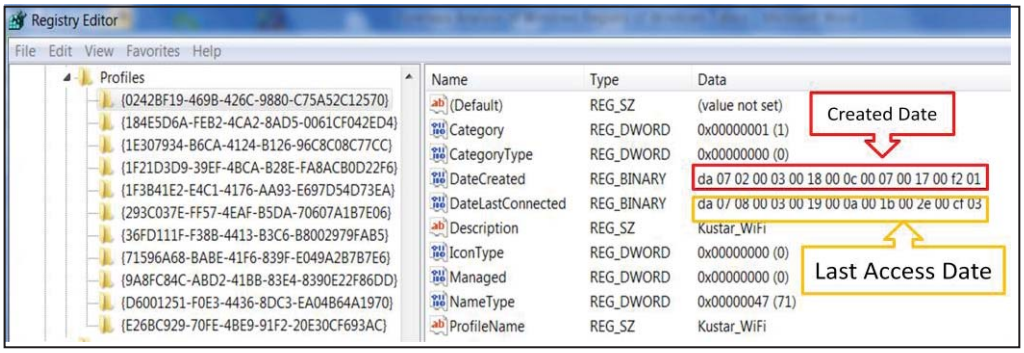

Figure 15: Created date and last connected date of Wireless network

The type of these values is binary data type. The following is an explanation how to view these values as a normal date time (Decoding the DateCreated and DateLastConnected SSID values From Vista/Win 7, 2010) :

1. The length of data of value is 16 bytes.
2. It stored using Little Endian, so convert it to big Endian before decoding the data as shown in Figure 16:

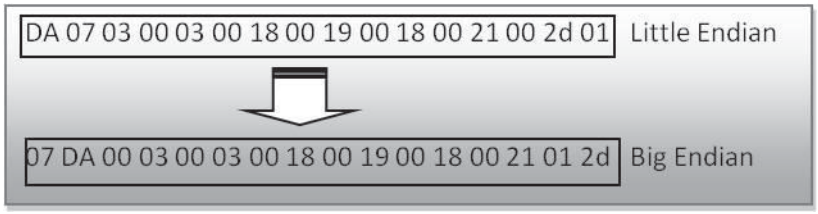

Figure 16: Convert DateCreated Registry value to big Endian format

3. The year value = 07D = 2010
   (Ignore last hex value which is [A] in the first two bytes)
4. The month = 00 03 = March
   (1= January, 2= February ...etc)
5. Each two bytes has a corresponding value for the year, month, date, hour, minute and second.
6. The weekday = 00 03 = Wednesday
   (0 = Sunday, 1 = Monday ...etc)
7. The date = 00 18 = 18th
8. The hour = 00 19 = 19:00 or 7:00 pm
9. The minutes = 00 18 = 18 minutes
10. The second = 00 21= 21 seconds

Consequently, the decoded date is: 18th, March, 2010 19:18:21

Attached device analysis

a. Printers

There are a number of keys within the Registry that hold information about printer drivers that exist in the system. One of these keys is the following:

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Print\Printers

This key lists printer drivers that exist in the system. The investigator can get more information about each printer driver if he accesses the PrinterDriverData sub key. For example, installed date and model name as shown in Figure 17.

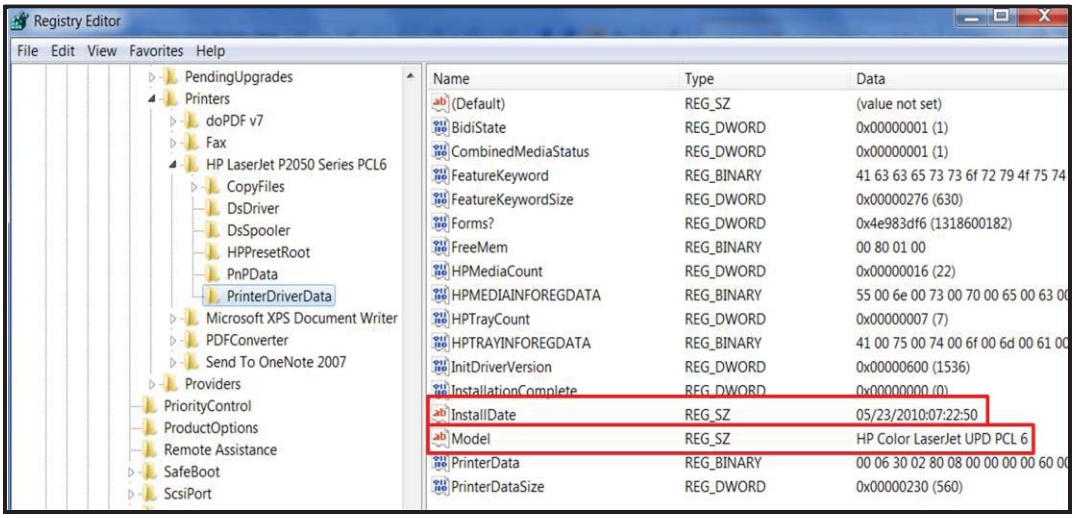

Figure 17: Valuable forensics elements of printer drive within Windows Registry

b. USB Devices

Any time a new USB Device is connected to the system, it will leave information about this USB device within the Registry. This information can uniquely identify each USB device connected to the system. The Windows Operating system stores vendor ID, product ID, Revision and Serial No. for each connected USB device. This information can be found in the following Registry key (Carvey & Kleiman, 2007):

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USBSTOR

Figure 18 shows how information about USB devices stored in the previous key.

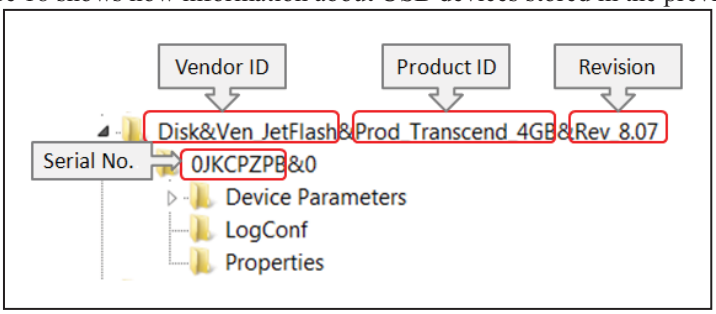

Figure 18: USB device information within Windows Registry

HISTORY LIST

The history lists highlights the most recent activity on the system. For example recently visited web pages or recently opened word files. There are several sub keys in the Registry that show recent activity by the system users. Table 2 represents the history list with corresponding sub keys in the Windows Registry.

Table 2: History lists

History list	Related windows registry sub key
Typed URLs in Microsoft Internet Explorer	HKEY_USERS\S-1-5-21-[User Identifier] \Software\Microsoft\Internet Explorer\TypedURLs
Most recently used Microsoft Word files	HKEY_USERS\S-1-5-21-[User Identifier] \Software \Microsoft\Office \12.0\Word\File MRU
Most recently used Microsoft Power Point files	HKEY_USERS\S-1-5-21-[User Identifier] \Software\Microsoft \Office \12.0\PowerPoint\File MRU
Most recently used Microsoft Excel files	HKEY_USERS\S-1-5-21-[User Identifier] \Software \Microsoft \Office \12.0\Excel\File MRU
Recent Acrobat Reader files	HKEY_USERS\S-1-5-21-[User Identifier]\Software\Adobe\Acrobat Reader\9.0\AVGeneral\cRecentFiles
Recent WinRAR files	HKEY_USERS\S-1-5-21-[User Identifier] \Software \WinRAR \ArcHistory
Most recently mapped network	HKEY_USERS\S-1-5-21-[User Identifier] \Software \Microsoft \Windows\CurrentVersion\Explorer\Map Network Drive MRU
Most recently used wallpapers in the desktop	HKEY_USERS\S-1-5-21-[User Identifer] \Software \Microsoft \Windows\CurrentVersion\Explorer\Wallpaper\MRU
Most recently typed command on the RUN dialog	HKEY_USERS\S-1-5-21-[User Identifier] \Software \Microsoft \Windows\CurrentVersion\Explorer\RunMRU
Recent .GIF files	HKEY_USERS\S-1-5-21-[User Identifier] \Software \Microsoft \Windows\CurrentVersion\Explorer\RecentDocs\.gif
Recent .jpg files	HKEY_USERS\S-1-5-21-[User Identifier] \Software \Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.jpg
Recent text files	HKEY_USERS\S-1-5-21-[User Identifier] \Software \Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.txt
Recent folders	HKEY_USERS\S-1-5-21-[User Identifier] \Software \Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\Folder
Recent Zip files	HKEY_USERS\S-1-5-21-[User Identifier] \Software \Microsoft \Windows\CurrentVersion\Explorer\RecentDocs\.zip

THE VALUE OF THE FORENSIC ANALYSIS OF THE WINDOWS REGISTRY

A systems analysis provides the forensic investigator valuable information about the system. It gives the forensic investigator a picture about the computing capabilities of the suspect machine such as the processor name, processor speed, system family, system name and system version. Beside this, the forensic investigator will get an investigation of the names, identities or nick names of people who were using suspect machines from the computer name and a list of user accounts. Moreover, the extracted last shutdown time will give the forensic investigator information about the last time the suspect machine was used. For example, this may indicate that this machine is not related to this crime.

The application analysis provides the forensic investigator worthwhile information about the applications that were installed in the suspect machine. The forensic investigator should check the startup programs, as they may contain malicious programs that could control the suspect machine and the system may have been run by an attacker rather than the user of the suspect machine. For instance, if the suspect machine was used to perform a crime such as DoS attack, the user of the system may not be the criminal who performed this attack. It may have been done by a criminal who was in control of the suspect machine. There is a list of some of the malware that may exist in the startup programs at (Forrest, Denham, Prevost, & Klein, 2010). Moreover, the forensic investigator may discover programs that have been used to perform a crime. For example in the case of software piracy, the criminal may use CD and DVD burners and labels. Also, the criminal may use software activation codes and software duplication codes. Thus, if the forensic investigator found any of the above programs, it can be considered as potential digital evidence in the crime. Furthermore, the forensic investigator will be interested to know whether the user of suspect machine used a chat application such as Microsoft Windows Live Messenger and Skype. It is also important to know the account name that the user of the suspect machine was using. For example, in cases involving child abuse, the criminal may communicate with the child using Microsoft Windows Live Messenger and Skype. Knowing the criminal's account name from the contact list of

the child and then finding the criminal account as a recent user or saved account in the suspect machine is considered as potential digital evidence.

Network analysis will give the forensic investigator an overview of networking activities that were performed by the suspect machine. From the list of network cards, the forensic investigator can identify all of the cards that were used by the system whether they were built in the system or externally attached to the system. Also, he will gain any list intranets that the suspect machine was connected to. Moreover, he will gain valuable information about the wireless networks that the system connected to including the profile names of any wireless networks, the created date and the last connected date.

The analysis of the attached devices will give the forensic investigator information about the devices that have been connected to the system. It includes two categories of attached devices, printers and USB devices. The list of printers and their information such as model name and installed date are valuable information to a forensic investigator and could be considered as potential digital evidence. For instance in a counterfeiting crime, the criminal will normally use high quality printers to produce a credit card that looks like the original. Furthermore, it's important to a forensic investigator to know what USB devices have been attached to the system and information such as product ID and serial No. especially in the case of the theft of data from a computer.

The history list provides the forensic investigator with the most recent activity on the system by each user, such as typed URLs in Microsoft Internet Explorer and most recently used Microsoft Word files. The typed URLs in Microsoft Internet Explorer can provide the forensic investigator with potential digital evidence in several types of computer crimes such as child abuse, computer intrusion, murder and harassment. The recent .jpg files and recent .GIF files can provide the forensic investigator with potential digital evidence about opened images in child abuse crime. In identity theft, counterfeiting and terrorism crimes, the criminal may store credit card information which has been used to transfer money in a text or word files. I have mentioned the location of the most recent used word files or .txt file with the Windows Registry in Table 2.

IMPLEMENTATION OF WINDOWS REGISTRY FORENSICS TOOL

As a result of this research, a tool has been created to extract potentially significant elements of information that may be valuable to forensic investigators from the hive files of the Windows 7 Registry and present them in a form that is useful to the investigator. The tool was implemented using Visual Basic .NET programming language. The tool uses several API functions to retrieve data from complex data structure of the Windows Registry hive files which are:

1. RegLoadKey
   This function is used to load hive files into the live system to start analysing them.
2. RegUnLoadKey
   This function is used to unload the loaded hive files from live system.

Importing the Microsoft.Win32 name space into Visual Basic .NET project, allows the use of various functions to deal with hive files that are loaded in the live system such as (RegistryKey Methods, 2010):

1. OpenSubKey
   This function allows the application to use a specified sub key in read-only mode.
2. GetSubKeyNames
   This function is used to retrieve a list of sub key names of the specified key.
3. GetValue
   This function is used to retrieve data of the specified value of a Registry key.
4. GetValueNames
   This function is used to retrieve a list of all values name of the specified key.
5. Close
   This function is used to close the Registry key that is opened previously by OpenSubKey.

The following figures are snapshots from the Windows Registry Forensics Tool which has been called the KUSTAR Windows Registry Forensics Tool. Figures 19 to 22 show screenshots of the tool.

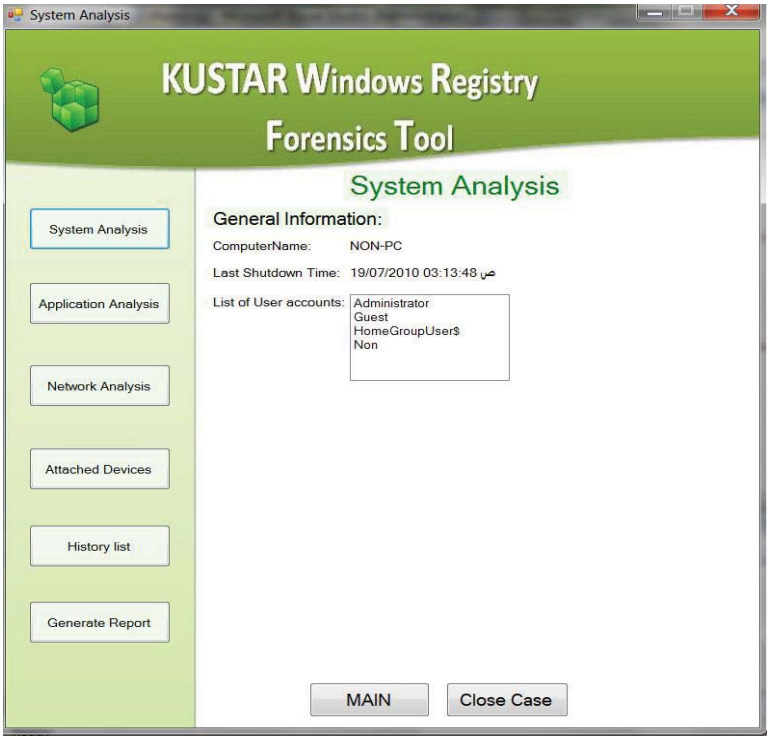

Figure 19: System Analysis window

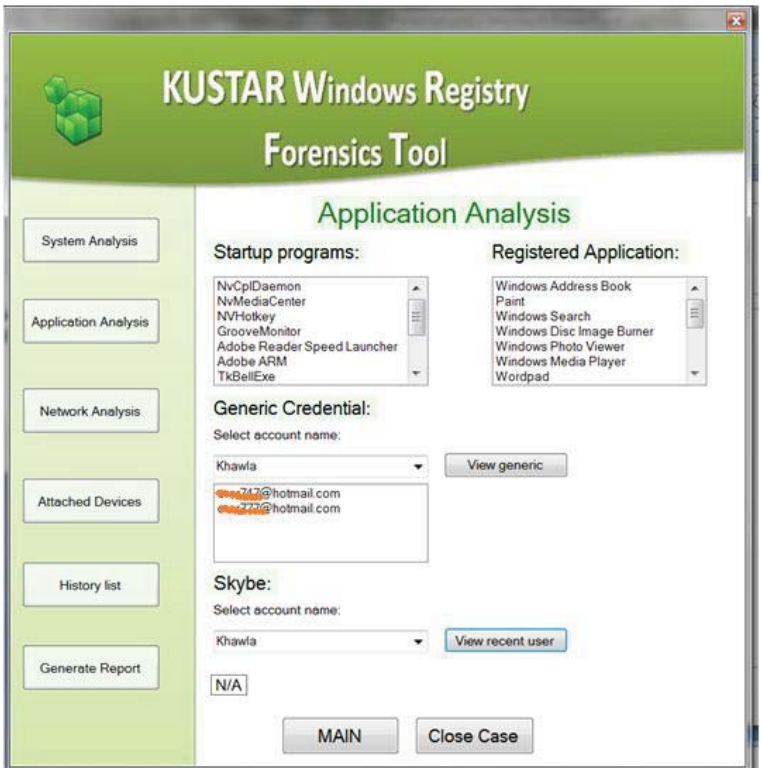

Figure 20: Application analysis window

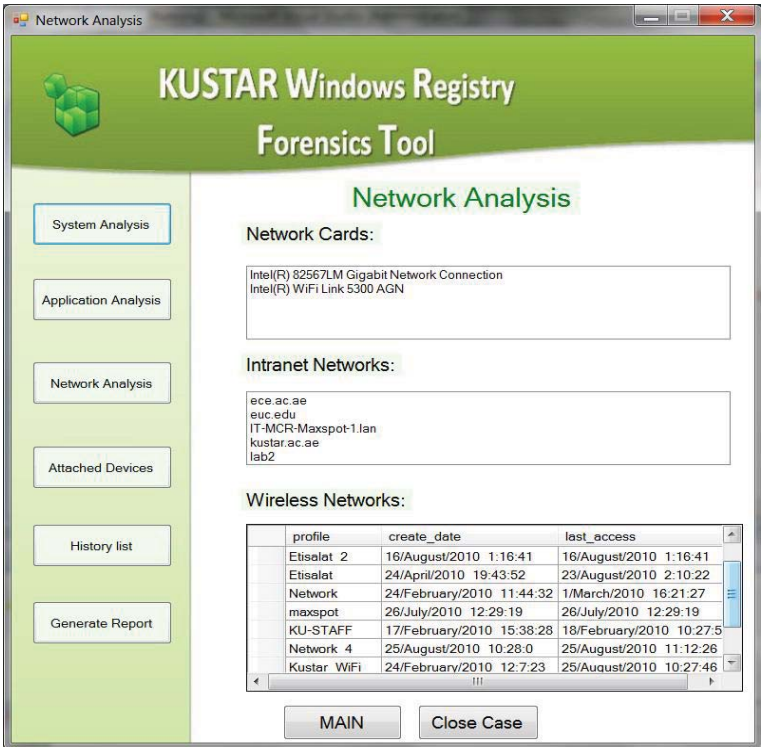

Figure 21: Network analysis window

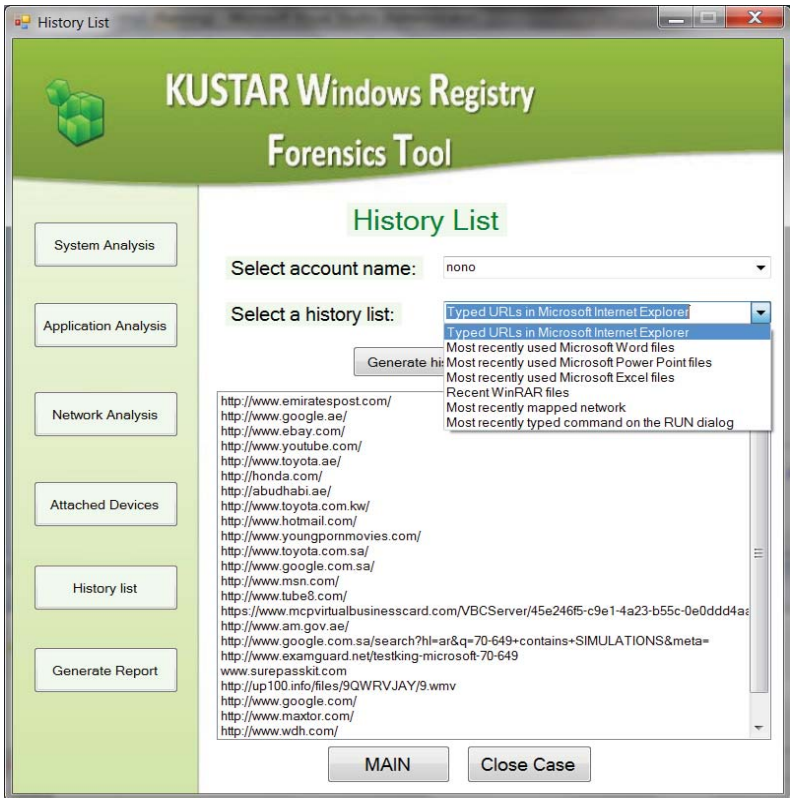

Figure 22: History list window

CONCLUSION

The Windows Registry is a database that has been implemented in the Microsoft Windows operating system to hold the settings and configuration of the system hardware, applications and users profiles. It is generally accepted that the Windows Registry holds several potentially significant elements of information that may be valuable to forensic investigators.

The identification and recovery of evidence from storage media that is constantly increasing in size is a time consuming process. There are several elements that can be valuable to the forensic investigators that are contained within Windows Registry, and it may help to reduce the time taken for an investigation if the investigator carries out an initial search of this repository. Once the investigator has found the relevant information, it may help to guide further work and provide information that was not available from other sources. Consequently, the investigation process could take less time and become simpler.

REFERENCES

(November 2009). *An on the Scene Reference for First Responders.* The National Institute of Justice.

Carvey, H., & Kleiman, D. (2007). Windows Forensic Analysis. Syngress Publishing.

Decoding the DateCreated and DateLastConnected SSID values From Vista/Win 7. (2010, February 12). Retrieved August 5, 2010, from securitybananas.com: http://securitybananas.com/?p=225

Dwyer, P. c. (2010, March 19). Cyber Crime in the middle east.

Farmer, D. J. (2008). *A Windows Registry Quick-Reference.*

Forrest, P., Denham, D., Prevost, S., & Klein, T. (2010, October 29). *Starup Application list*. Retrieved November 1, 2010, from SYSINFO: http://www.sysinfo.org/startuplist.php

Honeycutt, J. (2005). Microsoft Windows Registry Guide. Microsoft Press.

Kokoreva, O. (2002). Windows XP Registry. A-LIST.

Michael Solomon, D. B. (2005). *Computer Forensics, jump start.* SYBEX.

Microsoft Computer Dictionary. (2002). Microsoft Press.

MSN:P2P/Msnobj Description. (2009, June 22). Retrieved June 22, 2010, from OpenIM wiki: http://imfreedom.org/wiki/MSN:P2P/Msnobj_Description

RegistryKey Methods. (n.d.). Retrieved August 21, 2010, from MSDN: http://msdn.microsoft.com/en-us/library/microsoft.win32.registrykey_methods.aspx

Solomon, M., Barrett, D., & Broom, N. (2005). In *Computer Forensics JumpStart* (pp. 73-155). SYBEX.

Thomas, P., & Marris, A. (2008). An Investigation into Development of Anti-Forensic Tool to Obscure USB Flash Drive Device Information on a Windows XP Platform. *Third International Annual Workshop on Digital Forensics and Incident Analysis* (pp. 60-66). IEEE.

Vacca, J. R. (2010). *Computer Forensic, computer crime scene investigation.* Charles River Media.