A Practical Approach for Evidence Gathering in Windows Environment

Kaveesh Dashora
Department of Computer Science & Engineering
Maulana Azad National Institute of Technology
Bhopal, India

Deepak Singh Tomar
Department of Computer Science & Engineering
Maulana Azad National Institute of Technology
Bhopal, India

J.L. Rana
Department of Computer Science & Engineering
Maulana Azad National Institute of Technology
Bhopal, India

ABSTRACT
With theincrease in internet technology cyber-attacks have also increased, most of the sufferers from these cyber-attacks are novice windows end users. Windows is more popular due to the ease in use, and effective GUI; due to the unavailability of windows component source code the crime investigations in windows environment is a tedious and hectic job for law enforcement agencies. The unsystematic organization of the available sources of evidence in a windows environment makes the integration of these evidences a difficult task. In this paper a prototype model is developed and implemented to extract the various sources of evidence in windows environment. Investigation issues in Windows and Linux environment are also presented.

Keywords
Log File; Windows Registry Analysis; Operating System Forensics; Windows Event Logs; Evidence Collection.

1. INTRODUCTION
Computer forensics is concerned with the analysis of a computer system and a network suspected of being involved in criminal activity. The major target of the investigation is to find data and information that are important for the case under study or investigation. The main emphasis is the investigation is on the "convicting information present in the system" and "entry points for the convicting information".

Windows Forensics Process analyses the evidences gathered from the operating system activity. These evidences are generally present in Event Logs, Slack Space, Windows Registry and Temporary Files. Files that are related to the Windows Environment are collected with outmost Importance. The Event Logs captures data related to all of the events which may or may not affect the system, e.g. Change of Permission, User Logon/Logoff etc. The Windows Registry keeps a track recently accessed files/folders, user's preferences. The Windows Operating System has many places from where evidence can be extracted.[1],[2].

2. NEED OF FORENSICS IN WINDOWS ENVIRONMENT
Windows Forensics adds the ability of providing sound computer forensics. This helps to ensure the overall integrity and survivability of network infrastructure. If you consider computer forensics as a new basic element i.e. "defense-in-depth" approach to network and computer security then you can help in an organization's data integrity. The computer forensics must be practiced responsibly otherwise, there is a risk of destroying vital evidences or forensic evidence ruled inadmissible in the court of law. Also, you or your organization may run afoul of new laws that mandate regulatory compliance and assign liability if certain types of data are not adequately protected.

Identification, collection, presentation and analysis of data such that integrity of evidence collected is preserved and can be presented effectively in the court of law. This is the major task performed in computer forensics. There are two typical aspects of a computer forensic investigation. Firstly, the investigators have to understand the kind of potential evidence they are looking for such that they may identify the areas to be searched. Digital crimes have a large spectrum of variation in criminal activities from child pornography to theft of personal data to destruction of intellectual property. Secondly, the tools to be used for investigation are given proper importance. Recovery of detailed damaged or encrypted files is required so investigator must be familiar with all such approaches.

The collection of ephemeral data is one of the important tasks that are required to be performed by an investigator. The data which is present in hard disk and secondary storage is persistent but the data present in RAM, registers, cache is volatile. This volatile data is ephemeral and is to be taken care of.[3],[4]

3. WINDOWS FORENSICS VS LINUX FORENSICS
Table I.
Windows Forensics vs. Linux Forensics

	Windows Forensics	Linux Forensics
1	Windows is not open source	Linux is open source
2	Custom tools cannot be added to the windows environment as source code modification is not possible	Custom tools can be added to the Linux environment as it is source code is available
3	The Complete Windows Registry cannot be accessed completely at a time due to access restrictions	The Complete Linux Registry can be accessed easily.
4	The windows registry is stored in a single file which makes it easier to gather	Linux registry is stored in different folders making it a secure

	evidence	
5	Windows maintains different event logs for different purposes	Linux maintains only a single syslog with different levels of information

4. SOURCES OF EVIDENCE IN WINDOWS ENVIORNMENT

In our previous work [9] various locations were shown which can be looked for forensics investigations. Some of them are as follows. The Author in [5] has also elaborated some forensically important locations in Windows Registry and other places.

4.1 Windows Event Logs

The information present in the event logs is useful, especially when it comes to gathering evidence for forensic investigations related to malicious attacks intrusive actions of fraudulent behavior. The windows event logs are considered as important sources of forensic information as they relate certain events to particular point in time.

The windows operating system is built on a complex architecture with which to handle events like logging on requires proper security measures. It is also possible that the windows event logs are targeted to specific kind of events. The system logs and application logs can be used in a number of ways of writing specific events to the log. Windows also has a specific type of logging, the security logging system, which can only be written by the Local Security Authority Subsystem Service or LSASS.

Security policy of Windows Operating System is implemented by the LSASS process which is a vital part of security structure of Windows Operating System. The various functionalities that are provided by LSASS are for example, the verification of users logging on to the Windows system, handling password changes, creating access tokens and consequently writing entries to the Windows Security Log.

The windows event logging system logs events like account logon, account management, directory service access, object access, policy change, privilege use, process tracking, system

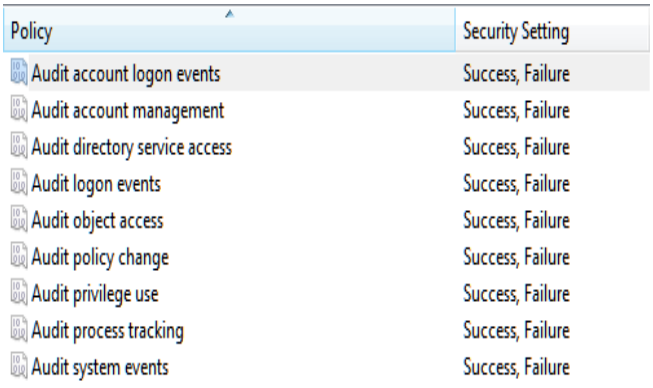

Fig. 1.Different types of Audit options for Windows Event Log.

events. Fig. 1 shows different types of logging options for Windows Event Log.

4.2 Windows Registry

The Windows Registry shown in Fig. 2 contains important information about the software installed on the computer; it also keeps a track of user's activities whichis important for forensics operation. Some keys present in the registry are application specific and some are general keys. Some of the important keys present in the registry are.

4.2.1 Run MRU:

This Registry Key stores information about the recently typed commands from the run window. This information is important for the examination of a computer forensics operation.

```
Computer\HKEY_CURRENT_USER\Software\Microsof
t\Windows\CurrentVersion\Explorer\RunMRU
```

4.2.2 Startup Objects:

These are the objects which are set to start automatically when windows start.This information is stored in various registry hives,

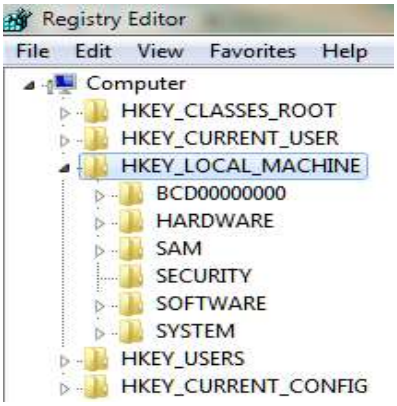

Fig. 2. Different Hives present in the Windows Registry.

i.e.

```
Computer\HKCU\<SID>\SOFTWARE\Microsoft\Windo
ws\CurrentVersion\Run
Computer\HKLM\SOFTWARE\Microsoft\Windows\Cur
rentVersion\Run
```

4.2.3 Last Accessed Key in Registry:

This key gives the information about what registry key was accessed last time.

```
Computer\HKEY_CURRENT_USER\Software\Microsof
t\Windows\CurrentVersion\Applets\Regedit
```

4.2.4 Internet Explorer Typed in Addresses:

This key gives the user information about what were the typed in websites from the Internet Explorer Address Bar.

```
Computer\HKEY_CURRENT_USER\Software\Microsof
t\Internet Explorer\TypedUrls
```

4.2.5 Last Saved Directory in Internet Explorer:

This key gives the user information about in which folder was the last downloaded file saved.

```
Computer\HKEY_CURRENT_USER\Software\Microsof
t\Internet Explorer – Download Directory
```

4.3 Volatile Data

This keeps the information about the environmental volatile data which is lost when the computer shuts down.

4.3.1 Running Processes:

These are processes which are currently active and running in the computer.

4.3.2 Recent Items:

This gives the information about the recently accessed files/folders on the computer.

5. POSSIBLE ATTACK SCENARIO AND THEIR RELATED EVIDENCES IN WINDOWS ENVIRONMENT

Windows environment is prone to many type of attacks, remote or local, each attack is done to perform some specific tasks one or the other way. The tasks may be like, luring the user to open a malicious website, send a malicious file through email, Logging on to the system, deleting/modifying/renaming files, creating files, starting or stopping Processes/Services etc. For these types tasks their related evidences are as under.

5.1 Opening a Website

Evidence can be found in Internet Explorer History and the Windows Registry.

5.2 Opening an E-Mail

Evidence can be found by taking an audit of all the E-Mails.

5.3 Logon/Logoff

Evidence can be found in the Windows Security Event Logs.

5.4 Attacker adds malicious files or deletes/changes/renames the important/critical system files

Evidence can be found out at the Windows Security Event Logs and File System/Process Logger Logs.

5.5 The attacker reads some private information from the windows system files

Evidence can be found out at the Windows Security Event Logs and File System/Process Logger Logs.

5.6 The Attacker changes registry keys

Evidence can be found out at the registry last viewed key in the Windows Registry.

5.7 The Attacker starts/stops processes/services

Evidence can be found out at the File System/Process Logger Logs.

Evidence can be found out at the Windows Security and Application Logs.

6. WINDOWS FORENSICS TOOLS

Many Tools have been developed to perform Windows Forensics some of them are:

6.1 Access Data – Forensic Toolkit

AccessData has pioneered digital investigations for more than twenty years, delivering the technology and training that empowers law enforcement, government agencies and corporations to perform exhaustive computer investigations of any type with speed and efficiency. Accepted all over the world as an industry leader, AccessData delivers state-of-the-art computer forensic, network forensic, eDiscovery, password cracking and decryption solutions. Its Forensic Toolkit® and network-enabled enterprise solutions allows establishments to preview, search for, forensically preserve, process, examine and produce electronic evidence. [6]

6.2 Guidance Software – Encase

Guidance Software is distinguished worldwide as the leader in eDiscovery and other digital investigations. Their EnCase® software solutions offer the basis for government and law enforcement agencies to perform detailed and effective computer investigations of any kind, including intellectual property theft, incident response, compliance auditing and responding to eDiscovery requests.[7]

6.3 Sysinternals – FileMon File Monitor

Sysinternals is a set of tools produced by the Microsoft Sys-Internals team and Mark Russinovich. This tool is used to view and collect volatile information about windows registry.[8]

7. IMPLEMENTATION

For conducting effective investigation process in windows environment a tool Windows Forensics Analyzer (WFA) is developed and implemented. To implement the WFAtool laboratory environment has been set up by using the C#.NET 2.0. This tool utilizes the WMI Library to extract the evidences.

Sort Entries By: All Rows | Refresh

Type	Time Generated	Time Written	Source	Category	Event
FailureAudit	04-08-2010 19:22:01	04-08-2010 19:22:01	Microsoft-Windows-Security-Auditing	(13571)	4957
FailureAudit	04-08-2010 19:22:01	04-08-2010 19:22:01	Microsoft-Windows-Security-Auditing	(13571)	4957
FailureAudit	04-08-2010 19:22:01	04-08-2010 19:22:01	Microsoft-Windows-Security-Auditing	(13571)	4957
FailureAudit	04-08-2010 19:22:01	04-08-2010 19:22:01	Microsoft-Windows-Security-Auditing	(13571)	4957
FailureAudit	04-08-2010 19:22:01	04-08-2010 19:22:01	Microsoft-Windows-Security-Auditing	(13571)	4957
FailureAudit	04-08-2010 19:22:01	04-08-2010 19:22:01	Microsoft-Windows-Security-Auditing	(13571)	4957
FailureAudit	04-08-2010 19:22:01	04-08-2010 19:22:01	Microsoft-Windows-Security-Auditing	(13571)	4957
FailureAudit	04-08-2010 19:22:01	04-08-2010 19:22:01	Microsoft-Windows-Security-Auditing	(13571)	4957
FailureAudit	04-08-2010 19:22:01	04-08-2010 19:22:01	Microsoft-Windows-Security-Auditing	(13571)	4957
SuccessAudit	04-08-2010 19:22:01	04-08-2010 19:22:01	Microsoft-Windows-Security-Auditing	(13573)	5447
SuccessAudit	04-08-2010 19:22:01	04-08-2010 19:22:01	Microsoft-Windows-Security-Auditing	(13573)	5447
SuccessAudit	04-08-2010 19:22:01	04-08-2010 19:22:01	Microsoft-Windows-Security-Auditing	(13573)	5447
SuccessAudit	04-08-2010 19:22:01	04-08-2010 19:22:01	Microsoft-Windows-Security-Auditing	(13573)	5447
SuccessAudit	04-08-2010 19:22:01	04-08-2010 19:22:01	Microsoft-Windows-Security-Auditing	(13573)	5447
SuccessAudit	04-08-2010 19:22:01	04-08-2010 19:22:01	Microsoft-Windows-Security-Auditing	(13573)	5447
SuccessAudit	04-08-2010 19:22:01	04-08-2010 19:22:01	Microsoft-Windows-Security-Auditing	(13573)	5447
SuccessAudit	04-08-2010 19:22:01	04-08-2010 19:22:01	Microsoft-Windows-Security-Auditing	(13573)	5447
SuccessAudit	04-08-2010 19:22:01	04-08-2010 19:22:01	Microsoft-Windows-Security-Auditing	(13573)	5447
SuccessAudit	04-08-2010 19:22:01	04-08-2010 19:22:01	Microsoft-Windows-Security-Auditing	(13573)	5447
SuccessAudit	04-08-2010 19:22:01	04-08-2010 19:22:01	Microsoft-Windows-Security-Auditing	(13573)	5447

Fig. 3.Windows Event Logs in WFA.

Sort Entries By: Source | All Rows | Refresh

Value Name	Item	Extra Information
m	D:\WebGoat-5.3_RC1\tomcat\webapps\webgoat\lesson_plans\English	1
p	C:\Users\Kaveesh Swarish\Documents\Downloads	1
o	C:\Users\Kaveesh Swarish\AppData\Roaming	1
n	bittorrent	1
l	\\KAVEESHSWARI-PC	1
b	explorer	1
k	winver	1
j	wmplayer	1
i	\\nikhil-PC	1
h	\Documents and Settings	1
g	regedit	1
f	F:\Downloads	1
c	notepad	1
e	calc	1
d	mspaint	1
a	D:\Downloads	1
MRUList	mponlbkjihgfceda	

Fig. 4.Windows Registry in WFA.

Sort Entries By: All Rows | All Rows | Refresh

Process Name	Owner	Creation Class Name	Creation Date	Machine Name	Process Path
System Idle Process		Win32_Process		KAVEESHSWARI-PC	
System		Win32_Process	20100619144412.109375+330	KAVEESHSWARI-PC	
smss.exe	SYSTEM	Win32_Process	20100619144412.125000+330	KAVEESHSWARI-PC	
csrss.exe	SYSTEM	Win32_Process	20100619144426.359375+330	KAVEESHSWARI-PC	C:\Windows\system32\csrss.exe
wininit.exe	SYSTEM	Win32_Process	20100619144429.515625+330	KAVEESHSWARI-PC	C:\Windows\system32\wininit.exe
csrss.exe	SYSTEM	Win32_Process	20100619144429.515625+330	KAVEESHSWARI-PC	C:\Windows\system32\csrss.exe
winlogon.exe	SYSTEM	Win32_Process	20100619144430.578125+330	KAVEESHSWARI-PC	C:\Windows\system32\winlogon.exe
services.exe	SYSTEM	Win32_Process	20100619144431.984375+330	KAVEESHSWARI-PC	C:\Windows\system32\services.exe
lsass.exe	SYSTEM	Win32_Process	20100619144432.312500+330	KAVEESHSWARI-PC	C:\Windows\system32\lsass.exe
lsm.exe	SYSTEM	Win32_Process	20100619144432.328125+330	KAVEESHSWARI-PC	C:\Windows\system32\lsm.exe
svchost.exe	SYSTEM	Win32_Process	20100619144432.609375+330	KAVEESHSWARI-PC	C:\Windows\system32\svchost.exe
svchost.exe	NETWORK SERVICE	Win32_Process	20100619144432.953125+330	KAVEESHSWARI-PC	C:\Windows\system32\svchost.exe
atiesrxx.exe	SYSTEM	Win32_Process	20100619144433.078125+330	KAVEESHSWARI-PC	C:\Windows\system32\atiesrxx.exe
svchost.exe	LOCAL SERVICE	Win32_Process	20100619144433.406250+330	KAVEESHSWARI-PC	C:\Windows\System32\svchost.exe
svchost.exe	SYSTEM	Win32_Process	20100619144433.531250+330	KAVEESHSWARI-PC	C:\Windows\System32\svchost.exe
svchost.exe	SYSTEM	Win32_Process	20100619144433.562500+330	KAVEESHSWARI-PC	C:\Windows\system32\svchost.exe

Fig.5.Volatile Information: Running Processes in WFA.

Item Name	Last Accessed Date
M:\Intel 32	17-06-2010 10:12:28 PM
D:\Games\UBISOFT\Prince of Persia The Sands of Time\Video\Intro.int	14-06-2010 8:43:56 AM
P:\Kavish\Introduction.docx	18-06-2010 7:01:46 AM
L:\New Folder\New Folder\Desktop\JavaApplication7.rar	17-06-2010 12:27:17 PM
D:\WebGoat-5.3_RC1\tomcat\webapps\webgoat\javascript\javascript.js	11-06-2010 12:46:51 PM
D:\Downloads\K'naan - Wavin' Flag [FIFA World Cup 2010] HQ MUSIC VIDEO H264 AAC [JAGUAR7]""	19-06-2010 2:31:39 PM

Fig. 6.Volatile Information: Recent Files and Folders

This tool provides a platform such that all of the important information for evidence collection can be collected at central zone. This tool extracts information from the Windows Event Logs, Windows Registry and the Volatile Evidences. The functionality details of WFA in windows environment are as follows.

7.1 Evidence extraction from Windows Event Logs

The windows forensics analyzer can be used to extract the windows event logs as shown in fig. 3. The windows forensics analyser first checks for all of the available windows event logs and then it give the user option to view them. The Logs can also be filtered on the basis of Entry Type, Source and Category.

7.2 Evidence Extraction from Windows Registry

Windows Registry has many sources of forensic evidence; some of the important evidences have been gathered by the Windows Forensics Analyzer, they are Run MRU, Start-up Objects, Registry Last Viewed Key, Registry Favorites, List of Typed addressed in Internet Explorer, Name of the folder to which the last downloaded file was saved, etc.

7.3 Evidence Extraction of the Volatile Information

7.3.1 Volatile Information – Running Processes:

As shown in Fig 5, the Windows Forensics Analyzer also checks the presently running processes through the WMI registry and gives a report for the same.

7.3.2 Volatile Information – Recent Files and Folders:

As shown in Fig. 6, the Windows Forensics Analyzer also looks up into the Windows Recent Folder, it takes all of the .lnk(Windows Shortcut Files) files present in the folder and it enumerates those files to connect them with their original location.All of the .lnk files are not processed, some of them are broken, they are shown in their original filename format.

7.4 File System/Process Logger

The Windows Forensics Analyzer also includes a tool which is used to log the changes in the file system and it also logs the process start and stop events. This tool stores log in a format which is parsed with the Windows Forensics Analyzer.

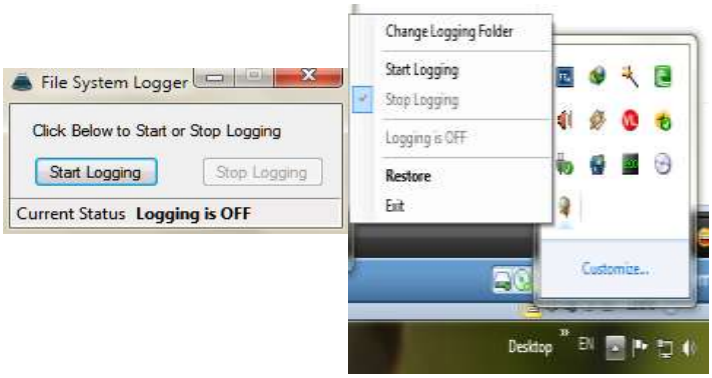

Fig. 7.File System/Process Logger

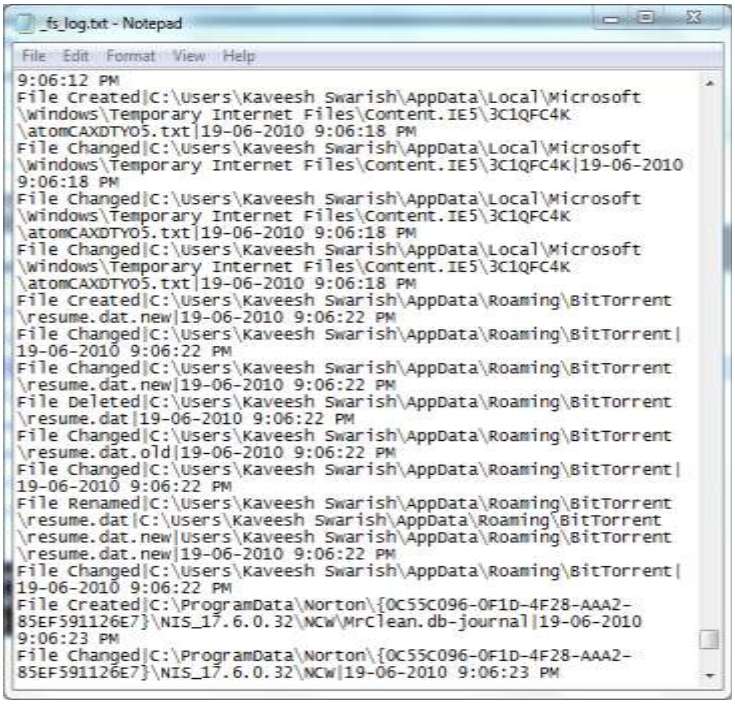

Fig. 7.File System/Process Logger Logs

As shown in Fig. 6. The Tool Provides the Utility of starting and stopping the Log and it also provides the utility to change the present logging folder. The Log generated by the File System/Process Logger is shown in Fig. 7.

8. FEATURES OF THE DEVELOPED WINDOWS FORENSICS ANALYZER (WFA)

The Developed Windows Forensics Analyzer provides a framework to collect and view all of the evidences on a single application. The WFA extracts all of the possible evidences in windows from the registry and the Event Logs. The WFA utilizes the WMI (Windows Management Instrumentation) Interface of the windows environment to collect the evidence, which makes the tool acceptably fast. The WFA can collect from all types of event logs present in the computer, it collects information regarding recently executed applications, it collects information about the start-up objects from the, it collects information about the Last Viewed Registry Key, it collects information about the typed in web addresses in Internet Explorer, it collects information about the folder in which the last downloaded file was saved, it collects information about the currently running processes, and it collects information about the recently accessed files from the recent folder. A prototype model for file system/process logger has also been implemented; it logs all the information about Process Start/Stop Events and File Creation/Deletion/Modification/Rename events, The Log created by the File System/Process Logger can be parsed by the Windows Forensics Analyzer.

9. CONCLUSIONS

Effective collection and analysis of digital evidence is a tedious task. In recent years the investigator had to use many forensics tools to perform investigation task. Integration of all types of forensics tools is a major challenge. The Developed and Implemented tool Windows Forensics Analyzer provides all the facilities to collect evidence from windows various sources viz. reading event log, reading specific registry locations, collection of volatile data i.e. running processes, recently used files/processes etc., in a single zone and meets this challenge to an extent. In future work, to make effective investigation the knowledge discovery techniques may be applied to analyze captured evidence in windows environment.

10. ACKNOWLEDGMENT

The research presented in this paper would not have been possible without our college, MANIT, Bhopal. We wish to express our gratitude to all the people who helped turn the World-Wide Web into the useful and popular distributed hypertext and providing information as it is anywhere. We also wish to thank the anonymous reviewers for their valuable suggestions, who helped in improving our paper content.

11. REFERENCES

[1] Huebner, E., and Henskens, F., "*The role of operating systems in computer forensics"*, SIGOPS Oper. Syst.Rev., 42(3), 1-3., 2008.

[2] "Forensic investigation on Windows Logs," [Online]. Available: http://www.icranium.com/blog/?p=194 [Accessed: Jun.02, 2010].

[3] "Wikipedia," [Online]. Available: http://en.wikipedia.org/wiki [Accessed: July.5, 2010].

[4] "Computer Forensics," US CERT Available www.us-cert.gov/reading_room/forensics.pdf [Accessed: June.10, 2010].

[5] "Forensically interesting spots in the Windows 7, Vista and XP file system and registry," [Online]. Available: http://www.irongeek.com/i.php?page=security/windows-forensics-registry-and-file-system-spots [Accessed: July 5,2010]

[6] AccessData, http://www.accessdata.com/

[7] Guidance Software, http://www.guidancesoftware.com/

[8] Sysinternals,http://technet.microsoft.com/en-us/sysinternals/default.aspx

[9] Dashora, Kaveesh, Tomar, Deepak Singh and Rana, J.L. *"A Framework for Windows Forensics"*. 2010. The Proceedings of National Conference on Recent Trends & Challenges in Internet Technology (RTCIT – 2010). pp. 167 - 171.

KaveeshDashoraM.Tech. (Final Year) in Computer Science &Engg., B.E. in Computer Science and Engg., research scholar of Maulana Azad National Institute of Technology(MANIT), Bhopal.

Mr. Deepak Singh TomarM.Tech& B.E. in Computer Science &Engg, working as Assistant Professor Computer Science &Engg. Department (MANIT, Bhopal). Total 14 Years Teaching Experience (PG & UG). Guided 16 M.Tech. Thesis.

Dr. J.L. Rana Professor & retired, Ex. Head of Department of in Computer Science &Engg, MANIT, Bhopal. PhD. IIT Mumbai M.S. USA (Hawaii). Guided 30 M.Tech. Thesis & Six Ph.D.