Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 6, June 2015, pg.625 – 631

RESEARCH ARTICLE

Investigating the Artifacts Using Windows Registry and Log Files

Milind G. Meshram[1], Prof. Deepak Kapgate[2]
[1]Department of Computer Science and Engineering
[1]G. H. Raisoni Academy of Engineering and Technology, Nagpur, India
[2]Department of Computer Science and Engineering
[2]G. H. Raisoni Academy of Engineering and Technology, Nagpur, India

Abstract:

Cyber attack comes in various approach and forms, either internally or externally. Access from remote machines and spyware are forms of cyber attack leaving an organization to be susceptible to vulnerability. This paper investigates of illegal activities and potential evidence of cyber attack through studying the registry on the Windows 7 and Event Log Files. The aim is to trace the registry and event log artifacts left by the attacker. With the growing importance of computer security today and the seriousness of cyber crime, this paper provide a solution for investigating the artifacts left by user which correlate to the user activity.

Keywords: Windows Registry , Event Log Files., Artifacts **,** Cyber Attack, Forensic Investigation.

I. INTRODUCTION

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 really a difficult and complex task for the forensic investigator to analyse all of the locations in the storage media. When these two factors are combined, it may result in a delay in bringing a case to court. The basic 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 and Event Log Files. Consequently, the forensic analysis process and the recovery of digital evidence may take less time than would otherwise required time. In this paper, the Registry structure of Windows 7 and Event Log Files is discussed together with several elements of information within the Registry of Windows 7 and Event Log Files that may be valuable to a forensic investigator. Event logs play an important role in modern IT systems, since they are an excellent source of information for monitoring the system in real-time and for conducting retrospective event analysis . As in recent times, the company machines are subjected to virtual network and these machines are accessed by remote users using remote desktop connections, the number of cyber attacks have been increased.

The increasing use of online workforce has exponentially increased the cyber attack threat. According to 20 12 Data Breach Investigation Report the most attacks experienced is malware. In 20 1 1, Spy ware is a form of malware stood at 48% of top mal ware threat. Spyware refers to the computer technology that gathers information such as recorded strokes (passwords), a list of Web Sites visited by the user, applications or Operating Systems (OS) that are installed on the computer without the user knowledge or consent. Online workforce has cultivated the implementation of remote access technologies to economically support their computer configuration and network issues on the client location. The use of remote access has an influence on cyber attacks due to the operating system and spyware usage. Forensic investigation is about finding the sufficiently reliable evidence that has relation to cyber attacks that can be used in court.

The forensic analyst may look at Windows registry to find information about hardware and software used. The registry contains the configuration information for the hardware and software and may also contain information about recently used programs and files. Proof that a suspect had installed a program or application may be found in the registry.

Microsoft Windows event logs are central to conducting an investigation when determining whether or not a virus has been installed on a targeted system. However, there was very little substantial research about Windows event logs and how they are used in conducting an investigation. Event log files can explore forensic artifacts recovered during an investigation to determine whether virus activity may be involved

A final clarification concerns the broader context for our technique to investigate artifact in the windows registry and algorithm for investigating the artifact in the event log files. Our focus is on the digital *forensic* task of discovering artifacts left by attacker, rather than a real-time monitoring system that analyzes live network traffic data and triggers alerts.. In real-time monitoring systems, efficiency is of crucial importance; any decrease in efficiency results in the highly undesirable scenario. In contrast, we assume that windows registry data have saved in static log files that are available for us to examine. Our technique will scan the windows registry more than once to attained the accuracy in investigating the artefact. On the other hand our algorithm will analyse the event log files. Efficiency, though important, was not our top priority when we designed the algorithm, since one of the underlying assumptions was that the data is historical and static, not growing dynamically at real-time. Our concern was mainly in the accuracy of discovering artifacts left by attacker.

II. RELATED WORK

In this section we provide a review of various papers relating to digital forensic.

1. Windows Registry Analysis for Forensic Investigation

In [1], according to Raihana Md Saidi, Siti Arpah Ahmad, Noorhayati Mohamed Noor, Rozita Yunos, cyber attack comes in various approach and forms, either internally or externally. Remote access and spyware are forms of cyber attack leaving an organization to be susceptible to vulnerability. This paper investigates illegal activities and potential evidence of cyber attack through studying the registry on the Windows 7 Home Premium (32 bit) Operating System in using the application Virtual Network Computing (VNC) and keylogger application. The aim is to trace the registry artifacts left by the attacker which connected using Virtual Network Computing (VNC) protocol within Windows 7 Operating System (OS). The analysis of the registry focused on detecting unwanted applications or unauthorized access to the machine with regard to the user activity via the VNC connection for the potential evidence of illegal activities by investigating the Registration Entries file and image file using the Forensic Toolkit (FTK) Imager. The outcome of this study is the findings on the artifacts which correlate to the user activity.

2. Forensic Analysis of Windows Registry Against Intrusion

In [2], As per, Haoyang Xie, Keyu Jiang, Xiaohong Yuan and Hongbiao Zen, windows Registry forensics is an important branch of computer and network forensics. Windows Registry is often considered as the heart of Windows Operating Systems because it contains all of the configuration setting of specific users, groups, hardware, software, and networks. Therefore, Windows Registry can be viewed as a gold mine of forensic evidences which could be used in courts. This paper introduces the basics of Windows Registry, describes its structure and its keys and subkeys that have forensic values. This paper also discusses how the Windows Registry forensic keys can be applied in intrusion detection.

3. Forensic Analysis of the Windows Registry

In [3], Lih WernWong, Windows registry contains lots of information that are of potential evidential value or helpful in aiding forensic examiners on other aspects of forensic analysis. This paper discusses the basics of

Windows XP registry and its structure, data hiding techniques in registry, and analysis on potential Windows XP registry entries that are of forensic values.

4. A Breadth-First Algorithm for Mining Frequent Patterns from Event Logs

In [4], Risto Vaarandi, Today, event logs contain vast amounts of data that can easily overwhelm a human. Therefore, the mining of frequent patterns from event logs is an important system and network management task. This paper discusses the properties of event log data, analyses the suitability of popular mining algorithms for processing event log data, and proposes an efficient algorithm for mining frequent patterns from event logs.

5. A Novel Technique For Mining Closed Frequent Itemsets Using Variable Sliding Window

In [5], Vikas Kumar , Frequent itemset mining over dynamic data is an important problem in the context of knowledge discovery and data mining. Various data stream models are being used for mining frequent itemsets. In a data stream model the data arrive at high speed such that the algorithms used for mining data streams must process them in strict constraint of time and space. Due to emphasis over recent data and its bounded memory requirement, sliding window model is a widely used model for mining frequent itemset over data stream.

In this paper we proposed an algorithm named *Variable- Moment* for mining both frequent and closed frequent itemset over data stream. The algorithm is appropriate for noticing latest or new changes in the set of frequent itemset by making its window size variable, which is determined dynamically based on the extent of concept drift occurring within the arriving data stream. The size of window expands when there is no concept drift in the arriving data stream and size shrinks when there is a concept change. The relative support instead of absolute support is being used for making the concept of variable window effective. The algorithm uses an in-memory data structure to store frequent itemsets. Data structure gets updated whenever a batch of transaction is added or deleted from the sliding window to output exact frequent itemsets. Extensive experiments on both real and synthetic data show that our algorithm excellently spots the concept changes and adapts itself to the new concept along data stream by adjusting window size.

6. System Monitoring and Security Using Keylogger

In [6], Preeti Tuli, It is likely that about one out of many large companies systematically monitors the computer, internet, or email use of its users employees. There are over hundred's different products available today that will let organizations see what their users do at work on their "personal" computers, in their email, and on the internet. But what do such numbers really mean? What does company monitoring of user/employee email, internet, and computer usage actually look like? What sorts of things can an organization/company see users do at their computers, and what sorts of computer activities are currently invisible to workplace monitoring? This admittedly document attempts to propose, as concretely as possible what "Informational Flow" on internet and computer usage looks like: its extent, the key concepts involved, and the forces driving its adoption. The keylogging program logs all keystrokes (aka Keystroke Logging) along with the name of the application in which the keystrokes were entered. Using keylogger we prevent the miscellaneous use of system. Using this we capture all information in text and image form.

7. Windows Registry Forensics: An Imperative Step in Tracking Data Theft via USB Devices

In [7], Tanushree Roy, Aruna Jain, Owing to the increasing pace of occurrence of crimes in digital world, cyber forensic investigation is becoming a burning topic in the field of information security. Registry is an important location in Windows system that contains footprints of user activities and other configuration data, which may be valuable for forensic investigators in collecting potential evidences from the system. This work aims to point out the significance of Registry Analysis, and attempts to answer why it should be carried as a part of digital forensic investigation by demonstrating the role played by Registry in tracking data theft from system to USB external devices.

8. Remote Access Forensics for VNC and RDP on Windows Platform

In [8], Paresh Kerai, There has been a greater implementation of remote access technologies in recent years. Many organisations are adapting remote technologies such as Virtual Network Computing (VNC) and remote desktop (RDP) applications as customer support application. They use these applications to remotely configure computers and solve computer and network issues of the client on spot. Therefore, the system administrator or the desktop technician does not have to sit on the client computer physically to solve a computer issue. This increase in adaptation of remote applications is of interest to forensic investigators; this is because illegal activities can be performed over the connection. The research will investigate whether remote protocols and applications do produce and leave valuable artefacts behind on Windows systems. The research aims to determine and retrieve any artefacts left behind remote protocols and applications in a forensic manner. Particular remote applications are selected to perform the research on and initial analysis will be performed on the applications to evaluate the potential forensic artefacts present on the computer system. The research will focus on Windows XP for analysis of the remote applications and find out what artefacts if any are left behind these systems

III. EVALUATION AND DISCUSSION

The following table gives a comparative description of some of the techniques that we have discussed above.

Sr.no	Paper Title	Technology used / Approach	Comment
1	Registry Analysis for Forensic Investigation[1]	Use of VNC and Key logger	Implementation is less efficient as algorithm executes iteratively.
2	Forensic analysis Against Intrusion[2]	Checks sub key of every five key	Increased implementation complexity
3	Forensic Analysis of the Windows Registry[3]	data hiding techniques in registry, and analysis on potential Windows XP registry entries that are of forensic values	Provides investigation only for windows XP.
4	BFA[4]	Uses Event Log file and mining algorithm for investigation	Efficient but Less effective if less itemsets are available.

Table-I. Comparison between various techniques.

IV. PROPOSED METHOD

Overall methodology for this study can be viewed as in Fig. 1.

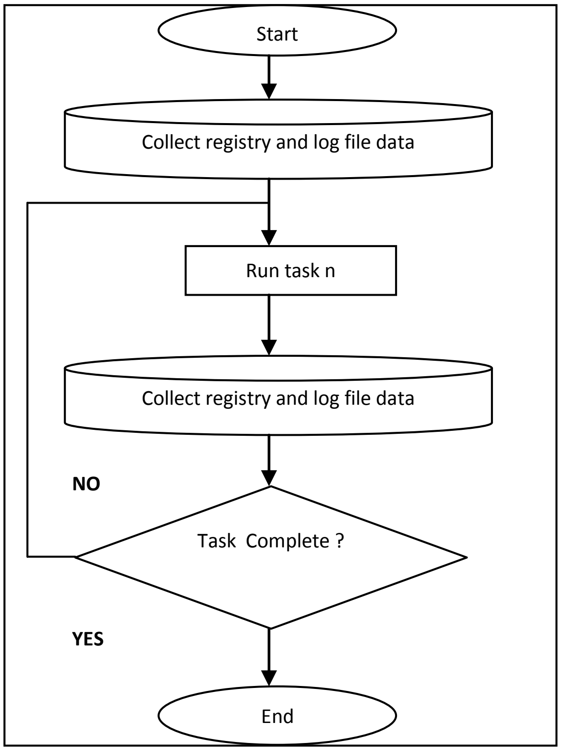
Start
Collect registry and log file data
Run task n
Collect registry and log file data
NO
Task Complete ?
YES
End

Fig. 1. Overall Research Methodology

The study begins with data collection from Event Log files and Windows Registry files. Then the data is stored prior to the experimental scenario for reference. The data once again is collected and stored after the experimental scenario and then finally the analysis is done.

A. Data Collection

The primary data collected in this study was the registry hive files which include the ntuser.dat and UsrClass.dat from the Users directory and Default, System, Software, Security and SAM from the Windows\System32\Config directory. The other data which is collected is from the Event Log files.

Table I lists the Registry files and their location for Windows 7 OS for the evaluation of possible artifacts.

Sr. No.	Registry File	File Path
1	Default	C:\ Windows\System32\Config\DEFAUL T
2	System	C:\ Windows\System32\Config\S YSTEM
3	Software	C:\ Windows\System32\Config\SOFTW ARE
4	Security	C:\ W indows\S ystem32\Con fig\SECURITY
5	Sam	C:\ Windows\System32\Config\SAM

Table II. Registry files location

B. Experimental Scenario

The experimentation in this study is being carried out by performing a scenario-based test. The implementation is done in Java and a client and server (Windows 7 Operating system (64 bit)) was configured. Some test scenarios were created as shown in Table III.

Sr. No.	Activity	Expected Outcome
1	Physically access the computer and create/delete a new/existing user	User account registry key Created on the SAM registry file
2	Connect the USB device to the computer	Registry key value is created in SYSTEM registry file
3	Access the restricted files, folders or database	Values stored in USER registry file and MRUList

Table III. Test Scenario.

C. Data Analysis

The registry and Event Log files were then analyzed. Changes of the registration entries (.reg) and Event Log files before and after experiment were identified and reviewed. Besides changes, any potential artifacts that can be extracted from the registry and Event Log files were also being analyzed.

V. ALGOROTHM FOR PROPOSED METHOD

```
Input: System registry / log files, Rules defining illegal activities.
Output: List of malicious users with their illegal activities.
Step 1: START
Step 2: For every user in the system
          do
                Read user log file
Step 3: if (log files contain illegal activities as specified by rules)
              Highlight that row and categories that user as malicious.
           else
              User is clean and no illegal activities found.
Step 4: Generate output with list of malicious users and clean users.
Step 5: END
```

VI. EXPERIMENTATION AND RESULT

In this section, we will discuss the experimentation and result analysis of the proposed algorithm. The values from registry files and event log files before and after test were compared to identify the changes. Apart from the changes any value from registry and event log file that is relevant and has potential to be used as evidence is being extracted. The artifacts extracted were only for relevant footprints with regards to the user and system activities.

Test 1: Start the system as Administrator, and then create the number of users you want.
Findings: User account registry key created on the SAM registry file every time the Administrator creates user.

Test 2: Log in as a user and connect the USB device to the computer and perform activities like copying data form USB device to system and vice versa.
Findings: Registry key value is created in SYSTEM registry file.

Test 3: Log in as an administrator and restrict some files as confidential files. Accessing restricted files will be an illegal action and user will be a malicious user. Now log in as one of the user and access the restricted file.

Findings: The users who accessed the confidential and restricted files are found to be malicious users with the help of values stored in USER registry file and MRUList. The Event log files can also be good resource for finding such users.

VII. CONCLUSION

The methods and algorithms that we have discussed above cover different problem areas in digital forensic investigation. Windows registry and event log files are an excellent source for potential evidential data. Knowing the type of information that could possible exist in registry and location to it gives forensic examiner the edge in the forensic analysis process. Investigator will get a better picture of the whole case.

REFERENCES

[1] Raihana Md Saidi, Siti Arpah Ahmad, Noorhayati Mohamed Noor, Rozita Yunos, “Windows Registry Analysis for Forensic Investigation”, ISBN: 978-1-4673-5613-8©2013 IEEE.

[2] H. Xie, K. Jiang, X. Yuan, H. Zeng, "Forensic Analysis of Windows Registry Against Intrusion," international Journal of Network Security & its Applications (IJNSA), Vol.4, No.2, March 2012, pp: 121-134.

[3] Lih WernWong, “ Forensic Analysis of the Windows Registry”.

[4] Risto Vaarandi, “A Breadth-First Algorithm for Mining Frequent Patterns from Event Logs”.

[5] Vikas kumar , "A Novel Technique For Mining Closed Frequent Itemsets Using Variable Sliding Window "978-1-4799-2572-8/14/$31.00c 2014 IEEE.

[6] P. Tuli, P. Sahu, "System Monitoring and Security Using Keylogger," international Journal of Computer Science and Mobile Computing, Vol.2, Issue 3, 2013, pp: 106-111.

[7] T.Roy and A.Jain, "Windows Registry Forensics: An Imperative Step in Tracking Data Theft via USB Devices", international Journal of Computer Science and information Technologies ", VoL3, issue 3, 2012, pp: 4427-4433.

[8] P. Kerai, "Remote Access Forensics for VNC and RDP on Windows Platform," Australian Digital Forensics Conference, Perth, Nov. 2010, pp. I06-116.

[9] Sonia Bui, Michelle Enyeart, Jenghuei Luong , “Issues in Computer Forensics ”.

[10] Verizon RISK Team, "2012 Data Breach Investigations Report", Verizon, DBJR.

[11] H. S. Lallie, P. J. Briggs, "Windows 7 Registry Forensic Evidence Created by Three Popular BitTorent Clients," Digital Investigation 7, 2011, pp:I27-134.

[12] A.Sivaprasad and S. Jangale, "A Complate Study on Tools and techniques for Digital Forensic Analysis", 2012 international Conference on Computing, Electronics and Electrical Technologies (iECCEET), 2012, pp: 881 - 886.

[13] S. Anson, S. Bunting, R. Johnson, S. Pearson, Mastering Windows Network Forensics and investigation. Canada: Wiley, 2012.

[14] Aggarwal, C, “A framework for diagnosing changes in evolving data streams,” In Proc. ACM SIGMOD int. conf. on management of data (pp. 575–586), 2003.

[15] Agrawal, R., & Srikant, R, “Fast algorithms for mining association rules,” In Proc. VLDB int. conf. very large databases (pp. 487– 499), 1994.

[16] Chang, J., & Lee, W. S, “Finding recently frequent itemsets adaptively over online transactional data streams,” Information Systems, 31(8), pp. 849–869, 2006.

[17] Han, J., Cheng, H., Xin, D., & Yan, X. Frequent pattern mining: Current status and future directions. Data Mining and Knowledge Discovery, 15(1), pp. 55–86, 2007.

[18] Y. Chi, H. Wang, P. S. Yu and R. R. Muntz. Catch the moment: maintaining closed frequent itemsets over a data stream sliding window. In KAIS, 10(3): pp. 265-294, 2006.

[19] C. Giannella, J. Han, J. Pei, X. Yan, and P. S. Yu. Mining frequent patterns in data streams at multiple time granularities. In Kargupta et al.: Data Mining: Next Generation Challenges and Future Directions, MIT/AAAI Press, 2004.

[20] Manku, G. S., & Motwani, R. Approximate frequency counts over data streams. In Proc. VLDB int. conf. very large databases (pp. 346–357), 2002.

[21] Zaki, M. (2000). Scalable algorithms for association mining. IEEE Transactions on Knowledge and Data Engineering, 12(3), 372– 390.

[22] Woo H. J., & Lee, W. S. (2009). estMax: Tracing maximal frequent item sets instantly over online transactional data streams. IEEE Transactions on Knowledge and Data Engineering, 21(10), 1418–1431.

[23] Koh, J.- L., & Lin, C.- Y, “Concept shift detection for frequent itemsets from sliding window over data streams”, lecture notes in computer science: Database systems for advanced applications (pp.334–348). DASFAA Int. Workshops, Springer-Verlag.2009.

[24] H. Li, S. Lee, and M. Shan, “An Efficient Algorithm for Mining Frequent Itemsets over the Entire History of Data Streams”, In Proc. of First International Workshop on Knowledge Discovery in Data Streams, 2004.

[25] F. Nori, M. Deypir, M. Sadreddini, “A sliding window based algorithm for frequent closed itemset mining over data streams”, journal of system and software, 2012.