UTM UNIVERSITI TEKNOLOGI MALAYSIA
INTERNATIONAL JOURNAL OF INNOVATIVE COMPUTING
ISSN 2180-4370
Journal Homepage : https://ijic.utm.my/

Case Based Interpretation of Windows10 Registry Forensics

Hasan Binjuraid, Mazura Mat Din and Hazinah Kutty Mammi
Faculty of Computing,
Universiti Teknologi Malaysia,
81310 UTM Johor Bahru, Johor, Malaysia
Email: hasanbinjuraid@gmail.com, mazura@utm.my, hazinah@utm.my

Submitted: 12/01/2018. Revised edition: 26/03/2018. Accepted: 8/05/2018. Published online: 21/05/2018

***Abstract*—With the advancement in computer technologies, cybercrimes advanced too. As in today's world, the technology knowledge to attack a computer is less than ever, with the help of advanced tools that does most of the work. Digital forensic investigations are crucial in solving this type of crimes, and it must be done professionally. Computer registries play a big part in the digital forensic investigation, it can help find artifacts that are left by the cybercrimes, dates of the crimes on the computer system and the user at the time of the crime. In this research, interpretation of these artifacts is the main focus, committees and jurors are the focus of the interpretations of the registries. Two types of cases are subject to investigation in this research. BitTorrent clients' use for downloading illegal o copyrighted content, and three clients are chosen for this digital forensic investigation uTorrent, Vuze and BitComet. Theft using USB storage devices is the second type of case, where there are three types of USB devices Mass Storage Class, Picture Transfer Protocol and Media Transfer Protocol, each type of USB devices leaves different artifacts behind during insertion and removal. A web based dashboard will be developed to help with the process of interpretation the artifacts found in the registry of the computer system. A categorization process of each cybercrime case will be conduct to evaluate the severity of the case depending on the artifacts found in the digital forensics investigation process. The research methodology will consist of three phases. The first phase will be information gathering including literature review, requirements gathering and dataset gathering for the research. Performing digital forensics analysis will be the second phase and it includes planning, identification and reconnaissance. Last phase will include result analysis and discussion.**

Keywords — Case based interpretation, Windows 10, registry, forensic

I. INTRODUCTION

With the development of computers and technology, they have necessary roles in our lives. Almost every communication we are having nowadays is made through a computer, whether it is in the form of PC or phones. With that much reliance on technology, there comes greater responsibilities, and these responsibilities are sometimes betrayed by crimes made using these computers and technologies. But every crime leaves a trace, and these particular type of crimes can be traced using digital forensics on registries. And in this project, the focus will be on Windows registry forensic analysis [1].

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 analyze 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 [2].

The main concept of this paper is to showcase different criminal cases that has been done using computers and identify the evidences and traces that are left on the Windows registry by these crimes. The concept also includes developing a dashboard that describes the evidences that lead to the belief of crimes being done on these different cases. There will be two different criminal cases that were done using computers. First is an illegal file sharing case using different BitTorrent clients. Secondly, an illegal access of information using a USB storage device.

II. PROBLEM BACKGROUND

Digital forensics on registries is an important part of investigation in a lot of departments of the everyday community. It can be used in an internal investigation of an organization regarding a specific incident in that organization, or it can be used by the law enforcement departments in regard of a certain criminal act which includes the use of computers or phones [3]. The evidence found in these type of investigation, can be then presented to a committee in a case of an organization investigation, or to a jury or a judge in a case of law enforcement investigation. In presenting evidences in these type of cases, an expert is required to interpret the findings, which costs more than if the interpretation was done by a computer. There are several types of cybercrimes, but in this project two types will be covered. BitTorrent illegal use to download copyrighted content is one of them. Also, USB flash drive illegal access cases will be covered. The free, open source BitTorrent protocol, created by Brahm Cohen in 2002, is the most popular means of sharing files across the Internet. It is designed to have lower bandwidth bottlenecks that often occur when many users download the same large file across the network and since it is utilized by nearly all modern file sharing applications, it is often at the center of illegal file sharing controversies [4].

USB flash drives are a popular and fast way to store and transfer data from a computer to another. This makes it an appealing way to use in personally identifiable information (PII) and intellectual property theft, as it is easy to plug in and plug out. With the increase of cyber-crimes, one of the increasing type of crimes is information theft using USB flash drives. Thus, it is very important for incident responders to understand variation of USB storage devices and the traces it leaves behind after plugging in and out in Windows operating system (NIST 800-122). Cybercrimes are the crimes that are done using a phone or a computer. Abhijeet Ramani [5] provided various details and artifacts to help on tracing the illegal access of files from a system using an external USB flash drive and Swasti Bhushan Deb [3] highlights the timestamps and artifacts left by insertion and removal of USB devices in the Windows 8 registry, and to the best of our knowledge, there are no existing papers about artifacts left by the insertion and removal of USB devices in Windows 10 registry.

III. Problem Statement

Technology advances on a daily basis, and platforms of computers change also. The rapid change in computers platforms require researches and investigators to be knowledgeable of the changes in the platforms to make the process of digital forensic analysis and investigation more efficient[6]. The change in Windows 10 registry is targeted by performing case based analysis and interpretation of the registry using two cybercrime cases.

IV. Objectives

- To perform digital forensic investigation on two types of cases and identify the evidences found in the process.
- To analyze the artifacts and results of the digital forensic investigation on the chosen cases.
- To develop a dashboard that describes the evidences of cybercrimes in Windows registries.

V. Research Framework

The research framework to conduct the proposed research is depicted in Figure 1. All the steps will be discussed in this chapter. In this research, it consists of three phases. The first phase is the information gathering which includes the literature review and related works. The second phase is the full and thorough investigation, evidence gathering and analysis for each cybercrime case. The last phase is the dashboard development.

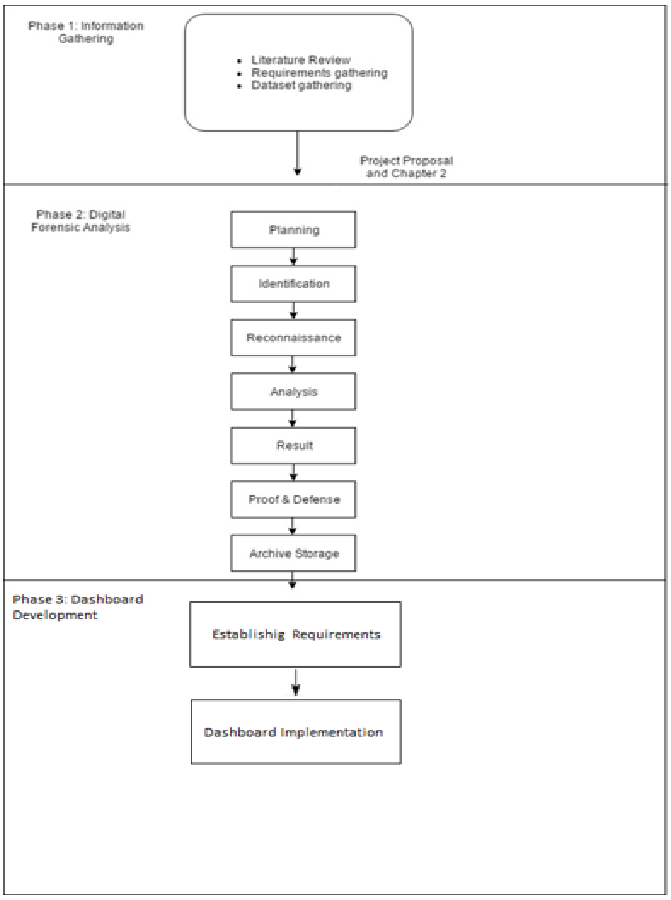


Fig. 1. The three phases of the research

A. Information Gathering

Information gathering is the main concept of this phase. First glimpse of the information gathering came in the literature review, when the analysis of the two cybercrime cases was discussed and reviewed. A detailed study of the different cases was conducted and presented to give the reader an idea about the tools used to conduct the digital forensics investigation and the tools to be investigated also.

During phase 1, the dataset for each cybercrime case are identified and documented. For the BitTorrent clients cases, the required resources to carry out the digital forensics analysis are listed out in previous parts of the research [10]. Also in previous parts the literature review of the BitTorrent protocol was presented with the three chosen BitTorrent clients.

The USB transfer protocols were presented in the second chapter of this research alongside with the definition of each protocol. The datasets for the theft using USB flash drives cases were identified and it will be presented in chapter 4 of this research.

B. Digital Forensic Analysis

In this phase, the process of the digital forensics investigation is done to the three types of cybercrimes that were chosen. The digital forensics investigation process will follow the digital forensics model based on Malaysian investigation process that was developed by Sundresan Perumal [2]. The model consists of seven stages including planning, identification, reconnaissance, analysis, result, proof and defense and diffusion of information.

The first stage, planning, includes both acquiring authorization and getting a search warrant. It is important to obtain both the authorization from the local law enforcement department and the search warrant to collect any possible evidences before proceeding with the digital forensic investigation. The second stage is the identification stage, which has two procedures that is identifying seized items and identifying fragile evidence. Identifying fragile evidence is concerned with the decision of pulling the plug or not on computer systems during the evidence collecting process. The traditional way that investigators go by is to shut down the computer systems, but live analysis of the system can provide insightful information on the memory details and registry keys.

The third stage is reconnaissance, which is concerned with the scope of the exploration of the investigation to gain evidence. Organizations nowadays tend to have huge computer systems with servers in multiple locations. A digital forensic investigator cannot go to every server and shut it down in order to analyze it, this is why only the necessary evidence is identified before conducting the evidence gathering. AccessData FTK Imager will help us in the process of collecting evidence using its ability of creating images of the registry at a certain time [9]. Transport and storage is the fourth stage, this stage is more concerned with the process of locating the evidence in secure locations so that it would not be facing any kind of change or tampering. Fifth stage is the analysis stage, in this stage the digital forensic investigator uses the needed tools to analyze the gathered evidence to make sense of the crime that is being investigated. The tools that will be used in this stage include Regshot, which compares the registry of the system in two different stages. AccessData FTK Viewer tool will help us to view the registry encrypted data, including usernames and passwords that are used in the system. Proof and defense is the sixth stage, which is concerned with how to validate the findings of the case with a proper scenario that would stand firm against the defense’s contrary hypothesis. Lastly, the archive storage stage, which includes storing all findings and evidences in case it is needed as a reference in the future or for training purposes. Figure 2 shows the flowchart of the digital forensics model.

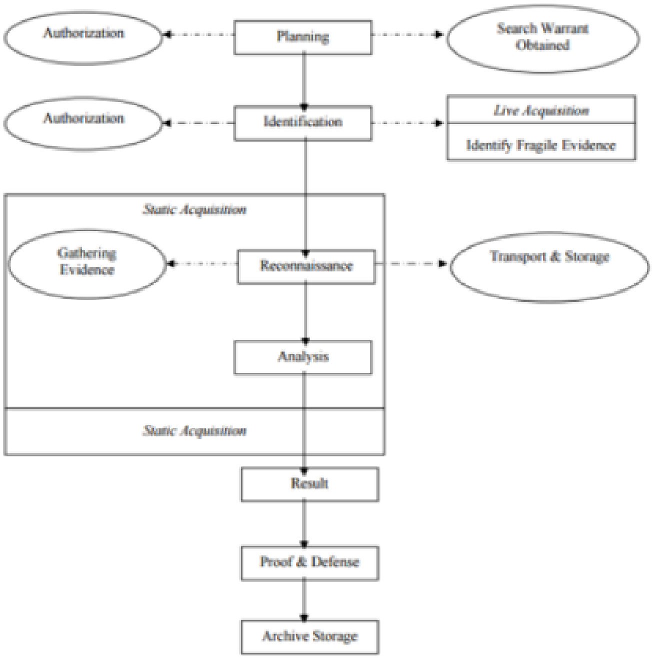


Fig. 2. The Flow of the investigation model

C. Dashboard Analysis

In this phase, the dashboard is developed using the waterfall web development model. The waterfall model includes five different phases that starts with the requirements gathering and analysis [11]. Then, it is followed by the design phase in which the software architecture is developed [12]. The implementation phase comes next, with the coding of the actual website, after that is the testing of the code developed. After that, the installation process is done to officially launch the website. Lastly, the maintenance phase is done when new features or debugging is needed.

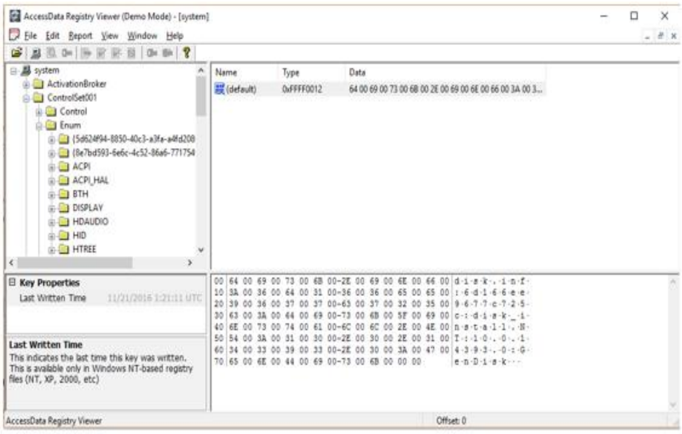
VI. BitTorrent Clients Dataset

The dataset of these cases will be created following the steps of Harjinder Singh Lallie and Philip James Briggs in their published paper about the evidences created by BitTorrent clients in Windows 7 [8]. The dataset for the three BitTorrent clients uTorrent, Vuze and BitComet is created by taking snapshots of the system registry using AccessData FTK Imager in five different stages of installing, running, downloading and uninstalling of the BitTorrent client. Figure 3 shows the snapshot from the registry using AccessData Registry Viewer. The five stages are:

- Before installing the BitTorrent client application.
- After installing the BitTorrent client application and before running it.
- After the first time running of the BitTorrent client application.

- After using the BitTorrent client application for the different downloading tasks for each user of the system. Tasks includes files queued for downloading, files incompletely downloaded, files fully downloaded and files that are deleted.

- After uninstalling the ButTorrent client application.


AccessData Registry Viewer (Demo Mode) - [system]
File Edit Report View Window Help
system
ActivationBroker
ControlSet001
Control
Enum
{5d624f94-8850-40c3-a3fa-a4fd208
{8e7bd593-6e6c-4c52-86a6-771754
ACPI
ACPI_HAL
BTH
DISPLAY
HDAUDIO
HID
HTREE
Name
Type
Data
AccessData Registry Viewer
Offset: 0

(default) 0xFFFF0012 64 00 69 00 73 00 6B 00 2E 00 69 00 6E 00 66 00 3A 00 3...

Key Properties

Last Written Time 11/21/2016 1:21:11 UTC

Last Written Time

This indicates the last time this key was written. This is available only in Windows NT-based registry files (NT, XP, 2000, etc)

```
00 64 00 69 00 73 00 6B 00-2E 00 69 00 6E 00 66 00 d·i·s·k·.·i·n·f·
10 3A 00 36 00 64 00 31 00-36 00 36 00 65 00 65 00 :·6·d·1·6·6·e·e·
20 39 00 36 00 37 00 37 00-63 00 37 00 32 00 35 00 9·6·7·7·c·7·2·5·
30 63 00 3A 00 64 00 69 00-73 00 6B 00 5F 00 69 00 c·:·d·i·s·k·_·i·
40 6E 00 73 00 74 00 61 00-6C 00 6C 00 2E 00 4E 00 n·s·t·a·l·l·.·N·
50 54 00 3A 00 31 00 30 00-2E 00 30 00 2E 00 31 00 T·:·1·0·.·0·.·1·
60 34 00 33 00 39 00 33 00-2E 00 30 00 3A 00 47 00 4·3·9·3·.·0·:·G·
70 65 00 6E 00 44 00 69 00-73 00 6B 00 00 00       e·n·D·i·s·k···
```

Fig. 3. A snapshot of the registry

VII. MSC Enabled USB Devices

It is to be noted that when a USB device is first inserted into windows 10 machine, the Plug and Play (PnP) manager receives the event and queries the device description residing in the firmware, such as manufacturer, serial no, etc. residing in the USB device. The vendor ID (idVendor) and the Product ID(idProduct) are used by Windows to construct a hardware ID for the device. This information's are then used by the PnP Manager to locate the appropriate driver for the device and this event is recorded in C:\ Windows\inf\setupapi.dev.log. file which contains information about Plug and Play devices and driver installation), and events with specific event ID's.

VIII. The DeviceClasses Keys

When a plug and play device driver is successfully loaded, the DeviceClasses sub keys are created. The DeviceClasses sub keys can be used to determine the first insertion times. Depending on the type of device being recognized, the DeviceClasses sub key found in the System registry under SYSTEM\ControISet\Control contains sub keys, each of which correlates to the type of device that is being recognized and the first insertion timestamps. It was observed that the MSC enabled test subjects were recognized under the following device classes:

- 10497blb-ba51-44e5-S31S-a65cS37b6661
- 53f56307-b6bf-I I dO-94t2-00aOc91 efb8b
- 53f5630d-b6bf-I I dO-94t2-00aOc91 efb8b
- 6ac27878-a6fa-4155-baS5-f9Sf491d4f33

Last write times of each of the keys mentioned below located under ControISet\Control\DeviceClasses of the SYSTEM hive correlates to the first insertion times of MSC enabled test subjects:

- SYSTEM\ControISetOOI\Control\DeviceClasses\{10497blb-ba51-44e5-S31Sa65cS37b6661}\##?#SWD#WPDBUSENUM#_??_USBSTOR#Disk&Ven_hp&Prod_ppppw&Rev_rrrr# 0340914 I 00006AS6&0#{53f56307-b6bf-I I dO-94t2-00aOc91efbSb}#{I 0497b 1 b-ba51-44e5-S31Sa65cS37b6661}
- SYSTEM\ControISetOO1\Control\DeviceClasses\{53f56307-b6bf-1IdO-94t2-00aOc91efbSb}\##?#USBSTOR#Disk&Ven_hp&Prod_pppw&RevJrrr#0340914100006AS6&0#{53f56307-b6bf-lldO-9412-00aOc91efbSb }
- SYSTEM\ControISetOO1\Control\DeviceClasses\{53f5630d-b6bf-lldO-9412-00aOc91efbSb}\##?#STORAGE#Volume#_??_USBSTOR#Disk&Yen_hp&Prod_ppppw&Rev_rrrr#0340914100006AS6&0#{53f56307-b6bf-lldO-9412-00aOc91efbSb}#{53f5630d-b6bf-ll dO-9412-00aOc91efbSb}
- SYSTEM\ControISetOO1\Control\DeviceClasses\{6ac2787S-a6fa-4155-baS5-f9Sf491d4f33}\##?#SWD#WPDBUSENUM#_??_USBSTOR#Disk&Ven_hp&Prod_pppw&RevJrrr#O340914100006AS6&0#{53f56307-b6bf-lldO-94t2-00aOc91efbSb}#{6ac27S7S-a6fa-4155-baS5-f9Sf491d4f33}

Where ‘vvvv’ is a 4-digit hexadecimal number that identifies the vendor, ‘pppp’ is a 4-digit hexadecimal number that identifies the product, ‘rrrr’ is a 4-digit hexadecimal number that contains the revision number of the device.

IX. MTP and PTP Enabled USB Devices

It is to be noted that when a USB device is first inserted into windows 10 machine, the Plug and Play (PnP) manager receives the event and queries the device description residing in the firmware, such as manufacturer, serial no, etc. residing in the USB device. The vendor ID (idVendor) and the Product ID(idProduct) are used by Windows to construct a hardware ID for the device. This information's are then used by the PnP Manager to locate the appropriate driver for the device and this event is recorded in C:\ Windows\inf\setupapi.dev.log. file which contains information about Plug and Play devices and driver installation), and events with specific event ID's.

X. The DeviceClasses Keys

Last write time of each of the keys mentioned below located under ControISet\Control\DeviceClasses of the SYSTEM hive correlates to the first insertion time of MTP, PTP enabled test subjects.

- {10497blb-ba51-44e5-8318- a65c837b6661} \##?#USB#VID_vvvv&PID_pppp&M1_00#8&ada652a&0&0000#{I0497bIb-ba51- 44e5-83I 8-a65c837b6661}

- {6ac27878-a6fa-4155-ba85-f98f491d4f33}\##?#USB#VID_vvvv&PID_ppp&M1_00#8&ada652a&0&0000#{6ac27878-a6fa-4155- ba85-f98f491d4f33}

- {a5dcbflO-6530-11d2-90If-00c04fb951ed}\##?#USB#VID_vvvv&PID_ppp#4d 008bOd3db15085#{a5dcbfl0-6530-11d2-901_00c04tb95I ed}

- {6bdd1fc6-81Of-IIdO-bec7-08002be2092f}\##?#USB#VID_vvvv&PID_pppp&M1_00#8 &ada652a&0&0000#{6bddIfc6-81Of-IIdObec7-08002be2092f}

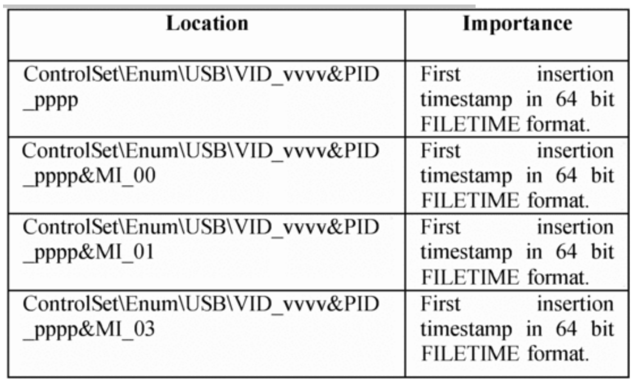
XI. The usbflags Key

After the operating system requests a Microsoft OS String Descriptor from a device, it creates the following registry key: SYSTEM\CurrentControISet\Control\UsbFlags\ vvvvpppprrrrr. The operating system creates a registry entry, named osvc, under this registry key that indicates whether the device supports Microsoft OS Descriptors. The key ControISet\Control\usbflags\04E868600400 under the SYSTEM hive correlates to the Vendor ID, product ID ,the revision number and the first insertion time of the MTP enabled USB device.

XII. The USB Key

No footprints of the insertion timestamps of the MTP enabled Samsung Galaxy tab were found under the USBSTOR key located under ControlSet\Enum of the SYSTEM hive. When the MTP, PTP enabled test subjects were inserted to the Windows 10 system, following registry keys as shown below in Table 1 were found to be forensically important.

TABLE I. Various keys and its importance



Location	Importance
ControlSet\Enum\USB\VID_vvvv&PID_pppp	First insertion timestamp in 64 bit FILETIME format.
ControlSet\Enum\USB\VID_vvvv&PID_pppp&MI_00	First insertion timestamp in 64 bit FILETIME format.
ControlSet\Enum\USB\VID_vvvv&PID_pppp&MI_01	First insertion timestamp in 64 bit FILETIME format.
ControlSet\Enum\USB\VID_vvvv&PID_pppp&MI_03	First insertion timestamp in 64 bit FILETIME format.

References

[1] Abhijeet Ramani, Somesh Kumar Dewangan. (2014). Auditing Windows 7 Registry Keys to Track the Traces Left Out in Copying Files from System to External USB Device.

[2] Bitcomet.com. (2010). BitComet Client Release Notes - A free C++ BitTorrent/HTTP/FTP Download Client

[3] Harjinder Singh Lallie and Philip James Briggs. (2011). Windows 7 Registry Forensic Evidence Created by Three Popular BitTorrent Clients.

[4] J. Sung, E. Baek, K. Byun, S. Lee, J. Lim. (2007). Digital Forensic Analysis of Peer-to-Peer Networking.

[5] J. Lewthwaite, V. Smith. (2008). Limewire Examinations.

[6] McDonough, J. and McDonough, S. (1997). *Research Methods for English Language Teachers*. London: Arnold.

[7] NIST. 2010. Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).

[8] Pyecha, J. (1988). A Case Study of the Application of Noncategorical Special Education in Two States Chapel Hill. NC: Research Triangle Institute.

[9] Swasti Bhushan Deb, Arjun Chetry. (2015). USB Device Forensics: Insertion and Removal Timestamps of USB Devices in Windows 8.

[10] Sourceforge.net. (2009-07-14). SourceForge Top Projects.

[11] TorrentFreak. (2009-12-04). Thunder Blasts µTorrent's Market Share Away.

[12] Zdnet.com. (2017-01-09). Today's Most Popular Operating Systems.

[13] Tanushree Roy, Aruna Jain. (2012). Windows Registry Forensics: An Imperative Step in Tracking Data Theft via USB Devices.

[14] TechRadar. Future. (June 3, 2015). Device Guard Safeguards Windows 10 with Hardware Authentication.

[15] V. Mee, T. Tryfonas, I. Sutherland. (2006). The Windows Registry as a Forensic Artefact: Illustrating Evidence Collection for Internet Usage.

[16] Windows.com. (June 1, 2015). Hello World: Windows 10 Available on July 29.

[17] Windows.com. (June 1, 2015). SetupAPI Logging.

[18] Yin, R., and Moore, G. (1987). The Use of Advanced Technologies in Special Education. *Journal of Learning Disabilities*, 20(1), 60.

[19] Zaidah Zainal. (2003). An Investigation into the Effects of Discipline-Specific Knowledge, Proficiency and Genre on Reading Comprehension and Strategies of Malaysia ESP Students. Unpublished Ph.D. Thesis. University of Reading.