ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645
Indian Journal of Science and Technology, *Vol 8(S7), 365–372, April 2015* DOI: 10.17485/ijst/2015/v8iS7/70420

Analysis of Time Records on Digital Forensics

Sungjin Lee* and Sunghyuck Hong

Division of Information and Communication, Baekseok University, Korea; lsj@bu.ac.kr, shong@bu.ac.kr

Abstract

Time analysis is important for digital forensic area, and Windows 7/8 are common to be used. However, there is not much research on time analysis for Windows 7 and 8. Time analysis is a critical proof for accusing criminal. There are various time zones, and time records on Windows operating system are not clear to understand which means RTC time or local time. Therefore, time analysis on Windows operating system must be firmed and documented for investigating forensic crime. We contribute to analysis time records whenever files are generated or modified by users, so we expect that our research will be able to make ambiguous time records clear for investigating digital forensics.

Keywords: Analysis of Time, Component, Digital Crime, Forensics, Time Recording

1. Introduction

Recently, the use of information devices are becoming active, accurate understanding and utilization of its kind, and performance, and capacity is being managed on a computer in a situation that has developed by leaps and bounds the time information is becoming very important in digital evidence analysis. Stored in binary data is that, as shown in Figure 1 and processed in the computer, which in hexadecimal representation, or in accordance with the intended time, CPU instructions, letters, numbers, or the like is used in a variety of forms. In particular, time information on the computer is to configure system hardware, operating system, application software, as well as due method according to interlock with the system configuration, the degree of the change differently systematic investigation and research on these has become urgent[1,14].In the control study focusing on how to interpret the information to be left on file at various times depending on the number of operations that occur while operating the way the window of how we can interpret the installation time due to various installation types for Windows is to make progress[4–7]. We recorded installation time for formal and informal Windows operating system, and procedures are following below.

**Author for correspondence*

1.1 Method for Formal Windows Operating System Install Time

We determined the installation time as normal installing Windows operating system and determined if there are any differences based on different version, or hardware specification such as Laptop or 32 bit/64 bit operating system. We used virtual machine such as VMW are or Virtual PC. We investigated the followings:

- Windows XP, Windows XP / SP1, Windows XP / SP2, Windows XP / SP3
- Windows 7 Home Premium, Professional, Ultimate Version
- Windows 8
- Whether the impact of the PC motherboard
- Whether the impact on the Notebook PC
- Whether influenced by the 32-bit and 64-bit operating system

1.2 Method for Informal Windows Operating System Installation Time (Windows Update, Restoring Ghost Image, etc.)

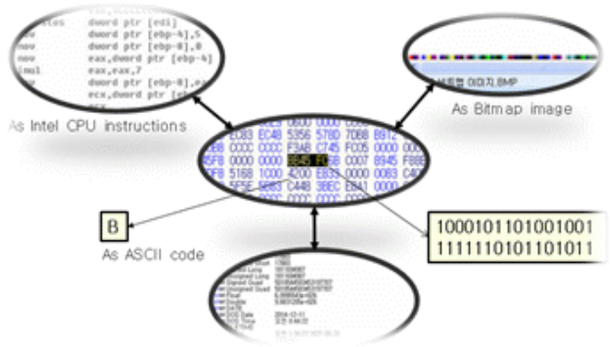

Figure 1. Various types of data.

In this informal Windows operating system installation, we determined installation times for without Window system such as Windows operating system updates, or restoring the ghost image. Many famous PC manufactures put Windows operating system on its local hard disk for reinstalling operating system. In this case, we investigate the installation times as well. The following versions are investigated:

- Windows XP Service Pack 1 and Service Pack 2, Service Pack 3
- Windows 7 Home Premium, Professional or Ultimate

We analyzed and investigated whether the time information on the main operating systems such as Windows XP, Windows 7, and 8 operating system that are currently used mainly ordinary users.

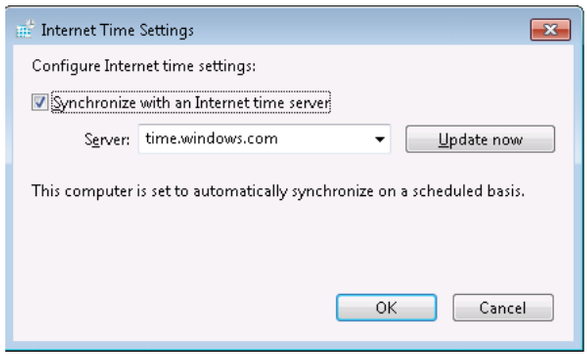

Figure 2. Windows date and time information.

CMOS chip calculates and setups from Jan 1, 2000 to 2099 by 1/1000 (m second) in Windows date and time information which is stored by PC's battery. However, it can be different based on motherboard's production year. When system is booted, RTC retrieves time information in normal condition. Sometimes, time information from time server is synchronized with a local machine time in Figure 2. Therefore, Windows operating time information can be different on PC based on which time server they use.

2. Related Work

2.1 Overview of Operating Systems

Operating systems are primarily resource managers. Namely, the main resource they manage is computer hardware in the form of processors, storage, input/output devices, communication devices, and data. Operating systems perform many functions such as implementing user interface, sharing hardware among users, allowing users to share data among themselves, preventing users from interfering with one another, scheduling resource among users, facilitating input/output, recovering from errors, accounting for resource usage, facilitating parallel operations, organizing data for secure and rapid access, and handling network communications.

2.2 Basic Structure of Operating Systems

Operating system consists of CPU, main memory, disk, network, video, source, and other devices which manage resources efficiently with various modules. Main modules are process manager, input/output manager, memory manager, file manager. Figure 3 shows the basic structure of multiprocesor. Main memory has two parts which are user programs and kernel program. Since the computer is also increased demand for multi-processing the more work that must be processed at the same time, recent CPU architecture has been designed to be suitable for implementing a multi-process. Among them is a typical feature of changing the CPU architecture for implementing virtual memory which makes a load multiple independent programs in memory when the program performed quickly according to the sequence or event for each program can be seen as if they were performed on a computer having a separate CPU. For example, place to store all of the CPU internal registers who gets up during the switching process is performing a program A (or task switching) using the CPU on PCB A, then do the other programs, the program again subjected to the same procedure A. When reading the CPU load on the CPU PCB

A register in order to return to performing. However, the program only has a slight lag time a may appear to be continued. This operation process is called a multi-processing[12,13].

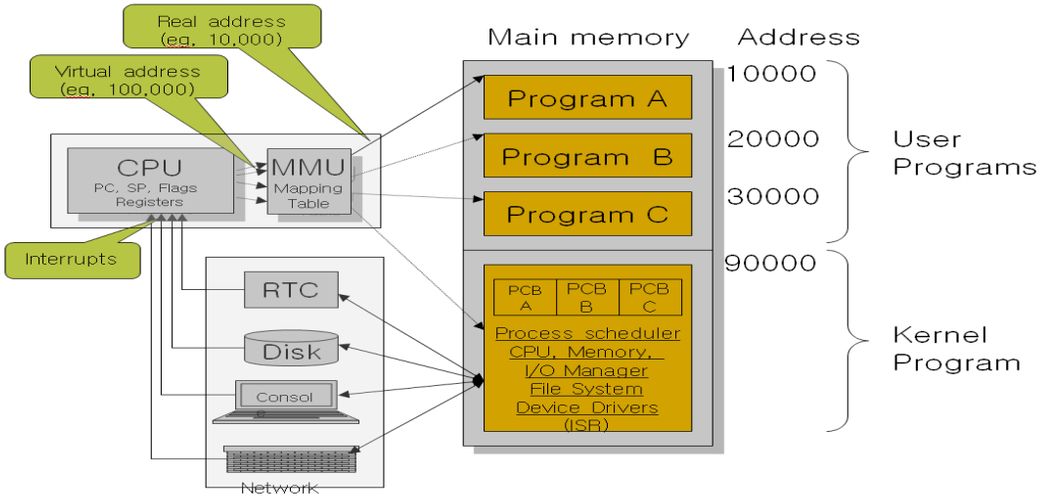

Figure 3. Basic structure of multiprocessor.

2.3 File System

The file system is organized into a stream data and a meta data areas; the former contains the data stored in files, while the latter comprises file information such as the name, time information, file size, and cluster location. The meta data is controlled by the different structures of the file system[1,3,9,11]. The FAT file system stores information on the date and time of creation, last modification, and last access separately as 2 bytes, according to the DOS time format1. The last accessed time actually refers to date information. Table 1 shows the rules governing time information in NTFS[2,4,10].

3. Proposed Method

3.1 Test Beds

The normal procedure by using the Windows installation disc and examine ways to determine if the system setup time to install the Windows operating system. And determine if there are differences by the Windows version, motherboard, notebook PC, etc.,or a change in 32/62 bit operating system checks8. By default, Windows will also examined by using virtual machines, install VMW are or Virtual PC investigating if necessary. We tested Windows 8 time analysis as well. We tested various hardware such as brand-name PC (Dell, Samsung), manufacturing PC, and notebook. We used Final forensics 3.1 and X-Way forensics 16.6. X-Way is famous for X-Ways software technology AG's product, and has Winhex and forensics functions.

This has fast performance and best for analysis binary data.

3.2 Analysis Tools

We used Final forensics as a primary analysis tool and also used X-way forensics 16.6 in order to reduce analysis errors. Final data is developed by Final forensics which is commonly used in forensic. Figure 4 shows Final forensics 3.1. X-way forensics is made by X-Ways software Technology AG which is a famous company for Winhex tool. X-Ways Forensics is based on the WinHex hex and disk editor and part of an efficient workflow model where computer forensic examiners share data and collaborate with investigators that use X-Ways Investigator.

We analyzed the files after installing Windows, and recorded generation time and log files by Final Forensics 3.1. We used X-way forensics 16.6 for analyzing $MFT file's binary. As a result, Table 2 shows Windows 7 installation time analysis.

3.3 $MFT File on Windows 7 Analysis

$MFT file installation time on Windows 7 is shown in Figure 8. It's 04:58:43 at Nov. 24, 2012 which is a UTC time and 9 hours must be added in that time. Therefore, Actual installation time is 13:58:43 at the same day.

Table 1. Rules governing time information in NTFS

Rules	Scenario	Created	Last Written	Last Accessed
1	File creation	File creation time	File creation time	File creation time
2	Same volume copy	File copy time	No change	File copy time
3	Same volume transfer	No change	No Change	File transfer time
4	Different volume copy	File copy time	No Change	File Copy time
5	Different volume transfer	File transfer time	No change	File transfer time
6	File download	Download time	Download time	Download time
7	Extract from the file	Extract time	Extract time	Extract time
8	Automatic scanning tool operation	No change	No change	Tool operation time
9	Preview Thumb.db	Preview beginning time	Preview ending time	Preview ending time

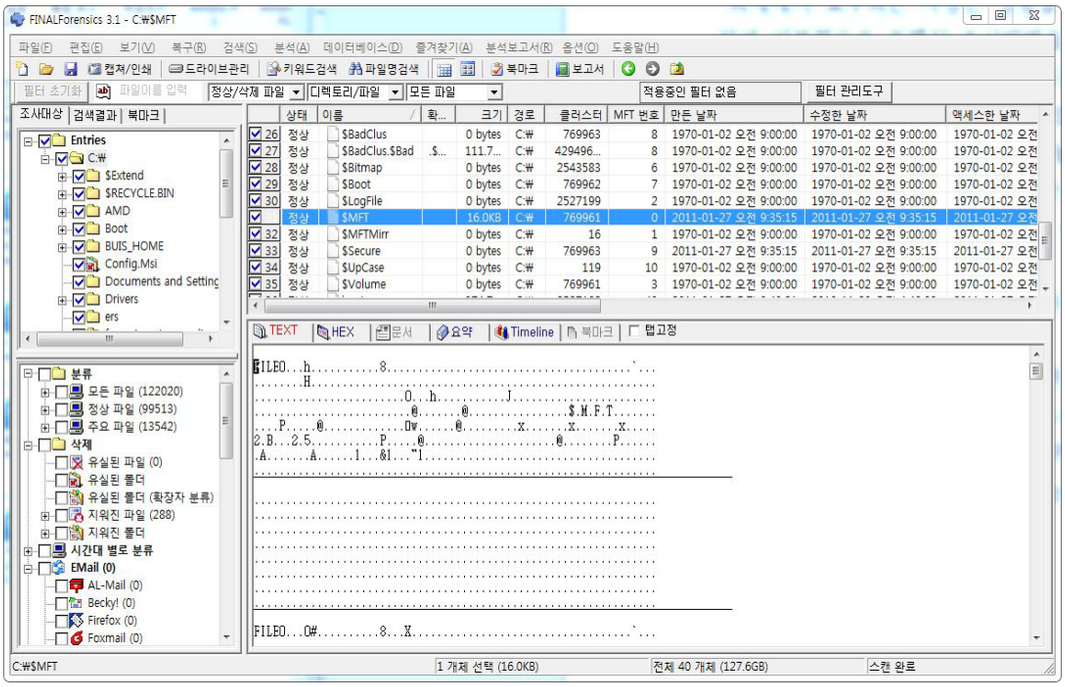

Figure 4. Final forensics 3.1.

3.4 $MFT File on Windows 8 Analysis

$MFT file installation time on Windows 8 is shown in Figure 9. It's 14:53:31 at Dec. 2, 2012 which is a UTC time, and 9 hours must be added in that time. Therefore, Actual installation time is 23:53:31 at the same day. We concluded that Windows 7 and 8 are the same. However, Windows XP has a different file saving time. It shows in Table 4.

4. Conclusion

As digital forensics become increasingly common in the court systems, educated, trained professionals are required to manage the lifecycle of evidence from initial collection through final disposition. In Table 4, $MFT binary files generation time on Windows XP stores as UTC time with 9 hour local time differences, while $MFT binary files generation time on Windows 7 & 8 stored in UTC time in Figure 8 & 9.

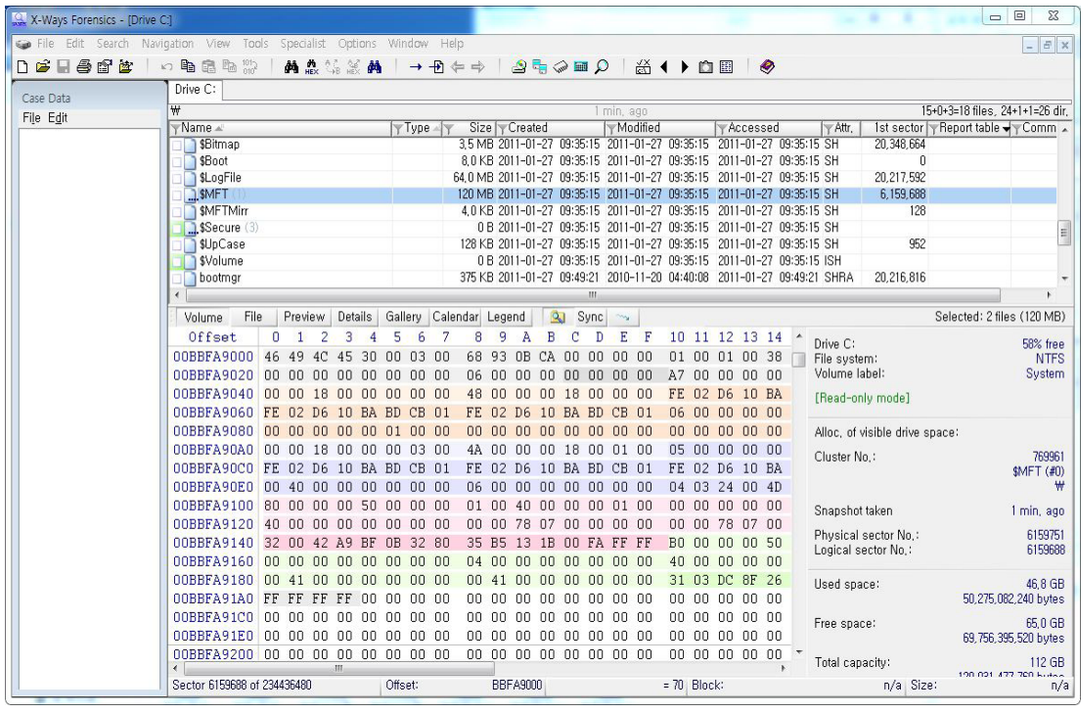

Figure 5. X-Way Forensics.

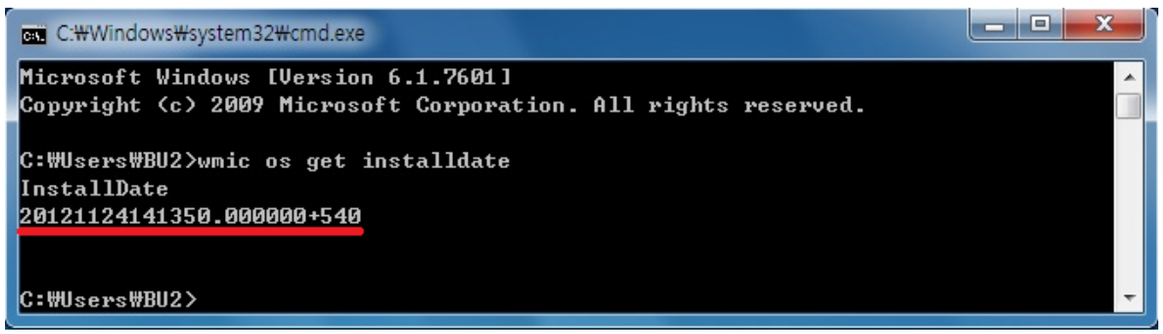

Figure 6. Windows 7 time for installation complete.

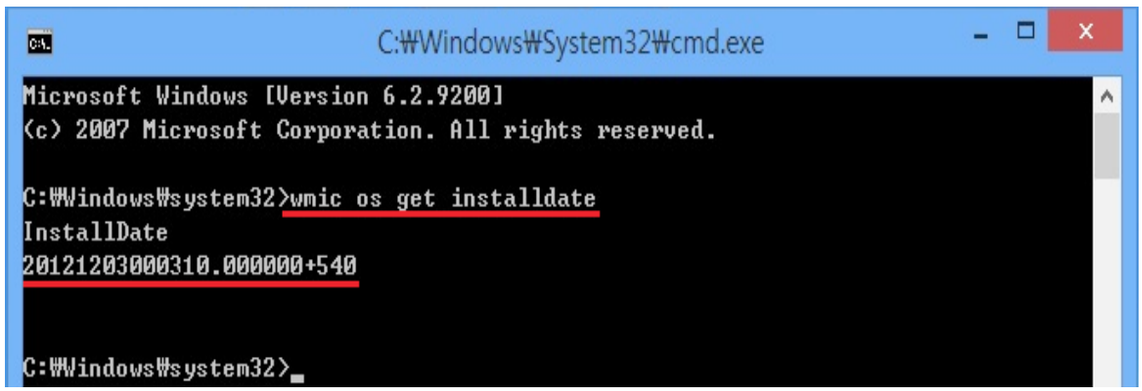

Figure 7. Windows 8 time for installation complete.

Table 2. Windows 7 installation time analysis

Step	Install Process	Observation Time	Generation Time	Generation files and note
1	Power on	13:52:10		CMOS Time : UTC (Local Time)
2	File loading	13:52:50		
3	Setting for language, time, keyboard	13:54:20		
4	Select types of installation	13:58:30		
5	**Starting format**	**13:58:35**	**13:58:34**	$MFT file generation
6	**Format completed**	**13:58:50**		
7	File copy	13:59:10		
8	File extension	13:59:20		
9	Function install	14:04:20		
10	Updateinstall	14:04:50		
11	Installation process	14:05:10		
12	1st rebooting	14:05:15	**14:05:21**	setupact(1), setuperr(1) log file generation
13	Update registry setting	14:06:30	**14:06:39**	setupact(2), setuperr(2) log file generation
14	Installation in process	14:06:35	**14:06:43**	WindowsUpdate, setupapi.dev,
15	Installation completed	14:10:53	**14:10:38** **14:10:40**	DDACLSys, setupact(3), setuperr(3) log file generation
16	2nd rebooting	14:11:02		
17	Ready for computer	14:11:40		
18	User name setting	14:12:17		
19	Password setting	14:12:20		
20	Auto protection and Windows enhancement setting	14:13:35		
21	Time and date setting	14:13:45		
22	Networking setting	**14:13:49**		After network setting and record installation complete time
23	Setting complete	14:13:50		
24	Desktop setting	14:13:53		
25	**Installation complete**	**14:13:50**		

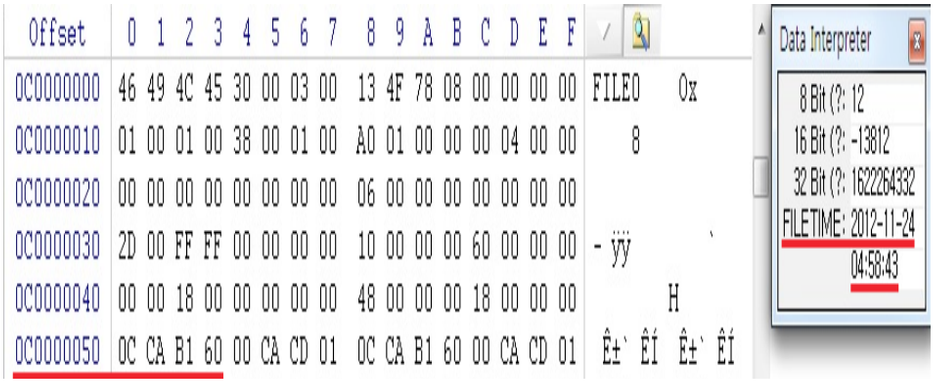

Figure 8. $MFT file installation time on windows 7.

Table 3. Windows 8 installation time analysis

Step	Install Process	Observation Time	Generation Time	Generation files and note
1	Power on	23:49:00		CMOS Time : UTC (Local Time)
2	File loading	23:50:20		
3	Setting for language, time, keyboard	23:51:55		
4	Start installation program	23:52:00		
5	**Start formatting**	**23:53:30**	**23:53:31**	$MFT file generation
6	**Format completed**	**23:53:32**		
7	File copy	23:53:50		
8	Ready for file installation	23:53:52		
9	Installation functions	23:59:23		
10	Installation updates	23:59:30		
11	1st rebooting	23:59:40	**23:59:41**	setupact(1), setuperr(1) log file generation
12	Installation in process	00:00:20	**00:00:47**	setupact(2), setuperr(2), setupapi.setup, DDACLSys, setupact(3), setuperr(3) log file generation
13	Installation completed	00:00:36	**00:01:02**	
14	Ready for devices	00:01:05	**00:01:03**	
15	2nd Rebooting	00:01:27	**00:01:04**	
17	User setting	00:02:10		
18	Setting Completing	**00:03:10**		After setting done and record installation completed time
19	Desktop setting	00:03:50		
20	**Installation completed time**	**00:03:10**		

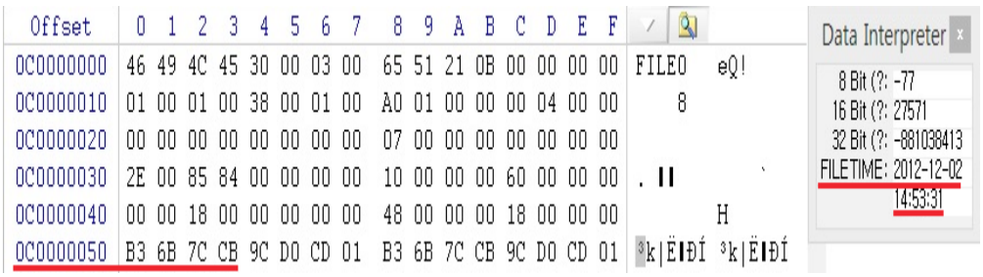

Figure 9. $MFT file installation time on windows 7.

Table 4. Windows 8 installation time analysis

Windows Version	File Saving Time with Binary	$MFT File Generation
Windows XP	UTC+(local time)	2012-11-24 21:03:35
Windows 7	UTC	2012-11-24 13:58:43
Windows 8	UTC	2012-12-02 23:53:31

Time information in digital forensics is important for digital evidence analysis, reconstruction of the incident, and forensic evidence because it is used as the basis guideline for direction of crime investigation. In this research, we tested and analyzed actual time records while Windows operating systems are installed. We proposed that how to prove and analyze Windows files' generation time record with using forensics tools.

5. Acknowledgement

This research is supported by 2015 Baekseok University research fund.

6. References

1. Carrier B. File system forensic analysis. Addison-Wesley; 2005.
2. Chow K, Law F, Kwan M, Lai P. The rules of time on NTFS file system. Proceedings of Systematic Approaches to Digital Forensic Engineering; 2007.
3. Bang J, Yoo B, Kim J, Lee S. Analysis of time information for digital investigation. Fifth International Joint Conference on INC, IMS and IDC, 2009. NCM '09; 2009. p. 1858–64.
4. Huebner E, Zanero S. Open source software for digital forensics. Springer; 2010.
5. Boyd C, Forster P. Time and date issues in forensic computing - a case study. Digit Investig. 2004.
6. Jones R. Internet Forensics. Addison-Wesley; 2005.
7. Steel C. Windows forensics: the field guide for corporate computer investigations. John Wiley & Sons; 2006.
8. Carvey H, The windows registry as a forensic resource, digital investigation. 2005.
9. Christopher WA, Procter SJ, Anderson TE. The nachos instructional operating system. Proceedings Winter 1993 Usenix Technology Conference; 1993. p. 479–88.
10. Rogers M, Seigfried K. The future of computer forensics: a needs analysis survey. Comput Secur. 2004; 23:12–6.
11. Castro M, Lopez-Rey A, Perez-Molina C, Colmenar A, de Mora C, Yeves F, Carpio J, Peire J, Daniel J. Examples of distance learning projects in the European community. IEEE Trans Educ. 2001; 44(4):406–11.
12. Latchman H, Salzmann C, Gillet D, Bouzekri H. Information technology enhanced learning in distance and conventional education. IEEE Trans Educ. 1999; 42(4):247–54.
13. Broucek V, Turner P. Winning the battles losing the war? Rethinking methodology for forensic computing research. J Comput Virol. 2006; (1):3–12.
14. Yasinsac A, Erbacher R, Marks D, Pollitt M, Sommer P. Computer forensics education. IEEE Security & Privacy. 2003 July; 15–23.