IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 22, Issue 3, Ser. I (May - June 2020), PP 42-45
www.iosrjournals.org

Conventional Forensic Approach to Computer Crime Detection

K. Manivannan and V. Ramanan
(Computer Forensics Division, Forensic Sciences Department, Government of Tamil Nadu, Chennai, India)

Abstract: *A novel method is briefed in this paper to verify and confirm whether a suspected computer system is in current date and time settings or not and thereby detecting a Cyber Crime. In this paper, a simplest and powerful methodology is described for collecting indirect clues to fix the computer crime when the chances for direct evidences to prove the crime are remote. A case study in which how the involvement of the digital media viz. a hard disk for sending disputed mail is investigated and by which the proposed method is validated.*

Date of Submission: 29-04-2020 Date of Acceptance: 13-05-2020

I. Introduction

A cyber forensic examiner is always bound with the limitations of the forensic software tools. Sometimes, the forensic scientist might be in the situation to think beyond the limitations to establish the justice. The ultimate aim of the judiciary system, police and forensic organizations is to prove the guilt and to enforce corrective actions on a criminal as well as to protect the innocent by proving his innocence. Hence, to establish the truth, a forensic analyst can go to any extent without deviating much from forensic procedures. In other words, the approach followed by a forensic scientist should not challenge the integrity and reliability of the results.

The forensic examination of digital evidences involved in computer related crimes is relatively a tough task and an expert approach is required to solve the queries raised in the investigation of those crimes (Casey, 2009; Carvey, 2012; Luttgens & Pepe, 2014; Vacca, 2005; Saferstein, 2018; Marcella & Menendez, 2008; Marcella & Guillossou, 2012; Jaishankar, 2011; Petherick, Turvey & Fergusson, 2009). Nowadays, as the usage of internet and browsing of web pages is increasing in exponential rate, the computer crimes extend its area to networks and in turn, crimes in the internet (cyber crimes) are increased to a high degree. So, the vestiges unknowingly (or even knowingly without realize its impact) left by a criminal in a computer on using its internet can be a potential evidence against him to prove his crime. In normal course, in a computer crime or network crime, to hide a particular criminal activity, a criminal can delete the concerned file or data immediately. But it can be retrieved easily using forensic software tools by parsing the physical area of the disk (said to be unallocated clusters or sectors). Unfortunately, in some cases, the concerned deleted file or data might be overwritten, and henceforth evidence may not be retrieved completely.

II. The Problem

Computer forensic analyses and reporting are largely relies on date and timestamp information of the files present in digital evidence (Boyd & Forster, 2004). Timestamps are nothing but metadata of files that reflects when a particular file was created, modified and last accessed. In some cases, while performing the forensic examination of digital evidences such as hard disks, the last access timestamp of the hard disk of a computer might be very well before (or after) the actual occurrence of the crime on the system. For instance, if a computer crime is said to be committed on a particular day but the data or information stored on the hard disk of the computer might not show even a single access on that day *i.e.* the access of the hard disk ended some weeks or months before the incident or occurrence of the crime. Then a forensic examiner immediately suspects that the computer's date and time settings might be purposely backdated using some anti-forensics tools such as "timestomp" (Offensive Security, 2020; Dumont & ESET, 2017) which can modify or delete the timestamps of a file's creation, modification and access. Using these tools, a user can make any number of files useless towards legal trial by challenging the credibility of the files. Unforeseen chaos is the ultimate result of a forensic analysis if tampering the date and timestamp records. Otherwise, unknowingly the system might have been used with earlier date and time settings. Moreover, one should look on the other side of the coin too *i.e.* one should not neglect the possibility for the innocence of the accused since, the whole judiciary system is following the "Blackstone's ratio" (Blackstone, 1893) which state that "*It is better that ten guilty persons escape than that one innocent suffer*". In such circumstance, the responsibility of a forensic electronic examiner becomes very crucial to prove the guilt or innocence.

In this context, if the computer as a whole is sent for examination, one can examine the Complementary Metal-Oxide Semiconductor (CMOS) setup to verify the current date and time of that system (it

is also true that the use of anti-forensics tools for date and timestamp tampering still complicates the analysis). The CMOS is a semiconductor chip mounted on the motherboard which includes a simple clock function that keeps the track of the current date and time information. However, in real cases, the concerned hard disk alone is seized and sent for examination for one of the following reasons.

1. It is practically difficult for the police to carry the whole computer system to the forensic laboratory for examination. It needs extra manpower and increases the transportation charges.
2. It is difficult to seize the server computers of an organization, company and so forth. In this circumstance, it is ideal to seize the hard disk alone.
3. If the computer or the motherboard are physically damaged by accident or intentional actions, the hard disk alone will be sent for examination provided it is undamaged.

Hence, a forensic examiner has to look forward for alternative methods. One such method is discussed below.

III. Suggested Methodology

In the concerned hard disks under investigation, the stored data pertaining to the web related pages should be examined carefully. On examining the contents of those offline web pages, some of the information in the web contents may represent the contemporary period of that file's creation. More clearly, a web content may have an information pertaining to a particular notable real event and the date of that event might be known to everybody for example, the date of sports matches, presidential elections of a country, terrorist attacks, natural calamity, famous supreme court verdicts, death of celebrities, notable events to mention a few. Some web pages may even pertain to e-news papers which may show the date itself, or the date can be ascertained from the content of the news. Once, one of these unique web contents were identified, by observing the date of creation of that web content or file would reveal the fact regarding the date of creation of that file. If the date of creation of the file is earlier to the date of that event, it can be concluded that the system was running with earlier date and time settings. If the date of creation of the file is later to that event, the system may be running with current and correct date and time settings and finally it can be concluded that the hard disk sent for the examination might or might not been involved in that crime.

Similarly, one can look forward the web pages displaying a running-clock-setting in its contents which can be readily examined to ascertain whether the date of creation of such a web page is comparable with the running-clock-time or not. In addition, one can ascertain whether the clock setting is synchronized with the web server's timestamp and time zone, by a close analysis of the html script of the web page which contains the clock setting. A case study in this regard is depicted below.

IV. A Case Study

History of the case: In a charge of anonymous threatening email sent to the VIP (Chief Minister of a State), a hard disk was seized from the suspected criminal and sent for forensic examination. The examination of the hard disk with a forensically sound software tool revealed that i) no evidence could be retrieved for sending email from it and ii) the last access shown on the hard disk was three months before the actual incident. However, the points to be ascertained were i) whether the evidence was over-written (non-recoverable) or ii) the hard disk was not used for sending email.

During the examination of web and mail related contents with the assistance of the forensic software tool EnCase v6.6, an offline web page (pertaining to Indian Institute of Science, Bangalore -Admission Details Page) was found to contain a running clock setting and the time and date shown was noted. The date and time shown in the web page was 13.03.2007 / 04:18:38 PM. The date of creation and last access of the file containing the above web content was also exactly same as the running date and the time shown was lagging behind about 1.5 hours and same could be attributed due to the difference in clock setting of the computer system used for browsing. More clearly, the time shown in the web page was basically dependent on the server time but the time of saving or creation of the web page onto the hard disk was dependent on the local time setting of the computer system in which the hard disk was connected. From the above findings, it was concluded that the hard disk was not being used to send the email, since there was no difference between the actual timestamp and the timestamp of the web content. On top of it, the date and timestamp further revealed that the recent access ("last accessed" timestamp) of the hard disk under examination was three months before the date of occurrence. The screenshot of the offline web page and its corresponding metadata are shown in Figure 1 and Table 1 respectively.

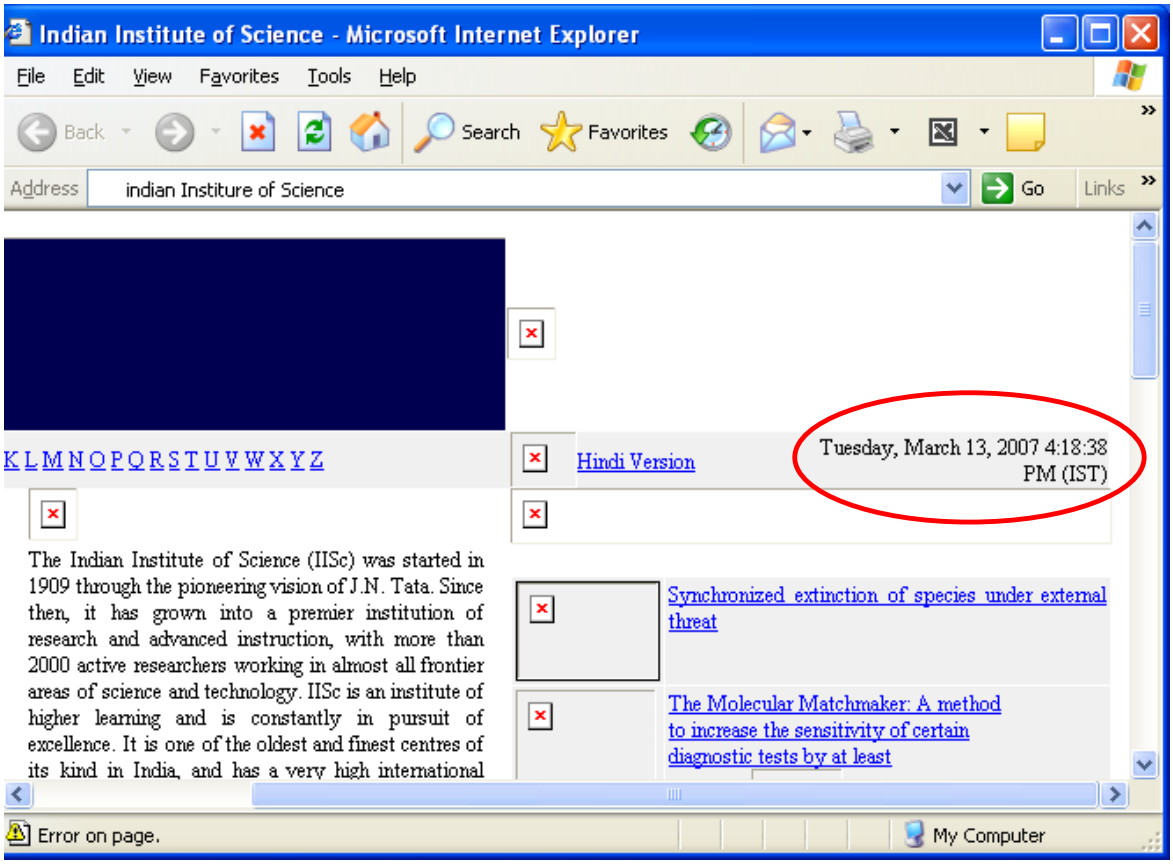

Figure 1. Screenshot showing clock settings (marked in red colour to highlight), in a web page pertaining to IISC, Bangalore, India

Table 1. Metadata of the web page pertaining to IISC, Bangalore, India

Name.Ext	iisc.ernet[1].htm
File Type	Web Page
File Category	Document
Description	File, Deleted, Archive
Last Accessed	03/13/07 05:51:45 PM
File Created	03/13/07 05:51:42 PM
Last Written	03/13/07 05:51:45 PM
Entry Modified	03/13/07 05:51:45 PM
Logical Size	65,243
Physical Size	65,536
Physical Location	22,858,841,600
Physical Sector	44,646,175
Evidence File	Disk Image
File Identifier	12778
Full Path	Disk Image\C\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\SZ2DWP6L\iisc.ernet[1].htm

V. Extension of the Methodology

The above methodology can also be extended to the standalone computers, i.e. the computer or hard disk that was not connected to the internet which ruled out the possibility for the presence of web related contents in the hard disk. In this case, another idea can be suggested. The files pertaining to the letters of correspondence or any other documents bearing dates included in the contents of the document should be examined carefully for their date of creation. If a letter/document bearing a particular date, by logic, that document could not be created before that particular date. Moreover, in the body of the letter or document, one may get the information of the contemporary period of creation of such document. If there is any time anomaly is noted in a particular file, the date and time difference can be used to calibrate the date and time of the file of interest.

VI. Conclusion

A plethora of reports are available in the literature that technically dealing with the computer crimes using forensic software tools. Whereas, the reports pertaining to handling of a computer crime with logical conventional approach, without using forensic software tools are lacking in the literature. Hence, there is no scope in the available literature, to make an examiner to think beyond the routine software-based forensic procedures. Logical thinking is an important criterion of a forensic scientist and the digital forensic examiners are not exceptions. Hence, documentation of the reports dealing computer crimes with logical approach is the need of the hour. In this paper, a conventional method to assess whether a suspected computer system is in current date and time settings or not, is briefed. The method involves use of conventional or logical forensic approach, rather than applying any hi-tech knowledge in computers, operating systems and application of software tools. Using this method, one can effortlessly ascertain whether the suspected computer system is running with current and correct date and time settings or not. This information will be of much significance in sensational cases where the date of creation of files plays a vital role.

Acknowledgements

Authors express their gratitude to Mr. M. Srinivasan, Director *i/c* of Forensic Sciences Department, Tamil Nadu, India, and extends their thankfulness to Mrs. A. Visalakshi, Deputy Director of Computer Forensics Division for their motivational supports. The authors also thank Dr. G. M. Ranjit Cecil, Additional Director (Rtd.), Dr. G. Thirunavukkarasu, Deputy Director of Ballistics Division, Forensic Sciences Department and Dr. N. Kala, Assistant Professor, Centre for Cyber Forensics and Information Security, University of Madras, for their persistent moral supports.

References

[1]. Blackstone, W. (1893). Commentaries on the laws of England in Four Books. Philadelphia: J.B. Lippincott Company.
[2]. Boyd, C., Forster, P. (2004). Time and date issues in forensic computing – a case study. *Digital Investigation, 1(1)*, 18-23.
[3]. Carvey, H. (2012). *Windows Forensic Analysis Tool Kit: Advanced Analysis Techniques for Windows 7, Third Edition*. Waltham, MA: Syngress.
[4]. Casey, E. (2009). *Handbook of Digital Forensics and Investigation.* Burlington, MA: Academic Press.
[5]. Dumont, R., ESET. (2017). Timestomp. Retrieved on 03.05.2020 from https://attack.mitre.org/techniques/T1099/
[6]. Jaishankar, K. (2011). *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior*, Boca Raton, FL: CRC Press.
[7]. Luttgens, J. T., Pepe, M. (2014). *Incident Response & Computer Forensics, Third Edition*. USA: McGraw Hill Education.
[8]. Marcella, A. J., Guillossou, F. (2012). *Cyber Forensics: From Data to Digital Evidence*. Hoboken, New Jersey: Wiley.
[9]. Marcella, A. J., Menendez, D. (2008). *Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, Second Edition*. Boca Raton, FL: Auerbach Publications.
[10]. Offensive Security. (2020). Timestomp. Retrieved on 03.05.2020 from https://www.offensive-security.com/metasploit-unleashed/timestomp/
[11]. Petherick, W. A., Turvey, B. E. Fergusson, C. E. (2009). *Forensic Criminology*. Burlington, MA: Academic Press.
[12]. Saferstein, R. (2018). *Criminalistics: An Introduction to Forensic Science, Twelfth Edition*. Boston, New Jersey: Pearson Education.
[13]. Vacca, J. R. (2005). *Computer Forensics: Computer Crime Scene Investigation, Second Edition*. Boston, Massachusetts: Charles River Media..

K. Manivannan. "Conventional Forensic Approach to Computer Crime Detection." *IOSR Journal of Computer Engineering (IOSR-JCE)*, 22(3), (2020), pp. 42-45.