Journal of Forensic Sciences And Criminal Investigation
ISSN: 2476-1311

Juniper Publishers key to the Researchers

Case Report
Volume 12 Issue 2 - July 2019
DOI: 10.19080/JFSCI.2019.12.555831

J Forensic Sci & Criminal Inves

Anatomy of a Bloggers Activity: A Case Study

Kananbala Jena*

Central Forensic Science Laboratory, 30 G C ROAD, Kolkata-700014, India.

Submission: June 21, 2019; **Published:** July 17, 2019

***Corresponding author:** Kananbala Jena, Central Forensic Science Laboratory, 30 G C ROAD, Kolkata-700014, India.

Introduction

Blogs emerged in the late 1990s as a means of publicising personal or group thoughts on World Wide Web in a diary like format. Availability of web publishing tools for computer users without knowledge of computer programming and website building worked as catalyst towards growth of blogging activity in different subjects. There are many blogging platforms options. some of the popular option are 'WordPress', 'Tumblr', 'Blogger', 'Weebly', 'Wix' and 'Squarespace'.

This paper will discuss examination of electronic exhibits allegedly seized from a blogger and the artefacts found in them. Computer forensic examiners challenge is to find traces of blogging activity and consider significance of this trace with reference to available technology. However, computer user being human is also an important factor to be considered. Certain Bents of Human mind is also obvious when handling a computer. It may be the way files and folder are named, choice of colors or preference of usernames. Observation of activities and finding trends in them can be very important resources for analysis when combined with results obtained from forensic tools.

Method

Case description

The exhibits seized contained one computer CPU and one tablet. Print out of the concerned blog pages as well as some screenshots of face book of the accused were supplied for comparison. The blogging site name 'xyz' (name changed as the matter is sub-judices) contained many cartoons with caption. It was suspected that the accused has hosted the website and using a mail address 'abc@gmail.com' (address changed as matter is sub-judice) to publish the blog 'xyz'.

Extracts from CPU

Bit stream image of the hard disk inside CPU was prepared using Encase Forensic software and examined by Encase forensic software and internet evidence finder.

Presence of relevant file and folder

The folder 'xyz files' could be found containing files with 'CSS', 'js' and 'HTML' extension as well as loaded_0 file within a folder 'my web pages'. In addition to 'xyz files' there were other folders with '_files' as the name of folder in the end. Name of all these folders was relevant to the subject which was depicted in blog under investigation. Each folder also contained some images with extension 'jpg', 'bmp' and 'png'. Some of the images were cartoon relevant to investigation. Some of the images were buttons and other indicators with same color as disputed web page.

There was folder containing cartoons in line with blog under investigation. Some of these cartoons which were images was also available in the supplied print outs of the blog and face book page screenshots. There were folders containing 'eBooks' with similar agenda as the blog under investigation. A folder with name 'blog data' was available containing files and folders with similar content.

Impression

The user is passionate about the subject of blog in question which is evident from reference to several resources available in his computer.

The files with extension 'CSS' stand for cascading style sheet which is used to define styles for web pages, including the design, layout and variations in display for different devices and screen sizes. The files with 'html' extension describe the content of a web page. Name of the blog could be found within the text of 'html' file. The. loaded_0 file format is used for JavaScript program files. This file format was developed by Google for the API (Application Programming Interface) of Google+ among their other tools and services. The data contained in these. loaded_0 files may contain code that instructs the application to load external libraries and other resources of other Google tools and services. JS file is a text file containing JavaScript code that is used to execute JavaScript instructions in web pages. It may include functions that open and close windows, validate form fields, enable rollover images, or create drop-down menus. Therefore, content of the web page was available in the user's computer.

Email analysis

One email archive 'outlook.pst' was available. Personal Storage Table (.pst) is an open proprietary file format used to

store copies of messages, calendar events, and other items within Microsoft software such as Microsoft Outlook. The archive found to be relevant to 'def@gmail.com' which is different from email address under investigation.

However, Keyword 'abc@gmail.com' could be found in keyword search. It is also observed that the recovered email from archive relevant to 'def@gmail.com' contained several sent mails to 'abc@ gmail.com' and other email addresses whose usernames and contents were in synch with the subject of blog under investigation. But the inbox recovered from archive did not contain any email received from the email address 'abc@ gmail.com' or other emails to which user was sending emails frequently. Some such emails contained links from blogs other than blog 'abc@gmail.com' under investigation. Though the contents of these links could not be verified name of the link indicated the contents may be relevant.

Impression

The user has contact with ''abc@gmail.com' and other email addresses whose usernames and contents were in synch with the subject of website under investigation. These emails including ''abc@gmail.com' do not send answer indicates the primary purpose is not email communication, but, sending records for some other application. In addition, there is strong indication that the user of the device has access to these emails on other devices not under current investigation. Link from other blogs also indicates he may be a contributor to these blogs.

Internet Artefacts

Chrome auto fill, Chrome bookmarks synchronous to investigation found. Facebook comments, Facebook pictures contain words relevant to subject under investigation. The rebuilt webpages indicate access to editing of relevant Webpages.

Extracts from tablet

Chat: The tab contained some 'WhatsApp' conversation regarding the blog and links were sent to contacts from the blog in question. There is conversation where the user admitted the fake account id is created by himself.

Email: The emails recovered suggest two email account was associated to the device. One of them is 'def@gmail.com' another is email 'ghi@gmail.com' which is not under investigation. The email 'ghi@gmail.com' was also available during earlier keyword searches in CPU. The activity analytics suggested 8 emails were sent from 'ghi@gmail.com' to 'def@gmail.com' whereas one email was received by ' ghi@gmail.com' fro 'def@gmail.com'. It is also observed that the 'def@gmail.com' sent mails to 'abc@gmail.com' and other email addresses whose usernames and contents were in synch with the subject of blog under investigation.

Impression

It is more established at this stage that there is interaction between the emails which was not available in CPU. Moreover, the two email addresses being owned by one device substantiates user has multiple email addresses and uses them selectively through different devices.

Web History and Web Bookmark

URL referred in web history and web bookmark section show many websites relevant to investigation.

Cookies

_utmz cookie containing name of the blogging site was available. _utmz holds information about the way user entered the website. Value of this cookie was '7433012.1463175562. 1.1. utmcsr=xyz. BlogSpot. in|ut mccn=(referral)|utmcm d=referral |utmcct=/∴ utmcsr= xyz.blogspot.in. Xyz being name of the blog site under investigation. In this context it deserves mention that there are different types of cookies by google:

_utma cookies

The first (at least in Google's naming scheme) cookie is used to identify unique visitors.

__utmb and __utmc,

These cookies are used to determine sessions. Together they are able to identify unique sessions.

utmz, identifies traffic sources.

Language

The language used by the user was one Indian language which is common to both devices. The user inserted many symbols which unique to the subject of his blogging are also found on both devices.

Inconclusive parts confirmed by user habit

Log in status of all the email could not be confirmed. However, it is observed that the user is in the habit of creating PowerPoint files frequently for print going by the creation date of files. Observation through PowerPoint reveals files one file containing username and password of 10 email address, 02 Facebook account, 03 blogger account including the account under investigation could be found.

Conclusion

The artefacts recovered may be considered an eco-system of activity of the user on electronic devices owned by the user. The user activities of both devices could be linked to each other on timeline and contents. Both internet artefacts as well as user activity has strong roles in decision making which could be demonstrated by facts of this case.

References

1. Nalawade, S Bharne, V Mane, (2016) Forensic analysis and evidence collection for web browser activity, 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), Pune pp.518-522.

How to cite this article: Kananbala Jena. Anatomy of a Bloggers Activity: A Case Study. J Forensic Sci & Criminal Inves. 2019; 12(2): 555831. DOI: 10.19080/JFSCI.2019.12.555831

2. K Dhar, Y Pingle, (2016) Digital Forensic Investigations (DFI) using Internet of Things (IoT). 2016 3rd International Conference on Computing for Sustainable Global Development (INDIA.Com), New Delhi, pp. 1443-1447.
3. Nik Zulkipli, Nurul Huda, Alenezi, Ahmed, Wills, et al. (2017) IoT Forensic: Bridging the Challenges in Digital Forensic and the Internet of Things pp. 315-324.
4. Bača, Miroslav, Ćosić, Jasmin, Ćosić, et al. (2013) Forensic analysis of social networks (case study). Proceedings of the International Conference on Information Technology Interfaces ITI, pp. 219-223.
5. Pajouh HH, Javidan, Khaymi, Dehghantanha (2016) A Two-layer Dimension Reduction and Two-tier Classification Model for Anomaly-Based Intrusion Detection in IoT Backbone Networks, 6750(c) pp. 111.
6. Zhang ZK, Cho MCY, Wang (2014) IoT Security: Ongoing Challenges and Research Opportunities. In 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications pp. 230-234.
7. Perumal S, Norwawi NM, Raman V (2015) Internet of Things (IoT) digital forensic investigation model: Top-down forensic approach methodology. In 2015 5th International Conference on Digital Information Processing and Communications (ICDIPC) pp. 19-23.
8. Oriwoh E, Jazani D, Epiphaniou G, Sant P (2013a) Internet of Things Forensics: Challenges and Approaches. In Proceedings of the 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Work-sharing. ICST.
9. Ruan K, Carthy J, Kechadi T, Crosbie M (2011) Cloud Forensics. In: Peterson G, Shenoi S. (eds.) Advances in Digital Forensics VII, of the series IFIP Advances in Information and Communication Technology, Springer, Berlin, Heidelberg Pp 361.
10. Edington Alex, RM, Kishore R (2017) Forensics framework for Cloud computing. Computers and Electrical Engineering 60: 193-205.
11. Dykstra J, Sherman AT (2011) Understanding issues in Cloud Forensics: Two Hypothetical Case Studies. Proceedings of the Conference on Digital Forensics, Security and Law p. 45-54
12. Kebande, Ray, (2004) Network traffic as a source of evidence: tool strengths, weaknesses, and future needs, Digital Investigation 1(1): 28-43.
13. Morrison L, Read H, Xynos K, Sutherland I (2017) Forensic Evaluation of an Amazon Fire TV Stick. In: Peterson G, Shenoi S (eds) Advances in Digital Forensics XIII. Volume 511 of the series IFIP Advances in Information and Communication Technology pp. 63- 379.
14. Liu C, Singhal A, Wijesekera D (2017) Identifying Evidence for Cloud Forensic Analysis. In: Peterson G, Shenoi S. (eds) Advances in Digital Forensics XIII. 410 of the series IFIP Advances in Information and Communication Technology pp. 111-130.
15. Hegarty RC, Lamb DJ, Attwood A (2014) Digital Evidence Challenges in the Internet of Things. Proceedings of the Tenth International Network Conference (INC 2014) 163-172.
16. O Shaughnessy S, Keane A (2013) Impact of Cloud Computing on Digital Forensic Investigations. In: Peterson G, Shenoi S (eds) Advances in Digital Forensics IX. Volume 410 of the series IFIP Advances in Information and Communication Technology pp. 291-303.
17. Ryder S, Le Khac, NA (2016) The End of effective Law Enforcement in the Cloud? To encrypt, or not to encrypt, 9th IEEE International Conference on Cloud Computing, San Francisco, CA, USA.
18. Lillis D, Becker B, OSullivan T, Scanlon M (2016) Current Challenges and Future Research Areas for Digital Forensic Investigation.
19. Ariffin A, Slay J, Choo KK (2013) Data Recovery from Proprietary Formatted CCTV Hard Disks Digital Forensics, Chapter in Peterson G, Shenoi S. (eds) Advances in Digital Forensics IX, Volume 410 of the series IFIP Advances in Information and Communication Technology pp. 213-223
20. Richard G, Le Khac NA, Scanlon M, Kechadi MT (2016) Analytical Approach to the Recovery of Data from CCTV File Systems, The 15th European Conference on Cyber Warfare and Security, Munich, Germany.
21. https://www.macrumors.com/2015/04/23/applewatchdiagnostic-port-confirmed

DOI: 10.19080/JFSCI.2019.12.555831

How to cite this article: Kananbala Jena. Anatomy of a Bloggers Activity: A Case Study. J Forensic Sci & Criminal Inves. 2019; 12(2): 555831. DOI: 10.19080/JFSCI.2019.12.555831