Volume 5, Issue 1, January 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

# Implementation of Email Tracing Algorithm

**Gurpreet Singh**
M.Tech Student (CSE), PTU
Punjab, India

**Mnupreet Kaur**
Computer Science Engineering, PTU
Punjab, India

***Abstract—Email is a data and correspondences technology. It utilizes technology to convey a digital message over the Internet. There are numerous software stages accessible to send and get. Clients utilization email in an unexpected way, based on how they consider it. The proposed work is to develop an algorithm to that works with all modern email companies including Hotmail, Gmail, Yahoo, AOL etc and all client side email programs including Outlook, Eudora etc. We do not need to download any software or plug-in to use our Email tracking Portal, just send the emails in the same way as we send now and find the results that how many recipient opened the email and how many times a single recipient opened it.***

***Keywords— Email, Cookies, Tracking, HTTP, SMTP.***

## I. INTRODUCTION

Email, short for Electronic Mail, consists of messages which are sent and received using the Internet. E-mail system comprises of various hardware and software components that include sender's client and server computers and receiver's client and server computers with required software and services installed on each. Besides these, it uses various systems and services of the Internet. The sending and receiving servers are always connected to the Internet but the sender's and receiver's client connects to the Internet as and when required [1].

Email tracking is a method for monitoring the email delivery to intended recipient [2]. Most tracking technologies use some form of digitally time-stamped record to reveal the exact time and date that an email was received or opened, as well the IP address of the recipient.

Email tracking is useful when the sender wants to know if the intended recipient actually received the email, or if they clicked the links. However, due to the nature of the technology, email tracking cannot be considered an absolutely accurate indicator that a message was opened or read by the recipient.

Most email marketing software provides tracking features, sometimes in aggregate (e.g., click-through rate), and sometimes on an individual basis.

The Internet has smuggled itself to become a large part of most people's lives up to the extent that some people cannot go an hour's length without login in online to do you-know-what or to meet you-know-who. Some are even live online 24 hours a day. It may or may not be possible to track what an actual user does while online but it is these persistent people's online activities that makes it easier for someone, if he wants to, to track them and know actually what they have done, the sites they visited and even their individual preferences. These methods of tracking is usually done by e-commerce websites in order to build customer profiles and spam their mailboxes and emails with junk mails containing adverts of what they think that customer might be interested in.

There are many areas to look at when formulating a method for actually identifying an individual user of an online session [3]. Some of the methods are given below:

### *A. Cookies*

Cookies (sometimes called HTTP Cookies) are text files created by a server that serves as a token and passed on to a client machine to be stored in the web browser in order to identify a returning user. Whenever the client logs in to the server again, the token will be sent to the server and it will identify him as a returning user and allow him to continue using the resources from where he left off the previous time. It will even indicate the links he clicked the last time he was there.

Cookies contains information such as a unique serial number for identification, your login details (only for some) and previous URL links clicked on the website among other things like domain name and expiration date [4 and 5]. Cookies provide the means for web servers to personalise and tailor browsing sessions for each individual user like remembering the items in a shopping cart from a previous visit to an e-commerce website.

### *B. Tracking Devices*

The next set of resources in tracking and identifying an online user is by the use of tracking devices. These can range from software that someone can install on his computer and monitor a particular person's network traffic to other shadowy means websites uses to track visiting users. The software could involve Roundup and Bugzilla as presented by Johnson and Dubois [6].

 

The tracking device we are going to focus on here is the one that websites use surreptitiously and covertly to track a user and it is called a Web Bug. It is also called Clear GIF or Web Beacons. A web bug is an invisible 1x1 pixel graphic image typically in the Graphic Interchange Format (GIF) that is placed on a website in order to track the activity of a user on that website or through a collection of sites. It sends information to the server of the users IP address, location, date, time and sites visited. Because these beacons are invisible and very small, they are almost impossible to be seen by the user. Web bugs raise a lot of issues because they track an individual user and transmit his information without him even knowing it or without his consent.

### *C. Scripting*

Online users can also be tracked by the use of scripting languages. Scripts are automatically activated whenever a user visits a website and the website can manipulate it to view portions of a user's browsing history and also create a log file for that user on the server.

### *D. Eavesdropping*

Eavesdropping is one of the basic attacks in order to track an individual user of his online behaviour. This involves the tracker capturing packets sent by the user in a particular network using packet sniffer software like Wireshark. The tracker can analyse the sender's IP address and the destination IP address, the packet payload, which might contain sensitive information like names, addresses and even phone numbers.

In order for the tracker to know the site that the user is visiting, he will have to enter the destination (server's) IP address in his browser for the DNS server to translate the name into a friendly language. The tracker can now update his tracked user's profile by adding that this particular user has visited this particular website.

It is sufficient to now that a user's IP address can be used to track his geographical location up to the level of his zip code because in each network, an IP address is unique to a particular machine. If a particular users IP address does not change every time he visits a website, then that site will have a good idea that it is the same user that visits every time.

## II. RELATED WORK DONE

Duane Bachmann et al. [7] in 1996 discussed that Advances in computer technology and the increased popularity of electronic mail applications have enhanced the potential for conducting survey research through e-mail. In an experiment comparing mail and e-mail data collection, email fared well with respect to response rates, item omission, response time, and data quality. The authors make a case for using e-mail to conduct research, but only under specific circumstances.

Matthew G. Schultz et al. [8] presented Malicious Email Filter, MEF, a freely distributed malicious binary filter incorporated into Procmail that can detect malicious Windows attachments by integrating with a UNIX mail server. The system has three capabilities: detection of known and unknown malicious attachments, tracking the propagation of malicious attachments and efficient model update algorithms. The system filters multiple malicious attachments in an email by using detection models obtained from data mining over known malicious attachments. It leverages preliminary research in data mining applied to malicious executables which allows the detection of previously unseen, malicious attachments. In addition, the system provides a method for monitoring and measurement of the spread of malicious attachments. Finally, the system also allows for the efficient propagation of detection models from a central server. These updated models can be downloaded by a system administrator and easily incorporated into the current model. The system will be released under GPL in June 2001.

Barry Leiba et al. [9] in 2005 explained that most proponents of domain authentication suggest combining domain authentication with reputation services. This paper presents a new learning algorithm for learning the reputation of email domains and IP addresses based on analyzing the paths used to transmit known spam and known good mail. The result is an effective algorithm providing the reputation information needed to combine with domain authentication to make filtering decisions. This algorithm achieves many of the benefits offered by domain-authentication systems, black-list services, and white-list services provide without any infrastructure costs or rollout requirements.

Vladimir V. Riabov [10] in 2005 explained that SMTP is an application protocol from the TCP/IP protocol suite that enables the support of e-mail on the Internet. Mail is sent by a series of request–response transactions between a client and a server. The transactions pass the message, which is composed of header and body, and the envelope (SMTP source and destination addresses). The header contains the mail address(es), which consists of two parts: a local address (also known as a "user mailbox") and a domain name. Both SMTP client and SMTP server require a user agent (UA) and a mail transfer agent (MTA). The MTA function is transferring the mail across the Internet. The command–response mechanism is used by SMTP to transfer messages between an MTA client and an MTA server in three stages: connection establishment, mail transfer, and connection termination. The envelope is transmitted separately from the message itself using the MAIL and RCPT commands. MIME, which is an extension of SMTP, allows the transfer of non-ASCII (multimedia) messages. POP3 and the IMAP 4 together with SMTP are used to receive mail by a mail server and hold it for hosts. The SMTP's lack of security is a problem for businesses. The security in the SMTP transactions can be supported by S/MIME and other methods. Vulnerabilities of SMTP, POP, and IMAP servers (buffer overflow, mail relaying, spoofing, and other attacks) have been analysed.

## III. METHODOLOGY

Flow Chart for email tracking is shown in Fig.1. The steps for email tracking algorithm is as follows:-

Step 1. Compose the email.

 

Step 2. Send the hidden link of query string behind an image.

Step 3. The recipient opens the email.

Step 4. Information (date of email reading, subject, email ID) of the recipient send to the server page by query string.

Step 5. Check whether the information is currently exists for particular subject. If the information is currently exists for particular subject then the counter is updated by 1 in the database. Otherwise the information is stored in the database.

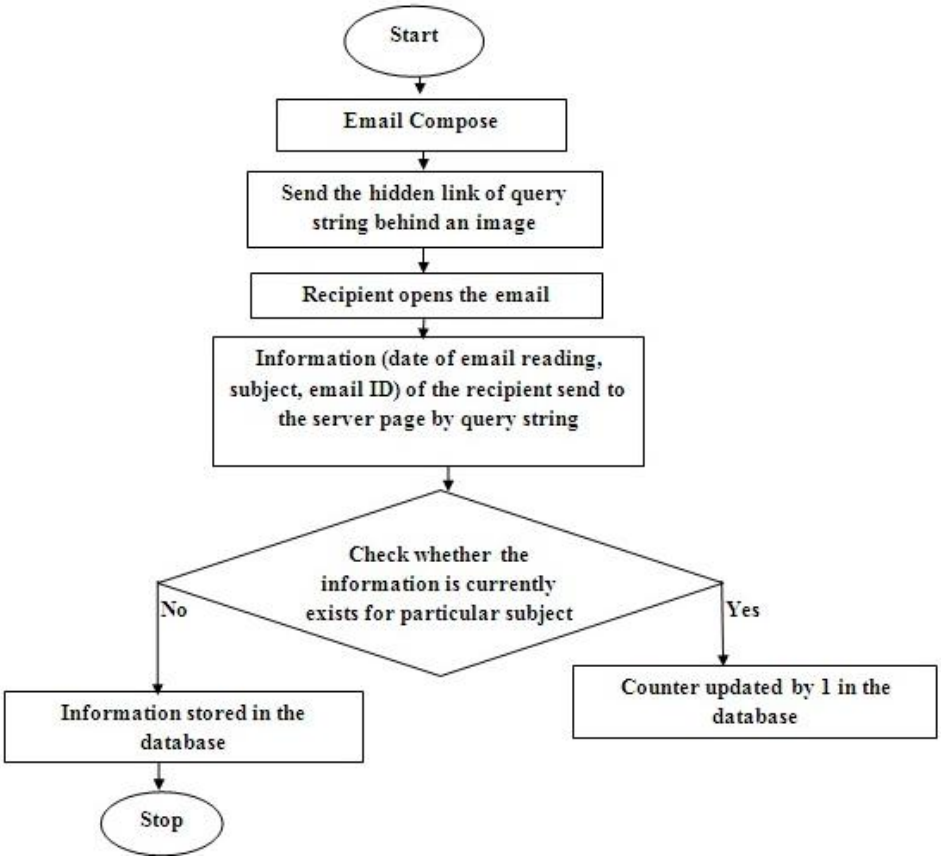


Fig.1 Flow Chart of the Purposed Method

## V. CONCLUSIONS & FUTURE SCOPE

Some email applications, such as Outlook, employ a read-receipt tracking mechanism. The sender selects the receipt request option prior to sending the message, and then upon sending, each recipient has the option of notifying the sender that the message was received or read by the recipient.

However, requesting a receipt does not guarantee that you will get one, for several reasons. Not all email applications or services support read receipts, and users can generally disable the functionality if they so wish.

Email tracking is useful when the sender wants to know if the intended recipient actually received the email, or if they clicked the links. However, due to the nature of the technology, email tracking cannot be considered an absolutely accurate indicator that a message was opened or read by the recipient.

But this web portal help the user to identify that how many and which recipient read the send mail. With the help of this application marketing company/executives have exact figures to track open, click-through and conversion rates, making it simple to spot how a campaign can be improved.

Nowadays and in the future, application developers have to take into consideration the use of email tracing methods in order to efficiently implement their systems. In the future, application developers should consider using those methods for email tracing presented in this thesis, to implement their systems with full efficiency.

As the objective of the research is to provide an algorithm to solve the problem that the user has exact figures to track open, click-through and conversion rates, making it simple to spot how a campaign can be improved. The query string method successfully works in implementation of email tracing. The sender gets confirmation when the recipient read email. In future developer may improve the efficiency of algorithm by adding the feature that sender gets confirmation when recipient delete or forward the email.

## ACKNOWLEDGMENT

I would like to thanks my parents and my friends for their support and trust.

## REFERENCES

[1] Suzuki, S., Nakamura, M. "Domain Name System—Past, Present and Future", IEICE Transactions of Communication, E88b (3), pp. 857-864, 2005.

[2] Email Tracking homepage on Wikipedia. [Online]. Available: http://en.wikipedia.org/wiki/Email_tracking

 

[3] Nasir Muhammad, "Tracking and Identifying Individual Users in a Web Surfing Session".
[4] (2013) Cookie handling functions by Quirks mode Source.[Online].Available: http://www.quirksmode.org/js/cookies.html
[5] (2013) How You Can Be Tracked homepage on abine [Online].Available: http://www.abine.com/tracking.php
[6] J. N. Johnson & P. F. Dubois, "Issue Tracking", *Journal of Scientific Programming* IEEE pp.71-77, 2003.
[7] Duane Bachmann, John Elfrink & Gary Vazzana, "Tracking the Progress of E-Mail Vs. Snail-Mail", Vol. 8, No. 2,1996.
[8] Matthew G. Schultz, Eleazar Eskin & Erez Zadok, "MEF: Malicious Email Filter, a UNIX Mail Filter that Detects Malicious Windows Executables.
[9] Barry Leiba, Joel Ossher, V. T. Rajan, Richard Segal & Mark Wegman, "SMTP Path Analysis".
[10] Vladimir V. Riabov, "SMTP (Simple Mail Transfer Protocol)", May 12, 2005.

 