Opening the " Private Browsing " Data – Acquiring Evidence of Browsing Activities

Conference Paper · August 2014

CITATIONS
2

READS
5,692

5 authors, including:

Rodrigo Ruiz
Centro de Tecnologia da Informação Renato Archer
46 PUBLICATIONS **40** CITATIONS

SEE PROFILE

Opening the "Private Browsing" Data – Acquiring Evidence of Browsing Activities

Rodrigo de S. Ruiz [1], Fernando Pompeo Amatte, Kil Jin Brandini Park D. Sc. [3]
1 Malware Analysis Nucleus (NUCAM)
Renato Archer Information Technology Center(CTI)
Campinas – SP, Brazil.
2 Independent Researcher, Campinas – SP, Brazil.
3 Computer Faculty (FACOM) –Federal University of Uberlândia
Monte Carmelo – MG, Brazil
rodrigosruiz@outlook.com, famatte@gmail.com, kil@facom.ufu.br

Abstract — The growing concern of users about the confidentiality of data generated by web browsing activities made browser developers include options for safer and confidential browsing in their products.

For users those options, when functionally compliant with data security guidelines, guarantee online privacy. For law enforcement agents, this functionality introduces another obstacle for data acquisition towards evidence gathering.

No matter which case, it is important to assess and validate private browsing techniques.

The presented method shows that for some browsers it is possible to recover text and graphical data related to pages visited during private navigation, in clear violation of this tool basic functional requirement.

Keywords: Private browsing, Browser safety, Browser forensics.

1 INTRODUCTION

The growing concern of users with the confidentiality of the data generated by the activities developed in the course of navigation through web pages fostered the development of navigation options that offer greater degree of security and confidentiality of the data.

The promise of the developers regarding the operation of this feature is to prevent others to reconstruct the steps the user took during his online activities.

On Mozilla's page we found this commercial text about privacy and private browsing:

"Sometimes it's nice to go undercover: Open a private window and protect your browsing history. You can switch between private and normal windows quickly, so it's easy to go back to what you were doing before. This feature is great if you're doing your online banking on a shared computer or checking email from an Internet café." [1]

On Chrome's browser, when the user enable incognito mode, the new tab opened displays the following message:

"You came in incognito mode. Pages you view in this window will not appear in your browser history or search history will ***not leave other traces,*** *like cookies, on your computer after you close all incognito windows open. However, all the downloads you make or bookmarks you create will be preserved."*

On Safari's page we found this commercial text about privacy and private browsing:

"...Safari can keep your browsing history private. When you turn on Private Browsing, Safari does not remember the pages you visited, your search history, or your AutoFill information..."[2]

On IE's page we found this commercial text about privacy and private browsing:

"While you are surfing the web using InPrivate Browsing, Internet Explorer stores some information—such as cookies and temporary Internet files—so the webpages you visit will work correctly. However, at the end of your InPrivate Browsing session, this information is discarded..."[3]

On the one hand such a feature, if operating perfectly aligned with security guidelines, provides the user privacy in their online activities, on the other hand it is clear that in case of unlawful behavior, law enforcement officers have to deal with this layer of protection to obtain the necessary data to provide evidence during the course of an investigation.

In both cases, it is important to verify the actual functionality of such a feature, if available implementations actually provide the degree of confidentiality offered, or if there are flaws that allow the retrieval of online activity data.

This paper is an extended version of a work previously presented by the authors [4], with additional results and analysis, and is structured in the following topics:

Method and Tests, which presents the method applied to tests performed in various browsers with the private browsing feature enabled.

Results and Discussion, which presents the results obtained by the tests adopted and discusses these results.

Finally, follow the conclusions, further studies and references used.

2 METHOD AND TESTS

When testing a security feature, it is necessary to define its functional requirements and the profile of the attacker who will try to disable or override this feature.

In a paper on the analysis of private browsing functionality, [5] lists the profiles of potential attackers, security models to be checked and the objectives to be met by browsers that implement private browsing. In this work, we start from the methodological framework presented by [5], for the construction of the following methodological model:

The profile of the attacker considered assumes that he has local access to the user machine. Consequently, attempts to circumvent the system of private browsing will occur from an image taken from the user's machine hard drive.

As the focus of the evaluation is the private browsing feature, we considered that the user does not adopt other security tools or techniques that could exert influence on the access of the data generated during navigation. Thus, we did not conduct any test with the adoption of cryptographic methods in the disk of the user's machine.

Furthermore, this paper focus on searching the user's machine for fragments of data from which text or images that brings information about pages visited could be extracted. Therefore, the specific analysis of changes to files used by browsers such as history, cookies, cache and certificates was not performed. Such analysis can be found in [5] and [6].

We tested Internet Explorer browser on bare metal hardware with the use of four notebooks equipped with Windows 7 Pro SP1.

For the other tests performed, we created a standard guest virtual machine - with the operating system Windows 7 Pro - in the host operating system - Windows 7 Pro - using the virtualization software Virtual Box [7].

An export (snapshot) of the newly installed Windows machine was created, considering the possible need for future comparison of the base guest machine with guest machines running the different browsers tested.

The browsers tested were Internet Explorer 10, Firefox 24.0_1, Google Chrome 30.0.159969M_1 and Safari 5.1.7_1. The base guest virtual machine for each browser was replicated 4 times, each to be used in the four different tests performed on each browser.

Based on those configurations, four different tests for each browser in private browsing mode were applied:

Test S (Shutdown): Consists of visiting a web site available on the internet, making operations to interact with the site, finish the execution of the browser correctly and generating the virtual machine image for analysis.

Test F (Freeze): Consists of visiting a web site available on the Internet, making operations to interact with the site and with the browser still active, generating the virtual machine image for analysis.

Test K (Kill process): Consists of visiting a web site available on the internet, making operations to interact with the site, requesting that the operating system interrupt the browser execution and generating the virtual machine image for analysis.

Test P (Power down): Consists of visiting a web site available on the internet, making operations to interact with the site, requesting the virtualizer to turn off the virtual machine - simulating a power outage - generating the virtual machine image for analysis.

For each test performed, the virtual machine image generated will be analyzed through the application of the program strings [8] found in many different Linux distributions.

This program is used for the search of strings inside the virtual machine images that could present relation to the webpage visited.

The images of the virtual machines will be analyzed for the search of graphic files associated with the visited webpage, through the usage of the foremost program [9], a renowned forensic tool for extraction of files - "data carving" - of different formats.

This tool works as follows: It reads a block of data - memory, disk or files - and looks for signatures related to files of well-known formats. It is noteworthy that in the present research we investigated only the persistent memory (i.e. physical and virtual disk).

Since these signatures are a sequence of bytes, there is the chance of occurrence of false positives and therefore the capture of incorrect file.

Furthermore, it is important to note that there exist several known problems associated with the use of tools aiming for "data carving", for example, limitations to the treatment of non-contiguous data. Thus, it is possible that an image whose sequence of bytes is dispersed will not be fully recovered, despite its possible existence in the block of data analyzed.

The WinHex tool was also used to search for keywords found in the navigated webpage.

3 RESULTS

Aiming to simulate an actual visit to any website available on the internet, a random selection was made, and the site chosen for the experiment was the [10]. Since some site information is proprietary, the figures recovered during the test will be only partially reproduced in the present work. We would like to acknowledge that those information are copyright of their respective owners.

SAFARI Browser

For the Safari browser, the following results were obtained:

F test (freeze)

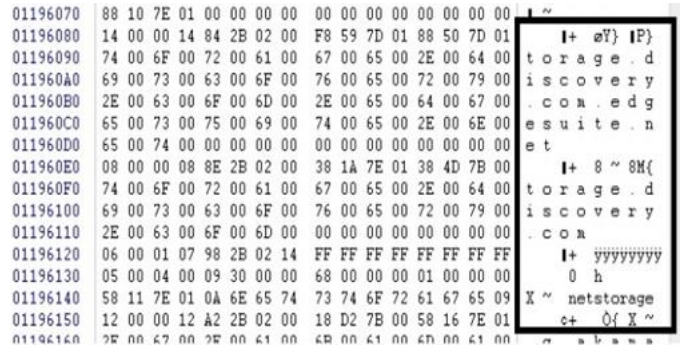

Figure 1- "storage.discovery.com" string located in virtual machine´s image.

No image fragments were found on the virtual machine´s hard disk image.

K Test (kill process)

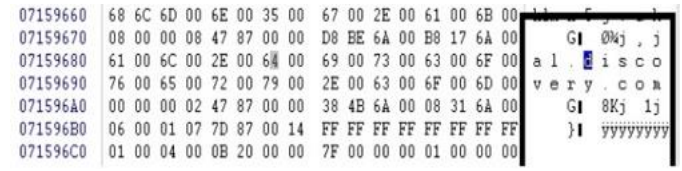

Figure 2- "discovery.com" string located in virtual machine´s image.

Images related to the webpage visited were found on the virtual machine hard disk image analysis:

Figure 3 – Image recovered on hard disk image analysis and found on Discovery.com website.

The strings utility could also recover text references in the virtual machine hard disk image analysis that indicated the webpage was visited:

p://dsc.discovery.com/videos

http://store.discovery.com/?ecid=PRF-DSC-101345&pa=PRF-DSC-101345

P Test (Power down)

Images related to the webpage visited were found on the virtual machine hard disk image analysis:

Figure 4 –Image recovered on hard disk image analysis and found on Discovery.com website.

The strings utility could also recover text references in the virtual machine hard disk image analysis that indicated the webpage was visited:

http://store.discovery.com/discovery/layout/favicon.ico
http://dsc.discovery.com/
http://games.dsc.discovery.com/
http://dsc.discovery.com/tv-shows
http://store.discovery.com/discovery/layout/favicon.ico

S Test (Shutdown)

Images related to the webpage visited were found on the virtual machine hard disk image analysis:

Figure 5 – Image recovered on hard disk image analysis and found on Discovery.com website.

The strings utility could also recover text references in the virtual machine hard disk image analysis that indicated the webpage was visited:

http://dsc.discovery.com/tv-shows
http://dsc.discovery.com/
http://store.discovery.com/discovery/layout/favicon.ico
http://dsc.discovery.com/videos
america.discovery.com.edgesuite.net
velocity.discovery.com
metrics.discovery.com
orate.discovery.com
animal.discovery.com.edgesuite.net

The results obtained for the Safari browser tests are grouped in table 1:

Table 1 – Results for Safari Browser

	F Test	K Test	P Test	S Test
Page address recover	Yes	Yes	Yes	Yes
Picture recover	No	Yes	Yes	Yes

FIREFOX browser:

F Test (freeze)

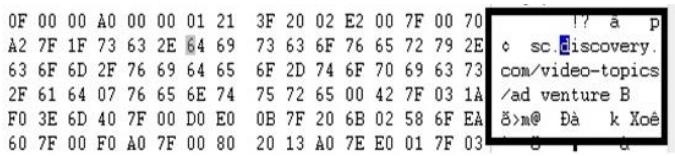

Figure 6 –"sc.discovery.com/video-topics" string located in the virtual machine´s image.

No images related to the webpage visited were found on the virtual machine hard disk image analysis.

K Test (kill process)

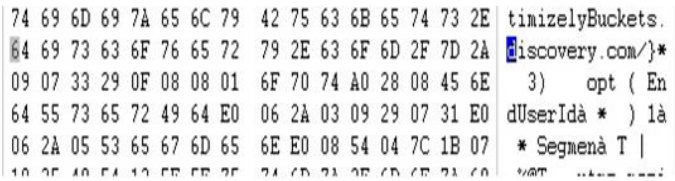

Figure 7 – "discovery.com" string located in the virtual machine´s image.

Images related to the webpage visited were found on the virtual machine hard disk image analysis:

Figure 8 – Image recovered on hard disk image analysis and found on Discovery.com website.

The strings utility could also recover text references in the virtual machine hard disk image analysis that indicated the webpage was visited:

C:\Program Files\Mozilla Firefox\firefox.exe
ttp://games.dsc.discovery.com/
/ttp://dsc.discovery.com/videos
http://games.dsc.discovery.com/word-games
http://games.dsc.discovery.com/sport-games
https://securestore.discovery.com/cart.php
https://securestore.discovery.com/cart.php
store.discovery.com
http://games.dsc.d

P Test (Power down)

Images related to the webpage visited were found on the virtual machine hard disk image analysis:

Figure 9 – Image recovered on hard disk image analysis and found on Discovery.com website.

The strings utility could also recover text references in the virtual machine hard disk image analysis that indicates the webpage was visited:

investigation.discovery.com.edgesuite.net
netstorage.discovery.com.edgesuite.net
netstorage.discovery.com
netstorage.discovery.com.edgesuite.net
netstorage.discovery.com.edgesuite.net
netstorage.discovery.com.edgesuite.net
games.dsc.discovery.com

S Test (Shutdown)

Images related to the webpage visited were found on the virtual machine hard disk image analysis:

Figure 10 – Image recovered on hard disk image analysis and found on Discovery.com website.

The strings utility could also recover text references in the virtual machine hard disk image analysis that indicated the webpage was visited. A fraction of strings retrieved in this test follows:

Fdsc.discovery.com%2Fvideo-topics%2Fadventure&u=oeu1381760545360r0.4355827774372748&wxhr=true&t=1381760579498&f=340937086

http://dsc.discovery.com/

h;e++)if(a[e].name=="keywords")if(b=="")b=a[e].content;else b+=", "+a[e].content;else if(a[e].name=="description")c=a[e].content;if(!(b.length+c.length>eb)){z("dmk",b);z("dmd",c)}}function ub(){var a="__cmb",b=[];for(var c in aa)c.indexOf(a)==0&&b.push(c
s_sess=%20s_cc%3Dtrue%3B%20s_campaign%3DPRF-DSC-101345%3B%20s_sq

Table 2 – Results for Fire Fox Browser

	F Test	K Test	P Test	S Test
Page address recover	Yes	Yes	Yes	Yes
Picture recover	No	Yes	Yes	Yes

GOOGLE CHROME Browser

F Test (freeze)

Some strings related to the webpage were also found in hard disk analysis:

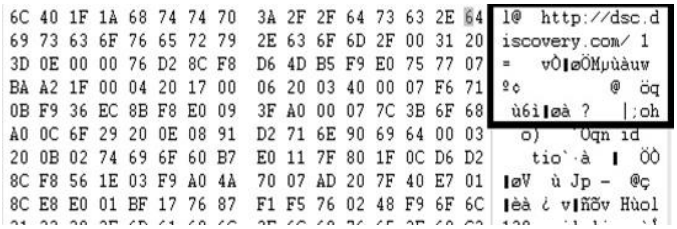

Figure 11- "http://dsc.discovery.com" string located in the virtual machine´s image.

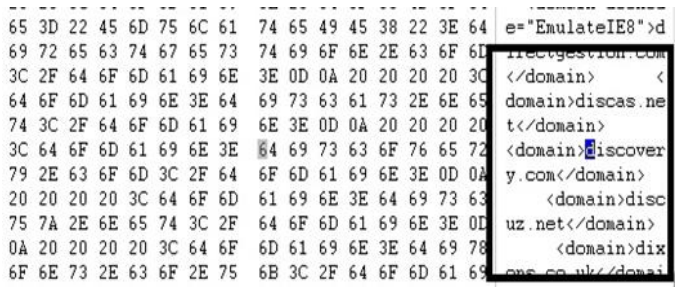

Figure 12- "discovery.com< /domain>" string located in the virtual machine´s image.

K Test (kill process)

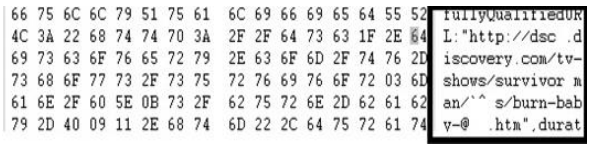

Figure 13 – "discovery.com/tv-shows" string located in the virtual machine´s image.

Images related to the webpage visited were found on the virtual machine hard disk image analysis:

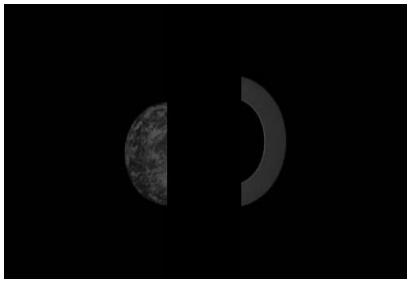

Figure 14 – Image recovered on hard disk image analysis and found on Discovery.com website.

Figure 15 – Image recovered on hard disk image analysis and found on Discovery.com website.

P Test (Power down)

Images related to the webpage visited were found on the virtual machine hard disk image analysis:

Figure 16 – Image recovered on hard disk image analysis and found on Discovery.com website.

The strings utility could also recover text references in the virtual machine hard disk image analysis that indicated the webpage was visited. A fraction of strings retrieved in this test follows:

//dsc.discovery.com/
://static.ak.facebook.com/connect/xd_arbiter.php?version=27#cb=fdde13148&domain=dsc.discovery.com&origin=http%3A%2F%2Fdsc.discovery.com%2Ff2a7e0cd34&relation=parent&error=unknown_user
/dsc.discovery.com/tv-shows
://dsc.discovery.com/
://dsc.discovery.com/
://dsc.discovery.com/
http://dsc.discovery.com/tv-shows
http://dsc.discovery.com/tv-shows
http://dsc.discovery.com/

S Test (Shutdonw)

Images related to the webpage visited were found on the virtual machine hard disk image analysis:

Figure 17 - Image recovered on hard disk image analysis and found on Discovery.com website.

The strings utility could also recover text references in the virtual machine hard disk image analysis that indicated the webpage was visited. A fraction of strings retrieved in this test follows:

":"Survivorman Videos","srtUrl":"","uuid":"8e18dcd9-8d1d-11e2-a7b7-06a90ff35868","bdat":"must watch","keywords":"survivorman,10 days,ten,days,must watch,mexico,tiburon,deserted,island,les stroud,survival,survivor,man,water,pool,algae,fresh,cane,reed,sludge","mediaType":"lift","mp4":[{"bitrate":"110k","src":"http://discsmil.edgesuite.net/digmed/hdnet/07/a7/13776400801197_102MissingPiece-110k.mp4"}f.akamaihd.net/i/digmed/hdnet/98/9a/13776401201197_104Stove-,400k,110k,200k,600k,800k,1500k,3500k,.mp4.csmil/master.m3u8","networkId":"DSC","thumbnailURL":"http://netstorage.discovery.com/feeds/brightcove/asset-thumbnails/dsc/0a5dbdfa893fec1f556a7d81c5b28bc470ecbb0e_0a5dbdfa893fec1f556a7d81c5b28bc470ecbb0e.jpg"

Table 3 – Results for Chrome Browser

	F Test	K Test	P Test	S Test
Page address recover	Yes	Yes	Yes	Yes
Picture recover	No	Yes	Yes	Yes

INTERNET EXPLORER Browser

F Test (freeze)

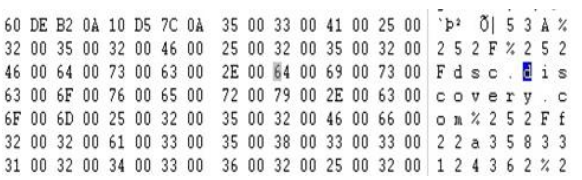

Figure 18 – "discovery.com" string located in the virtual machine´s image.

No images related to the webpage visited were found on the virtual machine hard disk image analysis.

K Test(kill process)

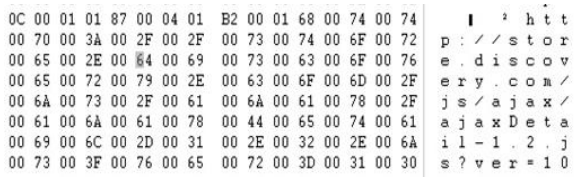

Figure 19– "http://store.discovery.com/js/ajax/" string located in the virtual machine´s image.

No images related to the webpage visited were found on the virtual machine hard disk image analysis.

P Test (Power down)

Images related to the webpage visited were found on the virtual machine hard disk image analysis:

Figure 20 – Image recovered on hard disk image analysis and found on Discovery.com website.

S Test (Shutdown)

On this test, another step taken was the analysis of log files generated by the Internet Explorer browser. It is easy to see that the page address is easily visible inside a log file:

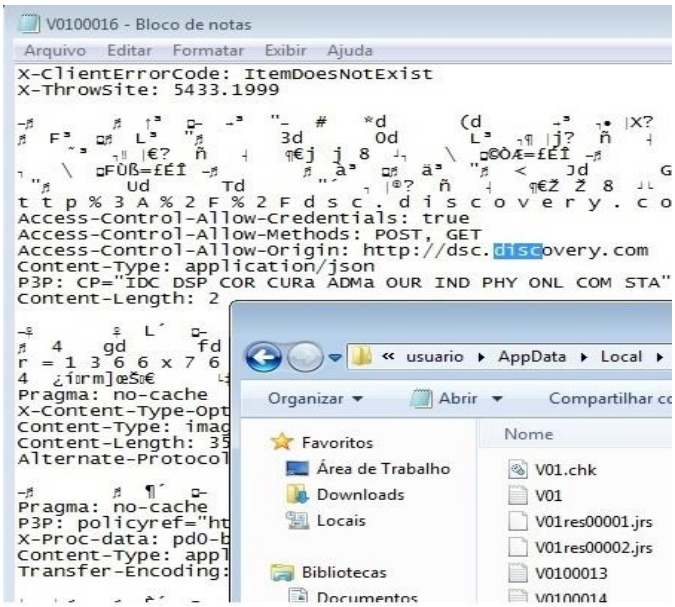

Figure 21 – Log file found using only the explorer and notepad. They demonstrate the system failure (string http://dsc.discovery.com found) in the private-IE10.

Table 4 – Results for IE10

	F Test	K Test	P Test	S Test
Page address recovery	Yes	Yes	No	Yes
Picture recovery	No	No	Yes	No

Further analysis to prospect the files and directories involved in the data leakage generated the following results:

In all browsers, some of the data associated with the navigation could be extracted from the file pagefile.sys. This proves that part of the data is leaking through the paging process´s storage mechanism used by the operating system.

In Internet Explorer´s case, more data could be found in a file located at the directory:

\user\<username>\appdata\local\microsoft\windows\temporary internet files\low\content.ie5\ndm4l4gv\

On Chrome´s case, more data could be found in the file:

\user\administrador\appdata\local\microsoft\windows\webcache\webcachev01.dat

Those files points to the fact that navigation data is leaking from cache files used by the browsers.

4 DISCUSSION

From the data generated by the tests, it is possible to assume that every implementation of the private browsing functionality in all browsers tested demonstrate some type of failure.

In some cases, those flaws allow an attacker to identify the pages visited by the user. In other cases, they generate enough data to allow the partial reconstruction of the pages visited.

We contact the developers about the results and obtained some mixed comments.

Microsoft answer to our request for comment:

"...We do encourage security researchers we are working with to present their research at events...
...The issue is still being scoped and researched. I will let you know once that has finished and a servicing decision has been made"

From the information about the private browsing functionality and the answers received, it is possible to extract that the average user is not well informed of the limitations inherent to the implementations of the service.

5 CONCLUSION

In all four types of tests performed, it is possible to verify that all browsers tested presented flaws in their private browsing feature.

Those flaws generates data that remains available in the system and allow not only the identification of pages visited but in some cases also to partially rebuild them.

Browsers promises to leave no traces of the navigation activities of users. This work proves that privacy as advertised is not provided.

In face of the results obtained, we would like to recommend the developers to explicitly alert the users about the limitations of the private browsing functionality implementation.

We would like to praise Microsoft´s answer because they both acknowledged the information received and approved the release of the study.

If on one hand this is a negative point for the user, on the other hand those flaws facilitate the work of law enforcers in cases where there is need for the data related to the navigation activity.

6 FURTHER STUDIES

In future researches, we plan to analyze the mechanisms and data structures - both browser and operating system related - involved in the browsing activities data leakage in-depth. This line of study could bring forth new techniques to avoid the problems presented in this paper on the implementations of the private browsing functions.

7 REFERENCES

[1] Mozilla private browsing. Available at: http://www.mozilla.org/en-US/firefox/features/ Accessed at: Oct, 24, 2013

[2] Archived - Mac Basics: Safari 5.1. Available at: http://support.apple.com/kb/ht4550. Accessed at: Nov, 21, 2013.

[3] What is InPrivate Browsing? Available at: http://windows.microsoft.com/en-us/windows7/what-is-inprivate-browsing. Accessed at: Nov, 21, 2013.

[4] RUIZ, R. S., AMATTE, F. P., PARK, K. J. B. Tornando Pública a Navegação "InPrivate". Prooceedings of the IcoFCS2012. Available at: http://www.icofcs.org/2012/ICoFCS2012_Full.pdf. Accessed at: Nov, 21, 2013.

[5] AGGARVAL, G. BURSZTEIN, E. JACKSON, C. BONEH, An Analysis of Private Browsing Modes in Modern Browsers. USENIX 2010, Available at: http://crypto.stanford.edu/~dabo/pubs/papers/privatebrowsing.pdf. Accessed at: Jun, 30, 2012.

[6] MAHENDRAKAR, A. IRVING, J. PATEL, S. Forensic Analysis of Private Browsing Mode in Popular Browsers. Available at: http://mocktest.net/paper.pdf. Accessed at: Jun, 301, 2012.

[7] VirtualBox tool. Available at: http://www.oracle.com/technetwork/server-storage/virtualbox/downloads/index.html. Accessed at: Jun, 13, 2013.

[8] Strings man page. Available at: http://linux.die.net/man/1/strings. Accessed at Jun, 30 2012.

[9] Foremost website. Available at: http://foremost.sourceforge.net/ Access at: Oct 14, 2012.

[10] Discovery.com website. Available at: http://dsc.discovery.com. Accessed at: Oct, 07, 2012.