Forensic Analysis of Private Browsing

Mary Geddes
De Montfort University
Leicester, UK

Dr Pooneh Bagheri Zadeh
De Montfort University
Leicester, UK

***Abstract*— Private browsing is popular for many users who wish to keep their internet usage hidden from other users on the same computer. This research examines what artefacts are left on the users' computer using digital forensic tools. The results from this research help inform recommendations for forensic analysts on ways to analyse private browsing artefacts..**

Keywords— Private browsing; Digital forensics; Acquisition; FTK Imager; RAM; Forensic investigation;

I. INTRODUCTION

Internet browsers advertise built in private browsing features to enable users to browse websites without their data being stored. This research will investigate artefacts left by a variety of Internet browsers and their private browsing from the perspective of a Forensic Investigator. The aim is to examine and investigate, using forensic tools, whether any artefacts are left on a user's system after private browsing has been used. Users choose private browsing over standard browsing because they believe that their internet history is not stored and they are able to browse anonymously. Private browsing artefacts are not left in the same places as other artefacts from standard browsing. For forensic investigators this means examining the entire computer to find artefacts left behind is vita.

II. BACKGROUND

The purpose of the private browsing feature is to allow reasonable users to browse the internet without information being stored on their local machine. However, private browsing appeals to criminals as it covers their tracks so it is necessary for Forensic Investigators to retrieve digital evidence from the internet browser used. This research will explore how various Internet browsers work to stop user data being collected and stored. Then by forensically analysing the system, the artefacts left behind will be highlighted using a range of forensic investigation toolkits, such as Encase, Forensic Toolkit (FTK) and Autopsy.

Private browsing modes are advertised by browsers to be used when secretly shopping for presents (Mozilla, 2015). Research into private browsing modes by Aggarwal, et al. (2010) proved this was not the case as most users preferred to use private browsing to browse to adult sites. Said, et al. (2011) investigated the effectiveness of private browsing modes and how to investigate whether the browsers have been used by criminals. From the experiments conducted it was clear to see that Internet Explorer performed the worst as evidence was found in physical memory and on the hard disk (Said, et al., 2011). However, the experiment only used a few keywords in search queries and a few URL's on a Windows XP machine. The lab conditions the experiments were conducted in have not been discussed so an assumption should be made that the results are not entirely accurate. Consequently, their research in 2011 is now outdated as the Windows XP operating systems they used is no longer supported by the modern web browsers.

Private browsers are a magnet for suspicious activity, as criminals believe that opening private browsing sessions will cover their tracks. When a suspect's machine is seized searching for artefacts left by any web browsing activity is a critical component for a digital forensic investigation (Oh, et al., 2011).

III. PRIVATE BROWSING

Background research has shown that there has been very little work done to analyse the latest versions of internet browser on a supported operating system, for example Said et al. (2011) presented his research on private browsing on a Windows XP machine. This paper will examine the following internet browsers on a Windows 7 Virtual Machine:

-Internet Explorer 11.0.0.1

-Google Chrome 47.0.2526.80

-Mozilla Firefox 42.0

-Safari 5.1.7

-Opera 34.0

The browsers will be used and artefacts created, the browser will then be closed and the data in the RAM will be collected. The Virtual Machine will be shut down and an image will be taken using FTK Imager.

IV. SOLUTIONS AND RECOMMENDATIONS

The research will be carried out in a forensic lab and on a virtual machine to ensure the data collected is accurate and not cross contaminated. A variety of keywords and URL are used to create enough artefacts. Encase and FTK are used to examine the images. This is a work in Progress paper and further results and recommendation on the types or artefacts remained on the system will be presented in the conference.

V. Future Research Directions

Further research needs to be done in newer operating systems such as Windows 8, 8.1 and 10. Analysis of artefacts left behind on Linux platforms, including OSX, needs to be carried out. Further research on analysis of mobile-based browsers in relation to private browsing in mobile devices is also under investigation.

References

Aggawal, G., Burzstein, E., Jackson, C. & Boneh, D., 2010. An Analysis of Private Browsing Modes in Modern Browsers. The 19th USENIX Symphosium on Security.

Mozilla, 2015. Private Browsing - Use Firefox without saving history | Firefox Help. [Online] Available at: https://support.mozilla.org/en-US/kb/private-browsing-use-firefox-without-history [Accessed 27 November 2015].

Oh, J., Lee, S. & Lee, S., 2011. Advanced evidence collection and analysis of web browser activity.

Said, H., Al Mutawa, N., Al Awadhi, I. & Guimareas, M., 2011. Forensic Analysis of Private Browsing Artifacts. 7th International Conference on Innovations in Information Technology.