NETWORK FORENSIC EVALUATION OF PRIVACY BROWSERS

Dr. Egho-Promise Ehigiator Iyobor (PhD, M.Sc., MBA, B.Sc., HND, DDP, EMCPM, CCNA, MCP)
Regional Technical Head
Glo Mobile Ghana Limited
Tamale, Northern Region
Ghana
eghopromise@yahoo.com

Isaac Quarshie
Software Developer
AdaptiveBIBO Innovations LLC
North Carolina, USA
youngquarshie@gmail.com

ABSTRACT
Web browsers are applications that are widely used by computer users to perform various activities such as downloading files, surfing the internet, using various social media programs, exchanging e-mails, and so on. Various cybercrimes are increasing every day, and users engaged in such malicious activities do not leave forensic artifacts. Networked web browser crimescene research is a key area of digital forensics and deals with web activities for all types of malicious users.

As users' interest in the privacy of data generated when they browse the web has increased, the developers of internet browsers have made it possible to browse the internet more securely and privately but this is a great disadvantage to the cyber forensics investigator because they will find it difficult to obtain digital data from visited websites in case any crime is committed. If internet browser engineersadhere to the recommendations in this study, cyber forensics investigator will be able to extract digital data from visited web sites. Tests were conducted on some selected browsers and feasible recommendations were made.

Keywords: private browsing, cyber forensics, computer forensic investigator

I. INTRODUCTION

Cyber forensics is a branch of computer science that deals with how to obtain, preserve, analyze, document and present digital data from cyber space. Cyber forensics investigator also refers to as cyber forensics analyst is a professional or expert who obtain digital data from cyberspace, perform analyses and documentations of the data. He ensures the integrity of the digital data is preserved to serve as evidence in the court of law in case cybercrime is committed.

The growing user interest in the confidentiality of data generated during website browsingactivities has facilitated the development of browsing capabilities that increase data security and confidentiality. The commitment of the developer to the operation of this feature, is to prevent other users from reconstructing the steps taken by the user during the browse network activities.

In Chrome, when the user enables incognito mode, the following message opens on a new tab. "**You are now in incognito mode. The page you view in this window does not appear in your browser history. Also, after opening all incognito windows, your search history will not leave other traces like cookies on your computer. However, all downloads and bookmarks are retained.** "

On the Mozilla page, the following commercial text about privacy and private search: "***You can quickly switch between private and regular windows so you can easily go back to your previous operations. This feature is perfect if you do internet banking on your shared computer or check email from internet cafes***. "

This commercial text on privacy and private search was found on the IE page: "***While you are surfing the web using In Private 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 the private browsing session, this information will be destroyed***".

On the other hand, these functions can provide users with privacy in network activities when running in full compliance with security guidelines. Meanwhile, with regard to violations, it is clear that law enforcement officials must deal with this level of protection in order to obtain the necessary information to provide evidence during the investigation.

In either case, if the available implementation provides the confidentiality that is actually needed, or there is a flaw that allows you to find data about network activities, check or activate the actual functionality of such features.

This study introduces an expanded version of the author's previous work (Satvat, Forshaw, Hao, Toreini, 2014).

1.1 Significance

The importance of this study is not only to obtain legal approval in the field of network forensics, but also for the benefit of society in ensuring that there is no network security violation.

At the same time, cybercrime continues to increase, and cyber fraudsters are becoming increasingly known in the process of avoiding the legal enforcement of identifiable evidence. This assessment aims to identify expected recyclable procedural artifacts that are critical to the legal prerequisites for advanced assessments to reveal hateful PC clues, for example, consistent with online stalking, cybercrime, or viewing and distributing juvenile entertainment content (NW3C, 2009).

It is important to identify expected process artifacts that can be recycled. In another review, authorities and cybersecurity awareness began convening a public forum on network security issues (double inspection). Internet browser engineers are already offering ways to privatize internet search. This study analyzed security cases created by web browser engineers for personal / private reviews and updated security features. Similarly, in a society that cannot be challenged and does not like security upgrades, would like to recognize whether private browsing is becoming more stringent on basic internet browsers which are the subject of curiosity about reusable programs. The degree of assurance is a vague technique of examination.

1.2 Scope

The study identified and addressed the three most commonly used Internet browsers: Google Chrome, Mozilla Firefox, and Internet Explorer. This study only investigated internet web browsers that were previously compatible with the Windows OS. Either way, at least some of the web browsers can work perfectly with other operating systems, such as Mac OS and Linux OS.

1.3 Objective

The objective of this research is to analyze the private mode browsing of the most commonly used internet browsers and determine whether traces of data can be retrieved or recovered from the user's computer after closing the browser.

II. REVIEW OF RELATED WORK

This section explores relevant materials related to internet security, internet browsers, advanced legal science equipment, computer science structures, and similar research systems.

Internet browser forensics has become an integral part of computer forensics exploration. Data collected through a web browser may be suspected in the case of ownership or illegal and explicit public entertainment, infringement of intellectual property rights or improper use of the internet connection in the waiver of terms of use (AUP).

Due to the rapid development of web innovation, crime research on web browsers is nothing new in the digital science of forensics. Web browsers have become versatile with certain releases of versions (Marrington, Baggili, Ismail, Kaf, 2012). This presents a challenge for advanced crime scene investigators who are committed to constantly investigating with different experiments in new web browsers on how to create forensically important artifacts for analysis.

Web browser privacy creates a private or secret mode, and criminals use this private mode feature to hide evidence of fraud. Several researchers are working on the privacy of different browsers. It helps forensic scientists discover artifacts of criminal activities in local systems. In a related study, Said and Noura Almutawa conducted an experiment to analyze the efficiencyof private mode browsing of mostly frequentlyutilized web browsers such as Mozilla Firefox, Internet Explorer, and GoogleChromeand to identify which of these browsers have been used for malicious and criminalmotives. During the experiments, Mozilla traces of data could not be found on Firefox and Google Chrome, except that Mozilla Firefox left certain traces of data in the pagefile.sys.During Internet Explorer analysis, the entire digital data on the drivewere scattered and full of evidence.

All three browsers (Said, Mutawa, Awadhi, Guimaraes, 2011) successfully revealed relevant information for private browsing sessions in local system RAM. As a result, Google Chrome was proven to be more secure while browsing private mode (Said. et.al, 2011).

Donny and Narasimha worked in private and portable modes in 2013, but their research was limited to Microsoft Windows 7 operating system and their outcome justified that information or data in private browsing mode of Firefox, Internet Explorer, and Google Chrome was retrieved from memory (Ohana, Shashidhar, 2013). In a study of portable browsers, Andrew Marrington analyzed the installed version of Chrome in “private” mode.

Their outcome showed that both versions left a lot of evidence on the hard drive which would be abundant for a digital investigator to rebuild browser activities. However, in their research their experiments were only performed on the Windows operating system without conducting RAM analysis (Marrington, et al., 2012) and also considering other Operating Systems.

Researchers (Aggarwal, Bursztein, Jackson, Boneh, 2010) also noted that most web browsers for some reasons failed in terms of their private browser policy due to browser extensions and add-ons. Additional work carried out by (Tunnicliffe, 2014) on the incognito modeof the three most popular browsers (Chrome, Firefox and Internet Explorer) by using open source too in which Internet Explorerbreached the privacy of incognito or private mode. To decide how incognito mode browsing affects digital research, theyfocused on the allocated space, unallocated space, and physical memory. After accomplishing the test, Internet Explorer successfully retrieved all traces from those locations, but Mozilla Firefox and Google Chrome successfully deleted the traces from the hard drive. But after a private browsing session, Google Chrome recovered some artifacts from RAM, as correlated to Mozilla Firefox. Therefore private browsing on Firefox will potentially frustrate cyber forensic investigators.

Further research on private mode forensics analysis for web browsers by Emad Sayed Noorulla. To test browser vendor claims, there were changes in file system and RAM during private browsing. Tests were conducted on the following browsers namely: Google Chrome, Internet Explorer, Firefox and Safari. As a result, it became clear that Firefox and Google Chrome did not leave any data in the file system. Safari left some artifacts in the "WebpageIcons.db" file. On the other hand, Internet Explorer wrote the data to drive and then deleted it. According to him, he worked on WindowsXP, 7 &8 OS and used various tools to extend his research to MAC OS and Ubuntu. However, in the case of RAM analysis, it was pointed out that the private search data was still found in the RAM in memory (Noorulla, 2014).

In 2015, R. Montasari and P. Peltola analyzed the performance of the most commonly used web browsers such as Safari, Chrome, Mozilla Firefox, and Internet Explorer. They discovered the reality of three web browsers, Mozilla Firefox, Apple safari and Internet explorer, which did not maintain sensitive browsing activities from local attackers. In contrast, experiments with Google Chrome conducted in private mode showedthat there was no trace on the local system. However,

these outcomes were inconsistent with the outcomes achieved by Mozilla Firefox completely (Tunnicliffe, 2014). However, Montasari and Peltola could not reveal the type of operating system these browsers were running on (Montasari, Peltola, 2015).

A lot of work has been done in the private mode of the web browser, but the focus of this study is to locatefragments of data on the user's computer to extract text or images to provide information about the visited page after the private browsing mode session expires.

III. METHODOLOGY

Experimenting any security characteristics, the functional requirements must be defined and the outline of the invader who tries to inactivate the features. The private browsing function analysis document (Aggarwal et al., 2010) shows the profile of potential attackers, the security model being tested, and the goals that the browser must achieve for private browsing. This article starts with the method framework he proposed (Aggarwal et al., 2010) to establish the following method model.

The attacker profile considered assumed that you have local access to the user's computer. As a result, attempts to bypass the private browsing system are the result of capturing images from the hard drive of the device user.

The purpose of this study is more related to private browsing, so users choose not to use any other security tools or methods, which can may affect access to data generated during web surfing.

In addition, this study focused on searching for data fragments on the user's machine and extracting text or images to provide information about the visited pagesafter the private browsing mode session expires.

Therefore, no specific analysis was performed on the file changes used by the browser (like cookies, history, cache, etc.). For such analysis, see (Aggarwal et al., 2010) and (Mahendrakar, Irving, Patel, 2012).

Tests were conducted using Oracle Virtual Box to create VM's to run the Windows 10operating system.

The tested browsers are Firefox, Internet Explorer and Google Chrome. The VM in each browser was cloned four times and used in four different tests performed in each browser. Based on these configurations, four different tests were performed on each browser in private browsing mode.

- **Freeze Test (Test F):** Visit a website accessible on the internet, interact with the website and the browser during the activity, and producethe VM image for examination.
- **Shutdown Test (Test S):** It includes visiting a website on the internet, interacting with it, successfully completing browser execution, and produce the VM image for examination.
- **Kill Process Test (Test K):** It visits a website available on the internet, takes certain measures to interact with the website, and causes the operating system to suspend browser execution and produce the VM image for examination.
- **Power down Test (Test P):** Visit sites available on the internet, perform site interaction operations, and request the virtualization device to shut down the VM-simulate a power outage-produce the VM image for examination.

For each test run, an array of programs found in many different Linux distributions were used to analyze the generated virtual machine (VM) image. This program is used to search the VM image for a string that can indicate a link to the visited website. Foremost softwarewas used to analyze the image of the VM and find the graphic files related to the webpage you visit. The foremost software is a well-known forensics tool used to extract files in various formats ("engraving data"). The operations of the toolincludes: read data blocks (memory, hard drive, files) to find signatures associated with files in known formats. It is worth noting that in this study, we only discussed persistent memory (physical and virtual drives). Because these signatures represent a series of bytes, they can cause false positive results and capture the wrong file. In addition, it is important to note

that there are known issues related to the use of "file carving "tools. For example, restrict the processing of incidental data. Although the bytes may be present in the analyzed data block, they are scattered and cannot be fully recovered.

The WinHex tool was also used to search for keywords found on web pages.

3.1 Tools and applications used

a. Winhex tool
b. Foremost Software
c. Oracle VM
d. Firefox, Chrome, Internet Explorer

3.2 How was the data collected?

Secondary data were used in the study and were collected from various archives.

IV. DATA ANALYSIS AND RESULTS

Selected cases were created to simulate verified website visits available on the Internet, and only few websites were selected for the experiments, because some of the information about thesewebsites unique, the numbers found during testing are only partially reproduced in our current study.

- **Mozilla Firefox browser:**

Freeze Test (Test F)

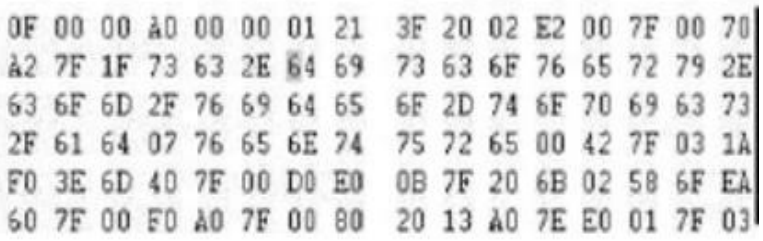

Figure1: A string in a VM image.

Image evaluation of the VM's hard drive did not find any images related to the web pages you accessed.

Kill Process Test (Test K)

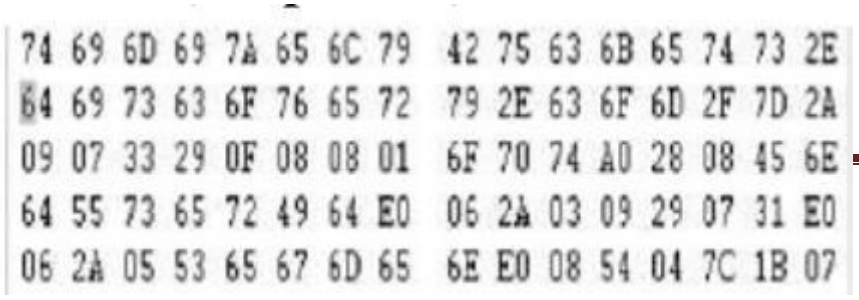

Figure 2: The series "google.com" in the image of the VM.

Images related to the websites accessed were found in the image analysis of the VM'shard drive:

Figure 3: Images returned by hard disk image analysis can be found at Discovery.com.

The page address which was retrieved by analyzing the image of the VM's hard drive can be found below.

https://www.google.com/search?q=random+image&client=firefox-bd&sxsrf=ALeKk01LHvH3xk9sH3GtOGbeVAMdGlITg:1596578509657&source=lnms&tbm=isch&sa=QiwAwiQbiAw6AwichAw6hWrwAhQwAwQrAwAwQwAhQrAWQwAQWQWAQAWQAQQAQAWQAQAQQAWQAWQAQAQQAWQAQAQAWQAQAQQAQAQAQAQAQAQAQAQQAQAQQAQA

Power down Test (Test P)

Images related to the websites accessed were found in the image analysis of the VM'shard drive:

Figure 4: The image was returned by analyzing hard drive images and found on google.com

The page address which was retrieved by analyzing the image of the VM's hard drive can be found below:

https://www.google.com/search?q=random+image&client=firefox-bd&sxsrf=ALeKk01LHvH3xk-9sH3GtOGbeVAMdGlITg:1596578509657&source=lnms&tbm=isch&sa=XAwQwAwQwiQAw6AwichQrAwQwAwQwAwQwAwQrAwWrAQQWQAWQAWQAQAQWQAQAWQAQAQAQAQAQAQQAWQAQAWQAQAQAQAQAQAQAQQAQAQAQAQAQAQQAQQAQA

Shutdown Test (Test S)

Images related to the websites accessed were found in the image analysis of the VM's hard drive:

Figure 5: The image was restored by analyzing the images on the hard drive and found on the fanpop.com website.

The page address which was retrieved by analyzing the image of the VM's hard drive can be found below:https://www.fanpop.com/clubs/animals/images/8676032/title/random-animals-photo

	Kill process Test	Freeze Test	Shutdown Test	Power down Test
Recover of Page Address	Yes	Yes	Yes	Yes
Recovery of Image	Yes	No	Yes	Yes

Table 1: Results of Mozilla Firefox

- **Google Chrome browser:**

Freeze Test (Test F)

Figure 6: Array in a VM image.

The image evaluation of the VM's hard drive did not find any images related to the web pages you accessed.

Kill Process Test (Test K)

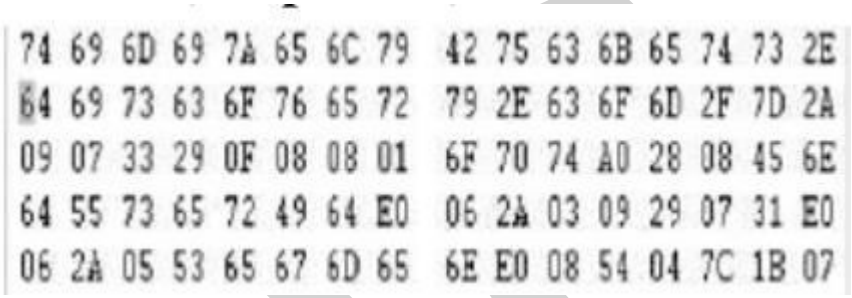

Figure 7: The "computerhope.com" strings within the VM image

Images related to the websites accessed were found in the image analysis of the VM's hard drive:

Figure 8: Images found on the computerhope.com website, and restored by analyzing hard drive images

The page address which was retrieved by analyzing the image of the VM's hard drive can be found below:
https://www.computerhope.com/jargon/r/random.htm

Power down Test (Test P)

Images related to the websites accessed were found in the image analysis of the VM'shard drive:

Figure 9: Images found on google.com, restored by analyzing hard drive images

The page address which was retrieved by analyzing the image of the VM's hard drive can be found below:https://www.gamasutra.com/view/news/320213/How_classic_games_make_smart_use_of_random_number_generation.php

Shutdown Test (Test S)

Images related to the websites accessed were found in the image analysis of the VM'shard drive:

Figure 10: Images on medicalnewstoday.com returned by hard disk image analysis.

Table 2: Google Chrome results

	Kill process Test	Freeze Test	Shutdown Test	Power down Test
Recover of Page Address	Yes	Yes	Yes	No
Recovery of Image	Yes	No	Yes	Yes

- **Internet Explorer browser:**

Freeze **Test (Test F)**

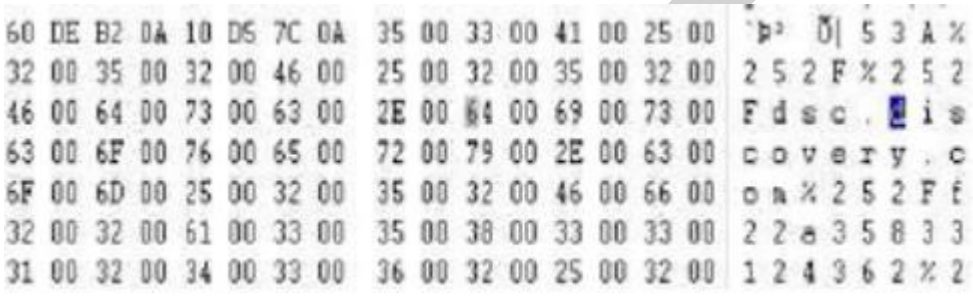

Fig11: Character string in the VM image.

The image evaluation of the VM's hard drive did not find any images related to the web pages you accessed.

Kill Process Test (Test K)

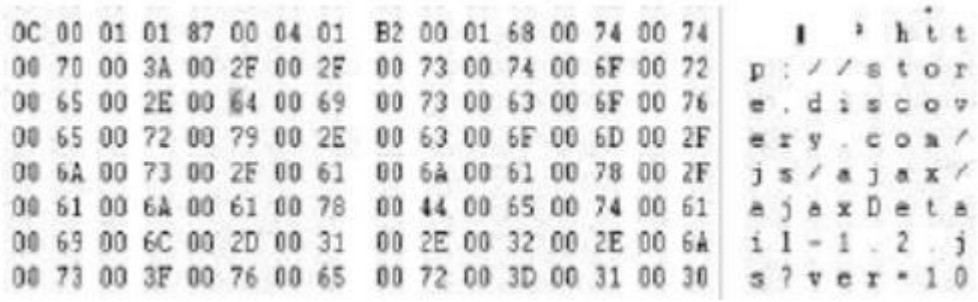

Figure 12: The "google.com" stringswithin the VM image.

Images related to the websites accessed were found in the image analysis of the VM'shard drive:

Figure 13: The image was restored by analyzing the hard disk images and found on unsplash.com.

The page address which was retrieved by analyzing the image of the VM's hard drive can be found below:https://unsplash.com/photos/ZJE5_qOaYxI

Power down Test (Test P)

Images related to the websites accessed were found in the image analysis of the VM's hard drive:

Figure 14: Images returned by hard disk image analysis were found at unsplash.com

The page address which was retrieved by analyzing the image of the VM's hard drive can be found below: https://unsplash.com/photos/-cDLLzxdYkM

Shutdown Test (Test S)

Images related to the accessed website could not be found in the VM hard drive image analysis:

The page address which was retrieved by analyzing the image of the VM's hard drive can be found below https://unsplash.com/photos/AHDeiqdiC7Q

	Kill process Test	Freeze Test	Shutdown Test	Power down Test
Recover of Page Address	Yes	Yes	Yes	Yes
Recovery of Image	Yes	No	No	Yes

Table 3: Internet Explorer Results

Further analysis to predict the files and folders involved in the data breach yielded the following results: In all browsers, some navigation data can be pulled out from the pagefile.sys file.

This proves that some data is leaked through the paging storage mechanism used by the operating system.

For Internet Explorer, you can find more information in files in a directory.

\ user \ <username> \ appdata \ local \ microsoft \ windows \ temporaryinternetfiles \ low \ content.ie5 \ ndm4l4gv \.

For Chrome, you'll find more information in the file.
\ User \ administrator \ AppData \ local \ Microsoft \ Windows \ WebCache \ webcachev01.dat.

These files indicate that the navigation data is missing files from the cache used by the browser.

V. DISCUSSION, CONCLUSION AND RECOMMENDATION

5.1 Discussion

Based on the results above, it can be concluded that all implementations of the private browsing security featureshave somevulnerabilities and this serves as a springboard for cyber forensics investigator to obtain digital data from visited websites.

5.2 Conclusion

From the results of the four tests conducted, it has been revealed that all the tested browsers have firm vulnerabilities in relation toincognito (private) browsing. These vulnerabilitiesgenerate usable data in the system and can not only identify the pages accessed, but can also incompletely update the pages.This is a disadvantage to the browser users, but on the other hand these vulnerabilitiesserve as great opportunity for the computer forensic investigators to obtain digital data from the visited sites in case any crime is committed.

5.3 Recommendation

It is recommended that the web browser engineers should not include security features in web browsers that will prevent computer forensics investigator from obtaining digital data from visited websites in case cybercrime is committed. If security features will hinder the investigator from obtaining digital data on the visited websites, investigator will not be able to present digital evidence in the court of law.

REFERENCES

1. Montasari. R &Peltola., P(2015). *Computer forensics analysis in private browsing mode. International Conference on Global Security, Safety and Sustainability.* pg. 96-109. Springer.
2. Ohana, D.J. and Shashidhar, N. (2013). *Do private and portable web browsers leave offensive evidence? Forensic analysis of backlogs from private and portable web browsing sessions.* EURASIP Journal for Information Security, (1): 1–13
3. Noorulla. S. (2014). *Forensic analysis of private web browser mode*. Master's thesis
4. Satvat, K., Forshaw, M., Hao, F. and Toreini E. (2014). *Forensic access to the privacy of browsing private pages. Data Privacy Management and Autonomous Voluntary Security*, 380 pg. 389, Springer
5. Marrington, A., Baggili, I., Ismail, A.T, & Kaf, A.A., (2012). *Web browser forensic browsers: a forensic study of the privacy benefits of portable web browsers*. Computer Systems and Industrial Informatics (ICCSII). pg. 1-6.
6. Said, H., Mutawa, A.H., Awadhi, A.I., Guimaraes, M. (2011).*Forensic analysis of private inspection artifacts*. Information Technology Innovation (IIT), International Conference 2011, pages 197-1202. IEEE,
7. Aggarwal, G., Bursztein, E., Jackson C., & Boneh, D. (2010). *Analysis of the way of private browsing of modern browsers*. USENIX Security Symposium, pg. 79-94.
8. *Mozilla private browsing*. Retrieved from:http://www.mozilla.org/en-US/firefox/features/(Accessed: August 7, 2020)
9. *Oracle Virtual box tool*. Retrieved from:https://www.oracle.com/technetwork/server-storage /VirtualBox / download / index.html(Accessed: 7 August 2020).
10. *Winhex Tool*. Get fromhttp://www.winhex.com/winhex/hex-editor.html (Accessed: 7 August 2020).
11. *Linux Strings*. Retrieved from https://linux.die.net/man/1/strings..(Accessed: 7 August 2020).
12. *Foremost.* Retrieved fromhttp://foremost.sourceforge.net/(Accessed: 7 August 2020).

13. Mahendrakar, A. Irving, J. &Patel, S.(2012).*In private browsing mode on popular browsers*. Available at http://mocktest.net/paper.pdf. (Accessed: 7 August 2020).