Received: 18 April 2020; **Revised:** 05 June 2020; **Accepted:** 05 June 2020; **Published:** 10 June 2020
Researchpedia Journal of Computing, Volume 1, Issue 1, Article 2, Pages 15-21, June 2020

Digital Object Identifier 10.1111/RpJC.2020.DOINumber

A Review of Web Browser Forensic Analysis Tools and Techniques

Aamir Rasool[1] and Zunera Jalil[2]
[1]Institute of Avionics and Aeronautics, Air University, Islamabad, Pakistan
[2]Department of Cyber Security, Air University, Islamabad, Pakistan

Corresponding author: Zunera Jalil (e-mail: zunera.jalil@mail.au.edu.pk).

ABSTRACT Browsers are essential to an active working environment but they also serve as the perfect cyber-attack vector. Cyber-attacks and crimes are multi-faceted in present era and having tendency to outgrow manifold. Digital forensic is a remarkable discipline to limit and investigate such threats by using its sophisticated tools. Web browser is the widely used application to access contents available on the internet and is user's face to the world. Typical browsing activities involve visiting web pages, accessing email accounts, using social media, uploading and downloading different files. User leaves digital footprints on computing device in the form of various artifacts while using browsers such as cookies, history, bookmarks, passwords, etc. These artifacts can be extracted through a specialized browser forensic toolkit to augment investigator's task. Researchers, in their previous work, have precisely focused towards specific mode of web-browsers' forensics and proposed viable investigative tools. In this study, accrued picture of all web-browsing modes (public, private and portable) has been crafted including potent forensic attributes for digital artifact's collection and comparative analysis of tools.

Keywords Browser forensics; artifacts; log files; Google chrome; live forensics; static acquisition.

I. INTRODUCTION

Web browser is an application required to access services provided over the web. According to a recent report, there were 4.39 billion internet users in 2019 [1]. Browser is a widely used application to access information available on the internet. Browsing activities involve accessing email, visiting web pages, online shopping, using social media, uploading and downloading files. Nexus was the first browser created by Tim Berners Lee in 1990 as W3C director [2].

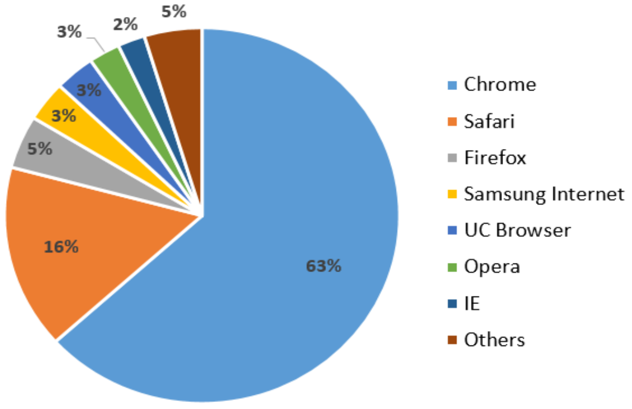


FIGURE 1. Market Share of web-browsers in terms of usage 2019 [3]

Some of the most popular browsers are Google Chrome, Firefox, Opera and Internet Explorer. Fig.1 shows market share of web-browsers in terms of usage in 2019 [3]. Different types of operating system are available in market, that have different hierarchy of storing data on disk of different applications. In 2019, trend for usage of operating system are given in Fig. 2.

During the process of accessing website, exchange of data occurs and some traces are left in computing devices. This information is stored in the form of cookies, cache files, searched terms, URL history, typed URL and session information. In most of the digital crimes, web browsers are important tools for crimes committed on digital devices. Artifacts left from use of web browser are key components for forensic examiners. Digital forensics investigation of web-browsers is executed to identify, collect and analyze the artifacts of distrustful activities of user. The suspect leave traces of their activities on computing device in different forms. It includes log files, slack spaces, registry, page files, etc.

The increase in cybercrimes that exploits network systems required enhanced information security management. Cybercrime includes theft of intellectual property, financial fraud, hacking, and damage of company service networks. Digital forensics appeared in response to rise in crimes done using computing devices. Digital Forensics refers to the process of identifying, preserving, analyzing and presenting digital evidence in court of law (if needed) [5].

To enhance privacy and anonymity of user, developers added private and portable modes of browsing. Onion Routing (OR) is one example of enhanced anonymity. Smart phones revolution produces edges for the human race and switch the planet into hand. Mobile web browsers are designed for use on mobile devices. Browsing internet on mobile devices creates immense potential for digital proof. As technology advances, it creates different challenges for the digital investigator.

Private mode of browsing, provides facility to avoid all traces of user's activity during a browsing session. History is not saved on the computing device. This makes analysis and access to location of evidence very difficult. As private mode doesn't store any web activity, but cannot stop operating system and routers to do so. Detection of this type of browsing is the most challenging task. If browser is opened, it is easy to detect private mode or incognito mode, but if browser is closed first it is ensured that if the private mode is turned on. Pagefile.sys file contains information related to private browsing, during swap process due to size of RAM available creates chances that may help to analyze.

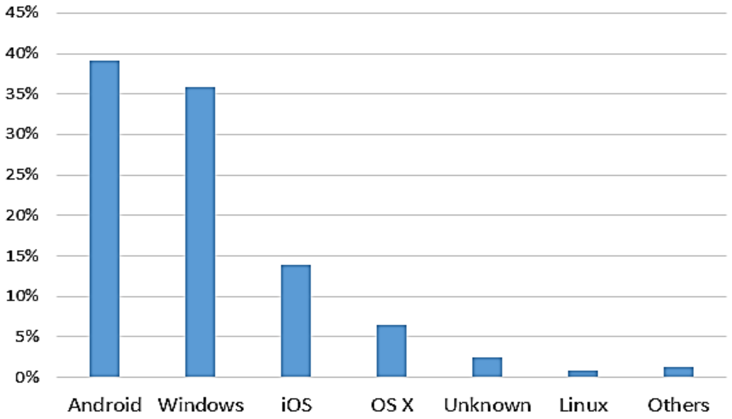


FIGURE 2. Operating system usage (in percentage) during 2019 [4]

In **portable mode** of web browser, browser is installed on removable media and launched from removable media. It stores data in the installed directory. The property defined that all traces of activities are removed when removable device ejected from computing device. As portable browser does not store traces in registry, so whole disk needs to be checked for the artifacts. Information available in RAM can be accessed by performing live memory forensics. This is another way of collecting artifacts. Detecting the user who used portable browser on the system is another challenging task.

World Wide Web represents a small piece of networked sites. It is estimated that 90% of internet is invisible or are using deep web [6]. Search engines like Google, are not able to recognize and reach to its data sites. It requires insider knowledge and a web browser like TOR. TOR browser uses Onion Routing (OR) to provide anonymity [7]. TOR is encrypted and virtual network; people used TOR browser to perform covert activities or to maintain anonymity during browsing the web. Due to this reason, it is difficult for law enforcement agencies and digital forensics experts to locate origin of traffic, location or proprietorship of any computing device. Accessing the leftovers of covert communication is a challenge.

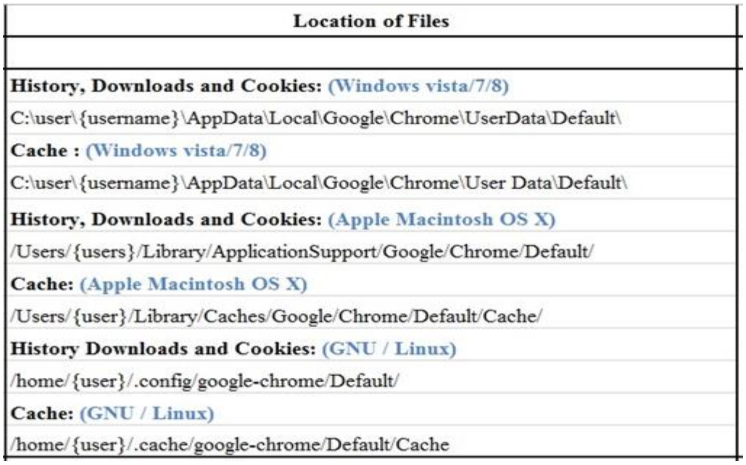
There are two types of digital data acquisition: (1) Static acquisition and (2) Live acquisition. In static acquisition, data is copied from powered off system whereas in live forensics, data is copied from system in running form. There are three methods of data acquisition: by making, bit-stream disk to image file, bit-stream disk to disk file and sparse data copy [8]. Many browsers now claim that their associated private mode browsing utility leaves no record on the device for forensics experts. Most popular web browsers also offer portable versions of browsers to be launched from removable device for user privacy.

The main contributions of this work are listed as follows:

- We have provided an insight about how browsers and operating system store information obtained from browsers in different working environment.
- Significant browser forensics tools are explored and feature wise comparison is presented.

- Best possible forensics approaches for digital artifacts created while browsing in normal, private and portable mode are discussed.

This paper is organized as follows: Section I contains details about web browsers usage and significance of different browsers for forensics investigations. In section II, literature review of browser forensic tools and research work in public, private and portable modes of browsing. Section III presents discussion on key findings and the last section concludes this discussion.



Location of Files
History, Downloads and Cookies: (Windows vista/7/8)
C:\user\{username}\AppData\Local\Google\Chrome\UserData\Default\
Cache : (Windows vista/7/8)
C:\user\{username}\AppData\Local\Google\Chrome\User Data\Default\
History, Downloads and Cookies: (Apple Macintosh OS X)
/Users/{users}/Library/ApplicationSupport/Google/Chrome/Default/
Cache: (Apple Macintosh OS X)
/Users/{user}/Library/Caches/Google/Chrome/Default/Cache/
History Downloads and Cookies: (GNU / Linux)
/home/{user}/.config/google-chrome/Default/
Cache: (GNU / Linux)
/home/{user}/.cache/google-chrome/Default/Cache

FIGURE 3. Default location of google chrome in various operating systems [10]

II. LITERATURE REVIEW

We analyzed forensic investigation tools available for web browsers and also explored research work done in this domain. Table I shows the detail of tools used for experiments that we reviewed in section III. Here, we briefly describe some of these tools.

Phrozen Browser Forensic [26] is a tool that creates a report for navigation history by keywords and make a matching with malicious words that allow security analyst a way to extract the information during a forensic analysis. It has multi browser support and works on Microsoft Internet Explorer, Google Chrome, Comodo, Dragon, Rock Melt as well as Opera. Default profiles include keywords such as LOIC, DDoS, anonymous, anonop, hack, malware, Zeus, spyey and more for analysis.

MyLastSearch [28] is a tool that scans the cache and history files of web browser. It locates all search queries that were made with the most popular search engines and with popular social networking sites. It also displays quires made during web browsing. It supports Internet Explorer and Mozilla Firefox browsers.

Chrome Cache View [31] is a tool that reads the cache folder of Google Chrome Web browser, and displays the list of all files currently stored in the cache. For each cache file, its displays URL, content type, file size, last accessed time, expiration time, server name and server response. This was designed for Google Chrome browser.

Internet Evidence Finder [32] is a tool by Magnet Axiom finds, analyzes and presents digital evidence found on computers, smartphones and tablets. It supports browsers forensics and can extract evidence from web apps such as chatting applications.

Web Historian [33] is a tool that collects web history, cookie history, file download history, and form history into data sets. Data displayed in grid view style with full search, sort, and filter capabilities. It has multi browser support; supports Internet Explorer, Mozilla Firefox, Opera and Safari.

In section A, general mode of browsing is discussed. In section B, portable mode and in section C, private mode of browsing is argued.

A. General Mode of Browsing

In 2016, Narmeen Shafqat [9], forensically analyzed Google Chrome in windows 8 environment. The results show file default locations listed in Fig. 3.

In [10], the author analyzes default location, history, login data, cookies, pre-fetch data, top sites and RAM dump to collect artifacts of Google Chrome on windows operating system. Google Chrome used for analysis, as market share of Google Chrome is 64.3% [3]. Valuable information is collected by analyzing google chrome using SQLite database viewer. Default location of history, Downloads, Cookies and cache in various operating system of google chrome is given in Fig. 3.

In 2018, author [11] proposes framework for web browser analysis using live forensics technique. Experiment is done using Google Chrome and Mozilla Firefox in private mode. It is shown that retrieving information about suspicious activities in private mode using live forensics is possible.

TABLE I. Comparative Analysis of Browser Forensic Tools

Tools Used	Functionality	Available for Windows	Available for Linux	License type
Phrozen Browser Forensics [26]	Perform search operations in web browser history	✓	×	Freeware
History Viewer [27]	Displays history of multiple web-browsers	✓	×	Freeware
MyLastSearch [28]	Display queries made during web-browsing	✓	×	Freeware
Chrome Cookie View [29]	View Google Chrome's cache	✓	×	Freeware
Chrome Password Decryptor [30]	Retrieve user name and password stored in Google chrome	✓	×	Freeware
Chrome Cache View [31]	Displays links stored in Google Chrome's cache	✓	×	Freeware
Internet Evidence Finder [32]	Recover and analyze digital proof	✓	×	Shareware
Web Historian [33]	Visualize browsing history of Google Chrome	-	-	Freeware [Educational Edition]
Belka Soft [34]	Data Acquisition Tool	✓	×	-
RAM Dump HXD [35]	Hexadecimal Editor	✓	×	Freeware
WEFA [36]	Collect and analyze browser's data	✓	×	Freeware
User Assist [37]	Displays list of programs executed on a Computer	✓	×	Freeware
Index.dat Analyser [38]	View, Examine and Delete contents of index.dat	✓	×	Freeware
Forensic toolkit (FTK) [39]	All in one digital forensics solution	✓	×	-
Win Hex [40]	Hexadecimal Editor	✓	×	Freeware
SQLite manager Firefox Add-on [41]	Manage, edit, manipulate, plot SQLite databases	-	-	Freeware
Autopsy [42]	Open Source digital forensics platform	✓	✓	Freeware

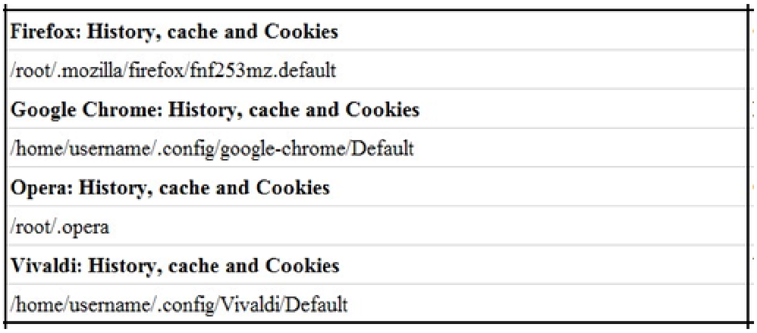
In 2019, Dinesh N. Patil [12], analyzed three types of activities: (1) Websites browsed (2) Emails send and receive (3) Upload and download of documents in Linux environment. In this study, he used Vivaldi, google chrome, Mozilla Firefox and opera web browser. Evidence collected and extracted from log files of afore-mentioned browsers. Default location of log files of used web-browsers is given in Fig. 4.

B. Portable Mode of Browsing

In another study, [13] Andrew Marrington et al., has highlighted the fact that not every commercial solution of portable devices is secured as they claim since they have observed traces left behind in the hard disk of the computer it has been used in.

In study [14], the authors have indicated information like file name, master volume information, and executable file name can be acquired from prefetch files. Divyesh G [15] has discovered that evidence can be obtained by windows registry and prefetch data. Two methods, live analysis and offline analysis are proposed for portable mode of browsing.

Apurva Nalawade et al. [16] has conducted a detailed analysis of different web browsers using different tools and technologies and has tabulated detailed results in the form of table giving insight information about traces left behind. Divyesh G et al. [17] conducted study about limitation of in-depth analysis of artifacts stored in local hard drive that included both live and offline modes. E.D. Adautin et al. [18] examined the remaining residual traces on Portable Google Chrome browser on Windows operating system.



Firefox: History, cache and Cookies
/root/.mozilla/firefox/fnf253mz.default
Google Chrome: History, cache and Cookies
/home/username/.config/google-chrome/Default
Opera: History, cache and Cookies
/root/.opera
Vivaldi: History, cache and Cookies
/home/username/.config/Vivaldi/Default

FIGURE 4. Web browser log file location in Linux File System [12]

C. Private Mode of Browsing

In [21], Rebecca Nelson used Google Chrome, Mozilla Firefox, their respective private modes, and TOR browser for study. The outcome of this study shows a lot of information is collected as evidence from Google Chrome and Mozilla Firefox. The main aspect of this study is, TOR browser's artifacts are also acquirable. Although less in amount, but still can be helpful in analysis.

In study [22], the inconsistencies between private browsing expectations and implementation has been highlighted where the study [23], on contrary, highlights the personal errors made by users while using such modes. In [24], study shows that given web browsers Mozilla Firefox, Internet Explorer and Apple Safari left artifacts in both common and uncommon locations on the hard drive. Huwida Said [25], it is possible to collect data from uncommon spaces i.e. physical memory (RAM) until the computer remains powered on. Firefox, Google chrome and Internet Explorer were used for the study.

III. DISCUSSION

This study was conducted to review the existing browser forensics tools and research efforts done in past in this domain. It is noticed that, Google chrome is mostly used for analyzing web-browser's artifacts due to its popularity mentioned in Fig.1 and generally Android OS & Windows environment used, because of its fame stated in Fig. 2.

Developers of web-browsers claimed, they enhance privacy by inducting modes (portable and private) than general mode. Despite their claim, they cannot stop operating system, router, switches and other devices from storing artifacts on the HDD. It is perceived that, artifacts always left on the devices. Although, magnitude of these artifacts varies with different mode of web-browser. But analyzing with different aspects can help in achieving a healthy amount of evidence.

Several artifacts of interest were found, e.g. browser history, cookies, and form autofill information in all general browsing sessions. These findings provided the baseline used for the investigation into several browsers' private sessions. When all browsers were compared to the Tor Browser Bundle, even those in private modes, presented more incriminating artifacts.

One significant forensics fact was also revealed is that when any forensic tool is run in both static and live analysis to acquire data, it may overwrite the data structure of previously running processes which can lead to inconsistency in evidence which are to be obtained for digital forensic analysis.

It is deemed that the traces of browsing will be deleted once the removable device is disconnected. For the artifacts detection in removable disk, the system can store artifacts at the registry and those artifacts contain many information about manufacturer name, connection time of removable disk, revision number, and product name.

Table I, shows the tools used in research papers that we reviewed in section II. Functionality of tools and their availability with respect to operating systems is also mentioned in table 1. There is a need to have a complete browser forensic solution with comprehensive features such as to extract browsing history, to dig searched keyword, to extract login credentials, cookies, to categorize user's behavior, to access intentional or unintentional stored files, to get plugins and add-on's information, to visualize cache and get bookmarks.

Browsers may be leaking our content during usage before an investigation even starts. The length of time a browsing session takes place may be forensically valuable which need to be analyzed as well. Hardware configurations also matter in browser forensics since each operating system will have its own memory caching processes and preceding volumes of leakage. Using virtual machine platform for web browsing adds another challenge for browser forensics with an additional layer which need to be addressed.

IV. CONCLUSION

In this paper, we have reviewed web browsers attributes in general, private and portable mode of browsing, limitations and associated tools. In the private browsing sessions of browsers, artifacts recovered were less significant than the public browsing sessions, validating several of the claims made by the producers of these programs. Whereas, TOR browser bundle did extremely well in minimizing the amount of information. Hence, the requirement is to use effective methodology with appropriate tool so that attacks can be noticed easily and alteration in memory contents can be minimized.

REFERENCES

[1] We Are Social. Digital 2019: Global Internet Use Accelerates - We Are Social. [online] Available at: https://wearesocial.com/blog/2019/01/digital-2019-global-internetuseaccelerates/ [Accessed 17 Jan. 2020].

[2] McPeak, A. (2020). A Brief History of Web Browsers and How They Work | CrossBrowserTesting.com. [online] CrossBrowserTesting.com. Available at: https://crossbrowsertesting.com/blog/testautomation/historyofwebbrowsers/ [Accessed 17 Jan. 2020].

[3] StatCounter Global Stats. (2020). Browser Market Share Worldwide | StatCounter Global Stats. [online] Available at: https://gs.statcounter.com/browser-market-share [Accessed 17 Jan. 2020].

[4] StatCounter Global Stats. (2020). Operating System Market Share Worldwide | StatCounter Global Stats. [online] Available at: https://gs.statcounter.com/os-market-share/ [Accessed 17 Jan. 2020].

[5] Infosecurityeurope.com. (2020). white Paper. [online] Available at:
https://www.infosecurityeurope.com/__novadocuments/83665?v=63 5652368156170000 [Accessed 26 Jan. 2020].

[6] TechCabal. (2015). 90% of the internet is hidden from your browser; and it's called the Deep Web | TechCabal. [online] Available at: https://techcabal.com/2015/11/18/90-of-the-internet-is-hidden-fromyour-browser-and-its-called-the-deep-web/ [Accessed 29 Jan. 2020].

[7] CompariTech (2019). What is Tor? How to use it safely and legally (plus 5 Tor alternatives). [online] Available at: https://www.comparitech.com/blog/vpn-privacy/ultimate-guide-to-tor/ [Accessed 4 June. 2020].

[8] Computer Forensics: Investigating Data and Image Files. (2009). 3rd ed. Cengage Learning, pp.2-18.

[9] Shafqat, N., 2016. Forensic investigation of user's web activity on Google Chrome using various forensic tools. IJCSNS Int. J. Comput. Sci. Netw. Secur, 16(9), pp.123-132.

[10] Rathod, D.M., 2017. Web browser forensics: google chrome. International Journal of Advanced Research in Computer Science, 8(7).

[11] Rusydi Umar, A.Y. and Faiz, M.N., 2018. Experimental analysis of web browser sessions using live forensics method. International Journal of Electrical and Computer Engineering (IJECE), 8(5), pp.2951-2958.

[12] Patil, D.N. and Meshram, B.B., 2019. Web Browser Analysis for Detecting User Activities. In Recent Findings in Intelligent Computing Techniques (pp. 279-291). Springer, Singapore.

[13] A. Marrington, I. Baggili, T. A. Ismail and A. A. Kaf, "Portable web browser forensics: A forensic examination of the privacy benefits of portable web browsers," 2012 International Conference on Computer Systems and Industrial Informatics, Sharjah, 2012, pp. 1-6.

[14] Choi JH., Lee K., Park J., Lee C., Lee S. (2012), "Analysis Framework to Detect Artifacts of Portable Web Browser". In: Park J., Kim J., Zou D., Lee Y. (eds) Information Technology Convergence, Secure and Trust Computing, and Data Management. Lecture Notes in Electrical Engineering, vol 180. Springer, Dordrecht.

[15] AR, Nagoor Meeran and others, "Forensic evidence collection by reconstruction of artifacts in portable web browser" International Journal of Computer Applications Volume 91 Number 4, 2014.

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

[17] Divyesh G, Nagoor A R. (2014). Forensic Evidence Collection by Reconstruction of Artifacts in Portable Web Browser. International Journal of Computer Applications. vol. 91, issue 4. (pp. 32-35).

[18] E. D. Adautin, "Forensic Reconstruction and Analysis of Residual

[19] Artifacts from Portable Web Browser," vol. 128, no. 18, pp. 19–24, 2015.

[20] D. J. Ohana and N. Shashidhar. Do private and portable web browsers leave incriminating evidence? a forensic analysis of residual artifacts from private and portable web browsing sessions. IEEE SPW '12, 2012.

[21] Tri Rochmadi, Imam Riadi and Yudi Prayudi. Live Forensics for Anti-Forensics Analysis on Private Portable Web Browser. International Journal of Computer Applications 164(8):31-37, April 2017.

[22] Nelson, R., Shukla, A. and Smith, C., 2020. Web Browser Forensics in Google Chrome, Mozilla Firefox, and the Tor Browser Bundle. In Digital Forensic Education (pp. 219-241). Springer, Cham. [21] G. Aggarwal, E. Bursztein, C. Jackson, and D. Boneh, "An analysis ofprivate browsing modes in modern browsers," In Proc. Of 19th Usenix Security Symposium, 2010.

[23] C. Soghoian, "Why private browsing modes do not deliver real privacy," Center for Applied Cybersecurity Research, 2011.

[24] Montasari, R. and Peltola, P., 2015, September. Computer forensic analysis of private browsing modes. In International Conference on Global Security, Safety, and Sustainability (pp. 96-109). Springer, Cham.

[25] Said, H., Al Mutawa, N., Al Awadhi, I. and Guimaraes, M., 2011, April. Forensic analysis of private browsing artifacts. In 2011 International Conference on Innovations in Information Technology (pp. 197-202). IEEE.

[26] SoftPedia. (2014). Browser Forensic Tool. [online] Available at: https://www.softpedia.com/get/Internet/Other-Internet-Related/Browser-Forensic-Tool.shtml [Accessed 27 Jan. 2020].

[27] Historyviewer.net. (2013). Download History Viewer for free. [online] Available at: http://www.historyviewer.net/download.htm [Accessed 27 Jan. 2020].

[28] NirSoft. (2015). MyLastSearch: View your search engine query in Google and others. Available at: https://www.nirsoft.net/utils/my_last_search.html [Accessed 27 Jan. 2020].

[29] NirSoft. (n.d.). View / delete cookies of Chrome Web browser. Available at: https://www.nirsoft.net/utils/chrome_cookies_view.html [Accessed 28 Jan. 2020].

[30] softpedia.com. (2019). Chrome Password Decryptor. Available at: https://www.softpedia.com/get/Security/DecryptingDecoding/ChromePasswordDecryptor.shtml [Accessed 28 Jan. 2020].

[31] softpedia.com. (2020). ChromeCacheView. [online] Available at: https://www.softpedia.com/get/Internet/Other-Internet-Related/ChromeCacheView.shtml [Accessed 28 Jan. 2020].

[32] Magnet Forensics. (2014). Magnet Forensics Releases Internet Evidence Finder v6.4 - Magnet Forensics. [Online] Available at: https://www.magnetforensics.com/news/magnet-forensics-releasesinternet-evidence-finder-v6-4/ [Accessed 28 Jan. 2020].

[33] Menchen-Trevino, E. (n.d.). Educators and individuals - Web Historian. [online] Web Historian. Available at: https://www.webhistorian.org/education/ [Accessed 28 Jan. 2020].

[34] Belkasoft.com. (n.d.). Belkasoft Acquisition Tool. [online] Available at: https://belkasoft.com/bat [Accessed 28 Jan. 2020].

[35] Hörz, M. (2019). Downloads | mh-nexus. [online] Mh-nexus.de. Available at: https://mhnexus.de/en/downloads.php?product=HxD20 [Accessed 28 Jan. 2020].

[36] Forensic.korea.ac.kr. (2019). DFRC - Digital Forensic Research Center. [online] Available at: http://forensic.korea.ac.kr/tools.html [Accessed 28 Jan. 2020].

[37] Didier Stevens. (n.d.). UserAssist. [online] Available at: https://blog.didierstevens.com/programs/userassist/ [Accessed 28 Jan. 2020].

[38] Systenance.com. (n.d.). Systenance Software - Index.dat Analyzer. [online] Available at: http://www.systenance.com/indexdat.php [Accessed 28 Jan. 2020].

[39] AccessData. (2019). Forensic Toolkit (FTK) version 7.1.0. [online] Available at: https://accessdata.com/product-download/forensictoolkit-ftk-version-7.1.0 [Accessed 28 Jan. 2020].

[40] AG, X. (2019). WinHex: Hex Editor & Disk Editor, Computer Forensics & Data Recovery Software. [online] X-ways.net. Available at: https://www.x-ways.net/winhex/ [Accessed 28 Jan. 2020].

[41] Addons.mozilla.org. (2019). SQLite Manager – Get this Extension for Firefox (en-US). [online] Available at: https://addons.mozilla.org/en-US/firefox/addon/sqlite-managerwebext/ [Accessed 28 Jan. 2020].

[42] Autopsy. (n.d.). Autopsy | Download. [online] Available at: https://www.autopsy.com/download/ [Accessed 28 Jan. 2020].

AAMIR RASOOL received his B.Sc. and M.Sc. degree in Computer Science from University of Sindh, Jamshoro, Pakistan, in 1992 and 1994 respectively. He later earned his M.Sc. War Studies degree program in National Defense University, Islamabad, Pakistan in 2016. He is currently the student of MS in Information Security at Air University, Islamabad and is working in the domain of cyber security and digital forensics. His current research interests include but are not limited to computer forensics, cloud computing security, artificial intelligence and cyber security governance.

ZUNERA JALIL received the B.Sc. degree from Punjab University, Lahore, Pakistan, in 1999, and then Masters degree in computer science from International Islamic University, Islamabad, Pakistan. She later earned scholarship from Higher Education Commission of Pakistan to pursue M.S. degree in computer science and then Ph.D. degree in computer science with information security specialization from the FAST National University of Computer and Emerging Sciences, Islamabad, Pakistan, in 2007 and 2010, respectively. She served at International Islamic University, Islamabad, Iqra University, Islamabad and then Saudi Electronic University, Riyadh, Saudi Arabia. She is currently with the Department of Cyber Security and is involved with National Cybercrimes and Forensics Laboratory, Air University, Islamabad, Pakistan. Her current research interests include but are not limited to computer forensics, intelligent systems, and data privacy protection.