International Journal of Digital Crime and Forensics
Volume 16 • Issue 1 • January-December 2024

Examining the Behavior of Web Browsers Using Popular Forensic Tools

Emad Ul Haq Qazi
https://orcid.org/0000-0003-1448-3632
Naif Arab University for Security Sciences, Saudi Arabia

Tanveer Zia
https://orcid.org/0000-0003-3802-5687
Naif Arab University for Security Sciences, Saudi Arabia

Areej Muqbil Alotibi
Naif Arab University for Security Sciences, Saudi Arabia

Salem Yahya Altaleedi
Naif Arab University for Security Sciences, Saudi Arabia

ABSTRACT

Mobile phones and computers are widely used devices these days, with almost everyone carrying a smartphone and multiple personal computing devices at their homes. Unfortunately, the perpetrator exploits these devices for their unlawful activities. They employ various tactics such as sending phishing emails, and malicious links to harvest confidential information and exploit users. The perpetrators often leave traces on search engines, where they search for illegal materials and weapons, or send threatening emails to victims. This paper primarily focuses on locating and retrieving browsers' artifacts while considering the challenges posed by private browsing modes, which perpetrator may use to cover their tracks. The study also compares well-known search engines like Edge, Safari, and Firefox, analyzing the strengths and weaknesses of their directories. Moreover, it explores evidence extraction from smartphones, comparing the success rates between rooted or jailbroken phones and evidence obtained from browsers versus applications.

KEYWORDS

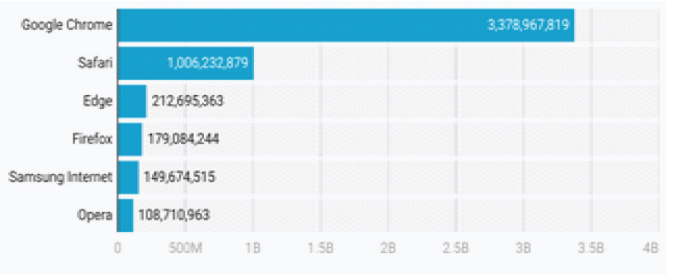
Browser Artifacts, Browser Normal Mode Analysis, Digital Investigations, Edge Analysis, Firefox Analysis, Safari Analysis, Web Browsers Forensics

Web browsers enable users to explore the internet and navigate various websites and web pages by establishing communication with web servers. These browsers store a significant amount of information, including usernames, passwords, web history, and temporary internet files. As a result, ensuring web browser security has always been a key objective for providers, as it is a crucial aspect of any online service. Understandably, users are constantly seeking the most effective tools to protect their data, creating an ongoing and evolving process of updates and patches to enhance and address any vulnerabilities in browsers. Currently, most web browsers offer different modes, such as the regular/normal browsing mode and the private/incognito mode, to enhance user privacy. The concept of private mode refers to a browsing mode in which no record of visited websites is retained.

This endeavor to provide a secure environment for everyone is commendable. However, like any other technology, web browsers can be misused as tools for committing cybercrimes. Criminals also exploit browsers and private modes to carry out illicit activities and conceal their actions. It is important

DOI: 10.4018/IJDCF.349218

Figure 1. Browser statistics



to note that these privacy features, such as private/incognito mode, present technical challenges for digital forensics investigators when attempting to recover evidence in cases involving criminals who utilize private browsing [20, 21]]. Furthermore, criminals constantly employ various methods to hide their activities while using private mode, including deleting or modifying their online actions.

Previous research in web browser forensics has often overlooked the variable effectiveness of forensic tools across different browser types and modes. This study addresses these gaps by providing a comprehensive analysis of how various tools perform across multiple browsers, shedding light on previously unexplored facets of browser forensics. This study's objective is to establish a standardized methodology for examining and verifying the claimed level of privacy provided by different browser vendors. Additionally, it aims to determine the extent to which forensic investigations can uncover relevant evidence artifacts of evidentiary importance.

METHODOLOGY

The methodology employed in this research is meticulously designed to systematically evaluate the forensic capabilities of selected web browsers. This involves the use of standard forensic tools to analyze browser artifacts under controlled conditions. The selection of browsers and tools is based on their prevalence in the industry and relevance to forensic investigations, ensuring that the findings are applicable to real-world scenarios.

Selection of Web Browsers

In this study, we selected three popular web browsers: Mozilla Firefox [1], Safari, and Microsoft Edge. These browsers were chosen due to their significant market share and frequent usage across various platforms. Google Chrome has already been thoroughly examined in normal and incognito modes [19]. Figure 1 shows the statistics about the browsers.

According to Firefox statistics for 2022, the browser has approximately 362 million users worldwide. Apple's Safari [2] is regarded as the safest browser, with only 26 vulnerabilities discovered in 2022. Microsoft Edge is Microsoft's recommended web browser and the default web browser for Windows; Windows supports web-platform-based applications.

Forensic Tools

To analyze the behavior of web browsers, we utilized industry-standard forensic tools, including Autopsy, AXIOM, and XRY. These tools enable the extraction and analysis of browser artifacts, allowing for a comprehensive investigation. We employed Autopsy for in-depth examination of computer images, supporting functionalities like keyword search, hash matching, and registry analysis. AXIOM was utilized for its superior capabilities in uncovering challenging digital evidence and integrating data from different sources into a single case file. Additionally, XRY was chosen for its