ABSTRACT

Browser technology and the need for privacy have led to the widespread use of private or incognito browsers. This mode can help users maintain their privacy by not storing browsing history and other data. However, private browsers are also often used as an anti-forensic method to remove digital evidence of online activities. Therefore, it is important to analyze the effects of using private browsers that may complicate digital forensic investigations. This research aims to investigate to what extent residual data can be collected when private browsers are used as a method of trace obfuscation. Firefox and Chrome web browsers were applied as case studies with simulated activities of online gambling scenarios created. Memory analysis was used as a forensic acquisition technique, while browser history extraction was performed to demonstrate the limitations of data collection in a private browser environment. The results of memory analysis showed that key artifacts such as Username, Email, Keywords, URL, and Games played were successfully recovered, except for location. Due to the changing IP addresses and the use of proxies, more knowledge, experience, and support from various parties are needed to deal with this to obtain comprehensive information. This research provides new insights into the importance of understanding the impact of using private browsers as an anti-forensic method in digital forensics.

Keywords : Forensics Browser, Private browser, anti forensic, privacy.