CC Cleaner Tool Analysis

Contents

[Introduction 3](#_Toc43296919)

[Methodology 3](#_Toc43296920)

[The Control Examination 4](#_Toc43296921)

[Running CCleaner 6](#_Toc43296922)

[The Experimental Examination 9](#_Toc43296923)

[Conclusions 12](#_Toc43296924)

# Introduction

CCleaner is a tool published by Piriform Ltd. It is one of several tools that they have released aimed at the average desktop consumer. Along with CCleaner they have released Defraggler, a hard drive defragging utility, Speccy, to analyze a computer’s hardware components and Recuva, a consumer grade file recovery tool. CCleaner claims to improve the privacy and efficiency of a windows PC by deleting browser artifacts, automatically deleting and modifying settings to improve efficiency, and giving people the ability to limit what programs boot on startup. It is its ability to remove browser artifacts automatically that I am the most interested in. In many forensic investigations, browser artifacts can be some of the most important components of the case. Seeing what sites have been visited, when they were visited, and other key information about the user’s browsing history can aid researchers in constructing a timeline. If CCleaner is able to significantly disrupt the number of artifacts that can be found after it has been run, that would make it a tool worth considering in the anti-forensics arsenal.

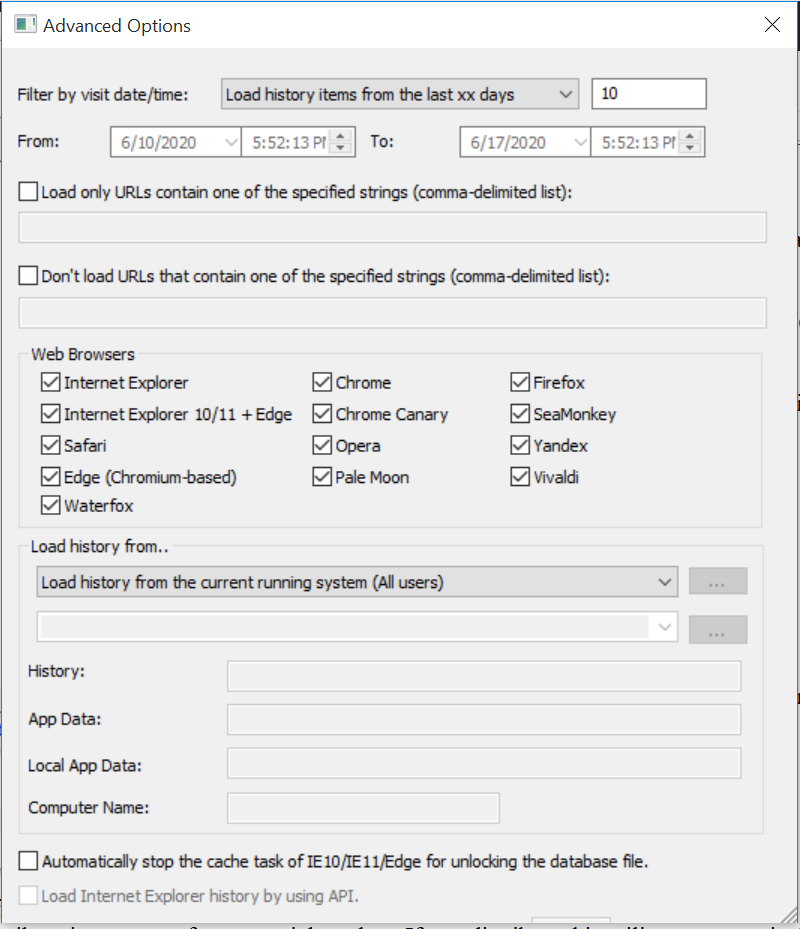
# Methodology

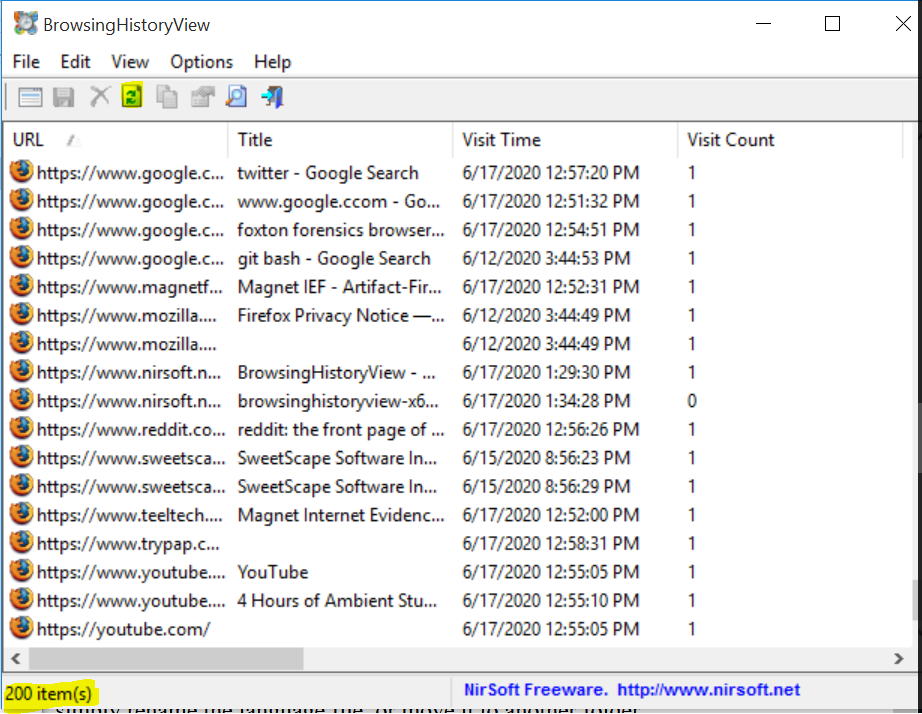
As I am attempting to examine the efficacy of this tool rather than the mere operating procedure as I had been for the other tools in this evaluation. I will be copying the methodology used in a Magnet Forensics test of the tool. You can find this analysis, and their results, by clicking [here](https://www.magnetforensics.com/resources/oh-no-the-suspect-ran-ccleaner-to-get-rid-of-the-evidence/).

The basics are as follows. I installed CCleaner by browsing to its download page which you can visit by clicking [here](https://www.ccleaner.com/ccleaner). I followed all the default installation steps, excepting I did not also install Google Chrome as I would be performing most of my web browsing on Firefox. With the tool downloaded and installed, I generated some web history by browsing to some common popular websites, as well as making use of “theuselessweb.com” to rapidly fill my web history with a variety of different pages. I have also downloaded and installed Nirsoft’s BrowsingHistoryView. BrowsingHistoryView is a great, free forensic tool that I have used as a part of my classes at Champlain College to examine web history. I will run it on my system and document the results to see how many artifacts exist as a control. I will then run CCleaner, restart the Virtual Machine, and again run BrowsingHistoryView and compare the results.

# The Control Examination

To begin this process, I ran a control examination of the browser history using BrowsingHistoryView. I began by launching the application, which immediately displayed a “Advanced Options” dialog prompt upon launching. This allowed me to specify whether I was targeting specific URLs, what the time-frame of the investigation was, and what browsers I wanted to have history pulled from. As per the methodology outlined in Magnet Forensics own experiment, I left all these settings to their default value, which you can view in figure one.

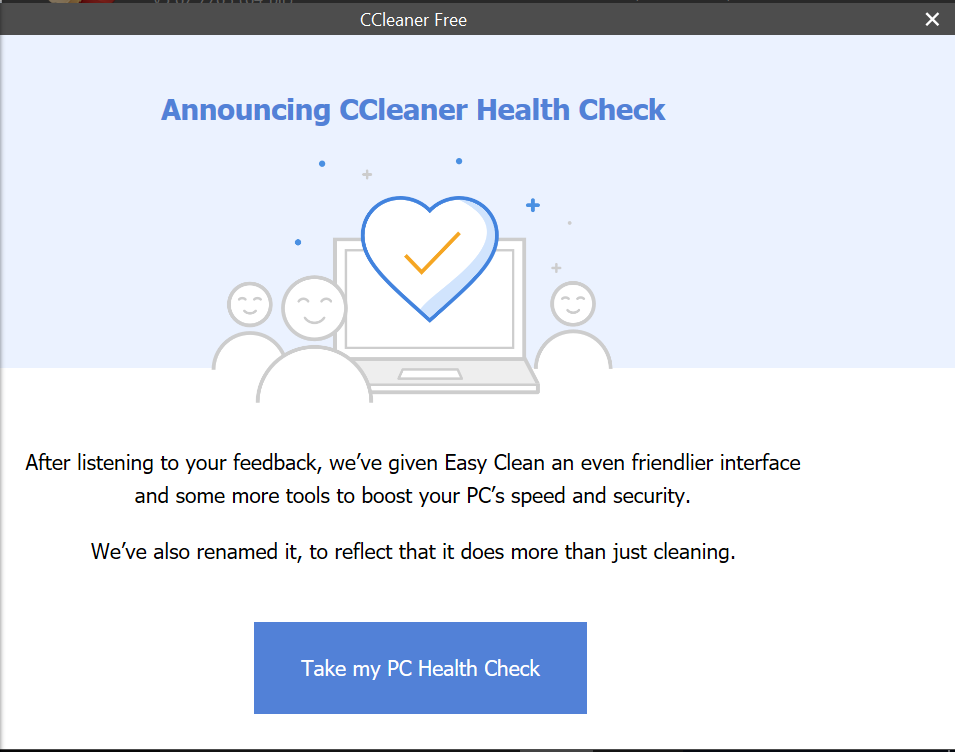
*Fig.1. Default Settings For BrowsingHistoryView*

I simply closed this window to confirm my settings. I was then presented with the main window of BrowsingHistoryView, devoid of any results. I then ran the tool for the first time by clicking the “Refresh” button located in the upper left-hand corner of the tool and highlighted in figure 2. This automatically captured all the web artifacts the tool was able to find, which came out to 200 items in total. This represented a capturing of all the web traffic that I had generated for my browser as part of the test.

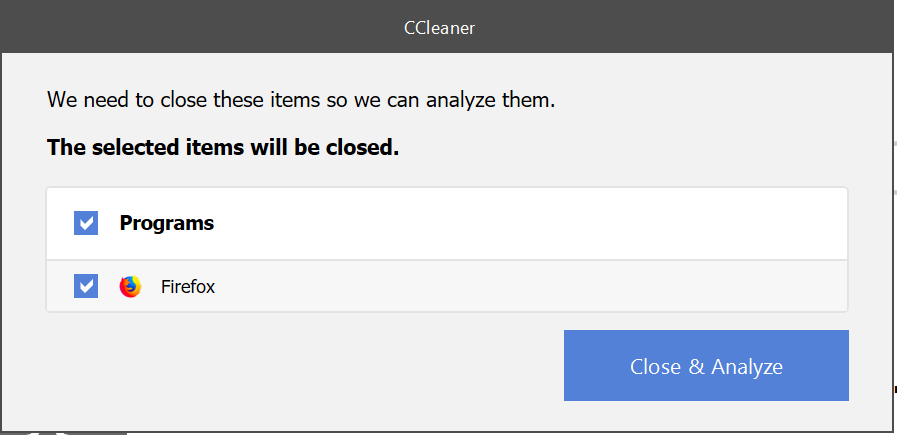
*Fig. 2. BrowsingHistoryView’s state after the control run.*

# Running CCleaner

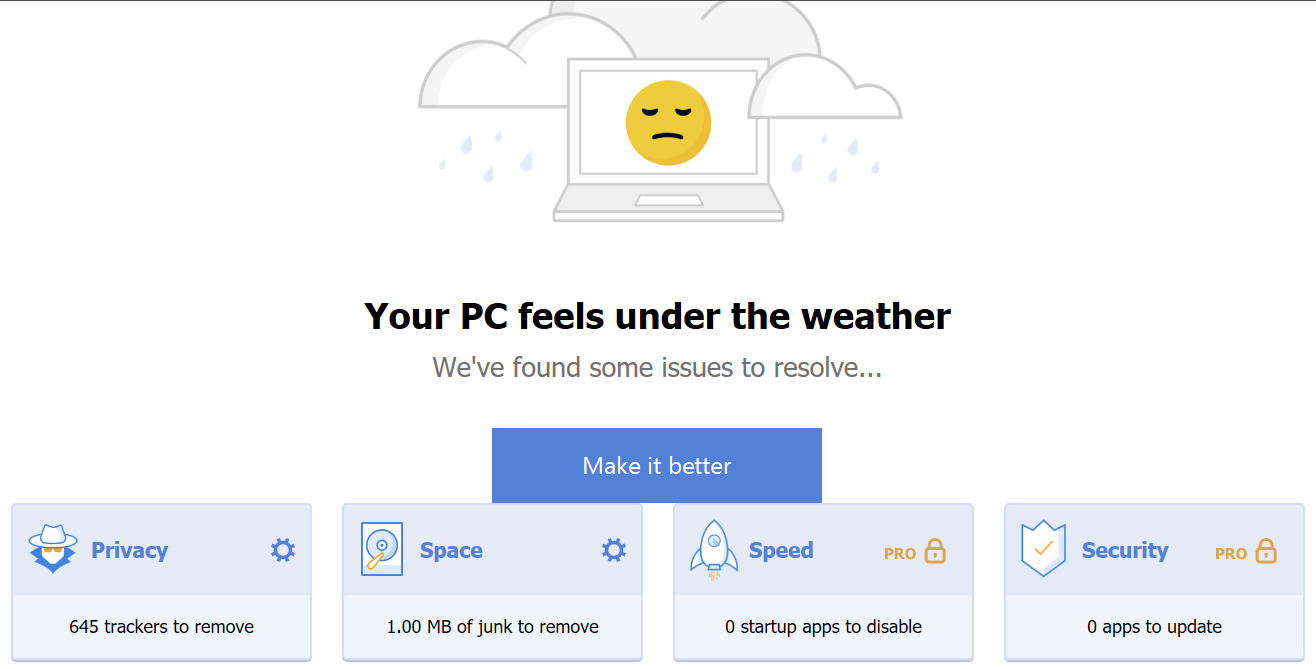
After capturing this baseline measure of the computer’s browsing artifacts the next step in the methodology was to launch CCleaner and run it to remove any browser artifacts using the default settings. Upon launching CCleaner I was prompted to “Take my PC Health Check.” This function appears to have replaced the “Easy Clean” setting, and I closed out of this offer so I could run the scan I desired manually.

*Fig. 3. The CCleaner Free PC Health Check Prompt*

After closing this menu I was presented with the CCleaner interface, which provided me with the Health Check option, as well as the option to run a Custom Clean, alter my registry, access other packaged tools, as well as to view the options or upgrade the program. At this point seeing that Health Check appeared to be the standard scan option, I decided to run it and see how it altered my browser history. In order to perform this scan, CCleaner required me to close my open firefox window, something not required by BrowsingHistoryView

*Fig. 4. The Prompt to Close Mozilla Firefox created by CCleaner*

After clicking the “Close and Analyze” button I waited a few moments for the scan to run, and then was presented with the following screen summarizing the problems that CCleaner had found on my system. I clicked the “Make it better” button here to resolve these issues without customizing any settings, following the methodology outlined in the Magnet Forensics report.

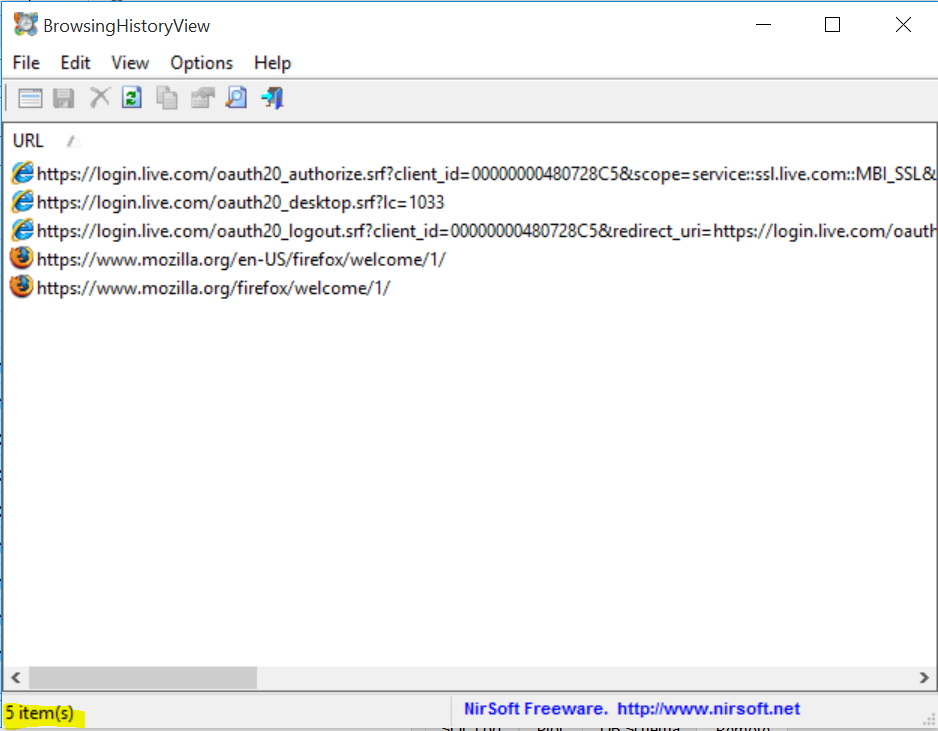


*Fig. 5. The CCleaner Summary Screen.*

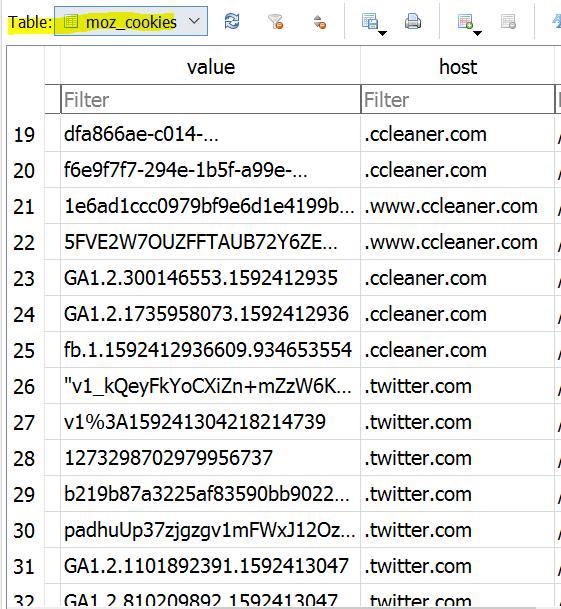
After running this scan I was notified that the junk had been removed, and the trackers had been deleted from my PC. I then restarted the computer as per the methodology and performed my second capture of the browser history.

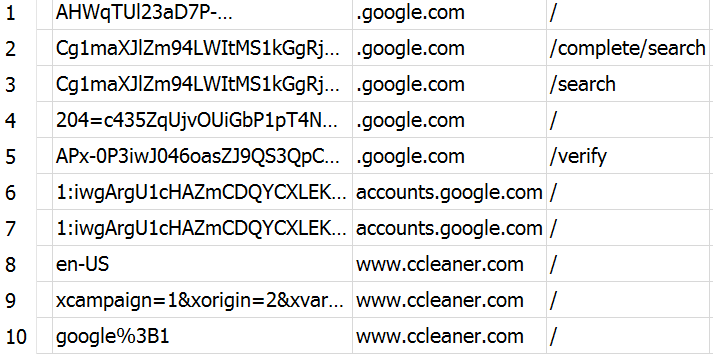
# The Experimental Examination

After running CCleaner, I then performed another examination using BrowserHistoryViewer to determine whether any artifacts on the machine had been deleted. After opening the program, closing the advanced settings window, and clicking the refresh button as I had done in the control examination, the result only 5 events in the history. Three were created by the program Discord, which I had installed on the test machine in order to better simulate an average user’s computer. The other two were the firefox welcome page, which were created when I launched FireFox. In short, CCleaner had completely wiped the browser history, or at least all traces of it that BrowserHistoryViewer were able to find.

*Fig. 6. BrowsingHistoryView’s state after the Experimental Run*

This result surprised me, as CCleaner had not succeeded in removing a significant number of artifacts in Magnet Forensics tests. For this reason, I decided to examine FireFox’s cookies.sqlite file to see how many cookies had remained following the cleaning. I downloaded the program “DB Browser for SQLite” to provide a human readable view of the SQLite file that was used to store the cookies. There were 47 cookies in tact, though a number of these were mozilla cookies that could have been created as a part of the download and installation process of SQLite. Cookies associated with twitter.com, ccleaner.com, and google.com all remained, however.

*Fig. 7.1. Some of the cookies preserved by CCleaner.*

*Fig 7.2. Some of the cookies preserved by CCleaner*

# Conclusions

The results of my own examination run contrary to the results found by Magnet Forensics. While in my examination CCleaner deleted 100% of the browsing history viewable by tools and a majority of the cookies, in Magnet Forensic’s examination there was a reduction on only some areas, with a majority of the artifacts still present to be viewed. I believe that there are a few reasons for this. Firstly, Magnet Forensic’s investigation is older, testing CCleaner v4.02.4115 as opposed to the most recent version of 5.67.7763. It may be that it has since been updated to provide improved performance. Secondly, Magnet Forensic used their own, professional grade examination software to find browser artifacts. This tool may have been able to scrape these results from deleted files on disk, something that BrowserHistoryView is unable to do. If I had the same software, I may have seen similar results.

Overall, it appears that the current version of CCleaner does an admirable job of deleting browser artifacts available using free tools available online. However, the Magnet Forensics study casts doubt that it would be able to perform on a professional level.