Staying Invisible: Analyzing Private Browsing and Anti-forensics on Mac OS X

Rick Schroeder

Staying Invisible: Analyzing Private Browsing and Anti-forensics on Mac OS X

GIAC (GCFE) Gold Certification

Author: Rick Schroeder, rschroeder6687@gmail.com
Advisor: *Jonathan Risto*

Accepted: March 25, 2021

Abstract

The increasing desire to protect personal information has resulted in enhanced privacy features in web browsers. Private browsing modes combined with the growing popularity of disk cleaning tools present a problem for forensic analysts. The increase in privacy features results in a reduction of forensic evidence on the suspect system. This added complexity makes it difficult for an investigator to determine which websites were browsed by the suspect. When the primary sources of forensic evidence are tampered with, it is necessary to identify secondary sources. In Windows-based investigations, secondary evidence is often discovered within hibernation files, operating system artifacts, or error logs. Digital forensic analysts require similar files in macOS. They need to understand how and when logs are written. Identifying and understanding secondary sources of evidence is essential for an analyst to support the details of their case.

1. Introduction

Understanding the activity that occurred during a web browsing session is a critical component to many forensic investigations. Whether the analysis focuses on browsing inappropriate websites or malware downloaded from a compromised website, the requirement is the same. Digital forensics and incident response analysts need a thorough understanding of web browser and operating system artifacts. Analysts conducting browser-based investigations need to know the primary sources of forensic evidence and which tools parse those evidentiary artifacts. They also need to know where to look when the primary sources of evidence have been altered. In Windows-based investigations, secondary sources of evidence include hibernation files, error logs, and other operating system artifacts (Schroeder, 2020). OS X, the tenth version of Apple's Unix-based operating system, was released in 2000. The name of the operating system subtly changed over the years until 2016, when it became macOS (Moreau, 2018). Among the many differences between Microsoft Windows and Apple macOS is how and where they store and log data. Microsoft Windows is the primary operating system installed on desktop computers by a large margin. Windows installations account for 76.26% of desktop operating systems, while OS X comes in second at 16.91% (StatCounter, 2021). There is a large difference separating the first and second most popular desktop operating systems. Even so, it is critical for analysts to understand macOS artifacts, their locations, and the most efficient tools to parse them.

Data privacy is a significant concern for everyone accessing the Internet. In addition to threats such as identity theft and phishing scams, people are worried about their web browsing (Kingpin, 2019). Limiting the amount of personal information users share online, using VPN software, and browsing the Internet using private browsing modes are all recommendations from Norton LifeLock, a leader in Cyber Safety (Rafter, 2021). In his article focusing on protecting online privacy, Dan Rafter states, "If you don't want your computer to save your browsing history, temporary internet files, or cookies, do your web surfing in private mode" (Rafter, 2021).

Cybersecurity best practices often employ a 'Defense in Depth' (DiD) approach when it comes to protecting data. This approach involves implementing multiple layers of

protection to establish redundancy (CIS, 2019). This approach is also common among people trying to protect their online privacy. In addition to private browsing modes, many people use disk cleanup utilities to remove web browsing data from their systems. Disk cleanup tools, also referred to as cache cleaners or cleaner software, are third-party applications that delete web history, browsing artifacts, and other files from computer systems. These applications are marketed as tools that increase privacy, protect personal data, increase system performance, and declutter hard drives (CCleaner, 2020).

While private browsing modes and disk cleanup utilities do offer enhanced privacy and security to users, they are not well received by forensic analysts. These tools complicate browser-based forensic investigations by erasing critical evidence from computer systems. Understanding the impact these tools have on forensic investigations has resulted in their misuse. Private browsing modes and disk cleanup utilities have become popular ways to remove evidence of inappropriate web browsing. The increased popularity of these tools, regardless of the user's intentions, require forensic analysts to search for secondary sources of evidence.

2. Forensic Lab Environment

The lab environment consisted of two Apple MacBook Pro laptops, an iMac analysis system, and a Windows 10 analysis workstation. The laptops were freshly imaged and rebuilt with macOS Mojave Version 10.14.6. The laptops were placed next to each other on a desk so the browsing sessions could occur simultaneously. One laptop browsed the web using Apple Safari Version 14.0, while the other used Google Chrome version 87. Nine specific websites were browsed for approximately 35 minutes. After the browsing sessions were complete, the browsers were closed, and the systems were shut down. The systems were booted to USB using Tsurugi Linux and forensic images of the systems were created. After imaging the hard drives, the laptops were rebooted. The CCleaner application was downloaded and run on both systems, and the imaging process was repeated. The laptops were wiped clean using the native Apple disk wiping tools and macOS Mojave operating system was reinstalled. The web browsing session was repeated using the browser's private browsing mode, Incognito Mode for Google

Chrome, and Private Browsing for Apple Safari. The imaging process was repeated. After the drives were imaged, the systems were rebooted, and CCleaner was installed and run. The systems were shut down and the final images were collected. This resulted in a total of eight forensic image files. There were four separate images for Chrome and Safari, as shown below.

Chrome	Safari
Normal browsing	Normal browsing
Normal browsing w/ CCleaner	Normal browsing w/ CCleaner
Private browsing	Private browsing
Private browsing w/ CCleaner	Private browsing w/ CCleaner

Table 1: Forensics Images

3. Mac Forensic Tools

Often, market share is a major consideration on whether a product is built and brought to market. This is especially true with digital forensics tools. The majority of digital forensic tools are focused on the analysis of the Microsoft Windows operating system. Very few commercial tools, and even less freeware, exist for Apple's macOS operating system. To further complicate Mac forensics, the most Mac-based forensic tools are either outdated Python scripts that are no longer supported or forensic acquisition tools. There is a short supply of forensic tools capable of analyzing data from macOS. Even searching for Mac forensics tools requires the use of carefully crafted Google search derivatives. The shortage of Mac forensics tools resulted in several unsuccessful attempts to use Windows forensics tools to analyze macOS artifacts. Web browsing analysis tools from NirSoft and other vendors could not parse Safari and Chrome history files from macOS.

After acquiring the forensic images, using guymager from a bootable USB drive running Tsurugi Linux, the files were copied to two analysis workstations. Three forensic methodologies performed the analysis on the images from the browsing sessions. The first analysis utilized a commercial offering of Magnet Axiom on a Windows 10

workstation, while Cellebrite BlackLight analyzed data on an Apple iMac workstation. The final method of forensic analysis consisted of multiple freeware tools including DB Browser for SQLite, mac_apt, GriffEye, UnifiedLogReader, and several native macOS tools. The manual analysis occurred on both the Windows and macOS workstations.

3.1. Magnet Axiom

Axiom is Magnet Forensics' newest offering and an extension of their most well-known tool, Internet Evidence Finder (IEF). Axiom utilizes an advanced artificial intelligence (AI) module that "searches both text-based and media content to automatically identify nudity, weapons, drugs, and sexual conversations" (Magnet, 2020). Digital forensics best practices recommend using an Apple system to conduct a forensic examination on an Apple device. This is primarily for the preservation of macOS extended attributes. Extended attributes are a form of metadata maintained exclusively within the APFS or HFS+ file systems. Axiom supports the extended attributes of macOS files. As long as the file is not exported from the Axiom application the extended attributes are maintained (Magnet, 2020). This feature makes Axiom an excellent choice as a Mac forensics tool.

Magnet Axiom's features and controls favor web-based investigations. Browsing data is broken down categorically to highlight websites visited, browsers used, searches performed, and more. Another useful Axiom feature is its skin tone finder. This feature, shown in the image below, allows the analyst to filter image and video files by the percentage of skin tone. This is especially useful when trying to identify files containing nudity. The Magnet Axiom analysis occurred on a custom-built Windows 10 workstation.

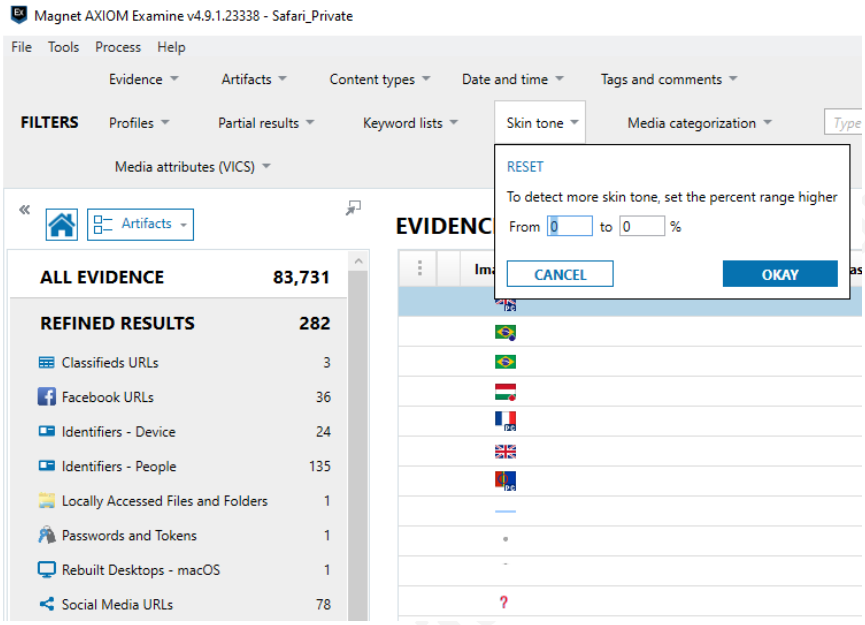


Figure 1: Magnet Axiom's Skin Tone Percentage

3.2. Cellebrite BlackLight

The second analysis method used Cellebrite BlackLight on an iMac desktop computer. BlackLight, soon to be rebranded as Cellebrite Inspector, is one of the few digital forensics tools capable of being installed on macOS. BlackLight, mostly known for its expertise in analyzing macOS, has several useful features to aid in browser-based investigations. “Image categorization reduces review time by revealing images and videos that may contain categories of interest” (Hernandez, 2020). As shown below, categories include porn, weapons, drugs, alcohol, and gambling. Another valuable feature of BlackLight is its ability to identify and parse macOS operating system artifacts such as plists, SQLite databases, and binary files.

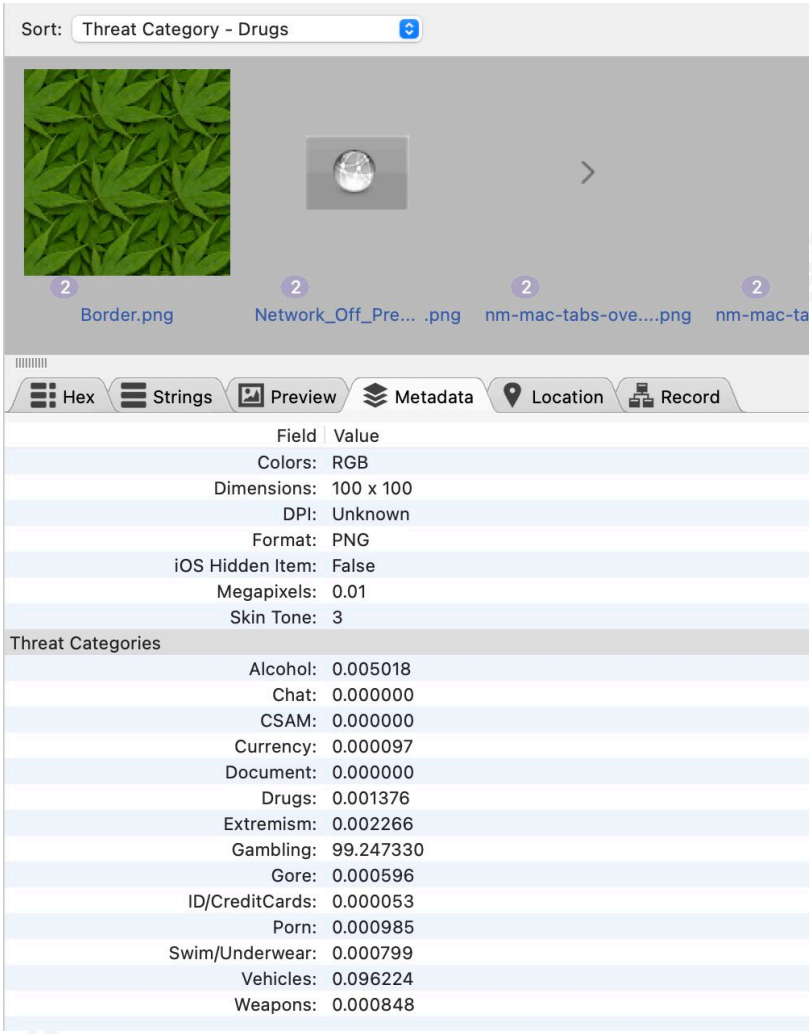


Figure 2: Cellebrite BlackLight's Image Categorization feature

Unfortunately, BlackLight cannot apply this feature to image and video files carved from the web browser cache. The image categorization feature only applies to files saved in image and video formats. Smart Indexing is another useful component of BlackLight. This feature allows the examiner to scan the evidence set for specific words quickly. The ability to analyze operating system artifacts from Windows and macOS gives BlackLight an advantage over other commercial forensics tools. However, the hard-to-maneuver user interface and limited search features limit its ability to find evidence.

3.3. Manual Analysis

The third and final method did not utilize any commercial tools for forensic analysis. Instead, this method relied on a combination of several freeware applications

and Python-based tools. AccessData FTK Imager mounted the image files allowing files to be exported for analysis. After identifying relevant SQLite databases, Liya, DB Browser for SQLite, and SQLite Expert were used to analyze the files and read the database tables. PlistEdit Pro parsed the macOS plist files. UnifiedLogReader and mac_apt, two Python-based tools written by Yogesh Khatri, were critical to the manual analysis. The image below shows UnifiedLogReader collecting macOS unified log files and converting them into both SQLite database and tab-separated value (TSV) formats. mac_apt was useful for processing image files and extracting data and metadata, including unified logs, for further analysis (Khatri, 2021).

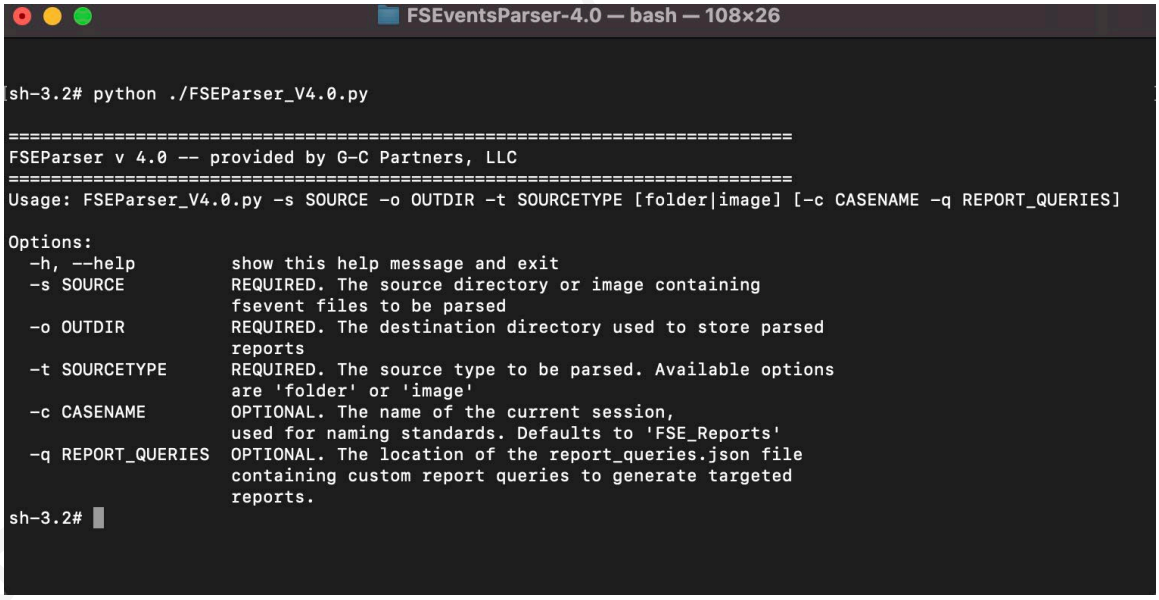


Figure 3: UnifiedLogParser

4. Understanding Normal Web Browsing

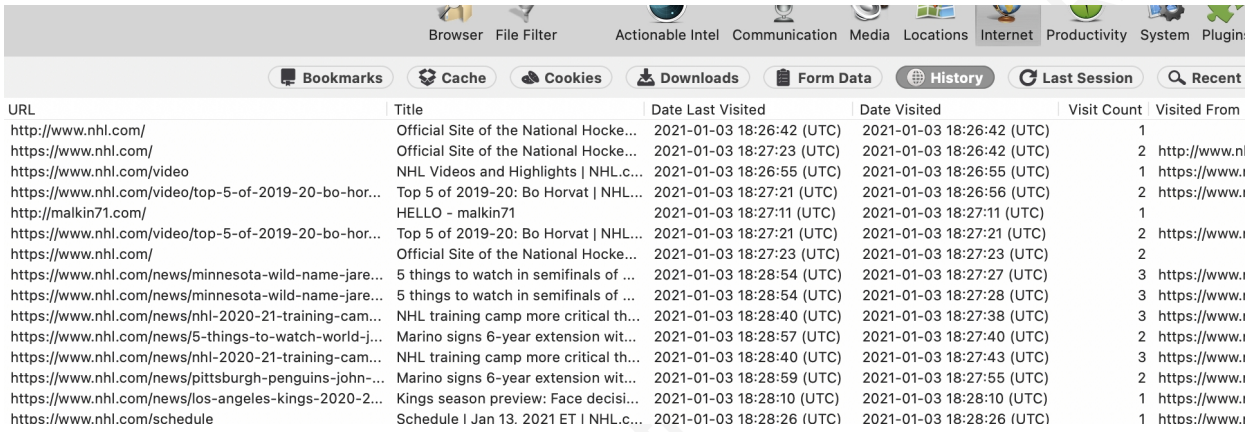
A prerequisite to identifying private browsing modes and disk cleanup utilities is a thorough understanding of web browser artifacts. Forensic analysts need to know what normal looks like before they can identify abnormal. It is important to know where application data and forensic artifacts are located. “MacOS stores the application data for each browser in the user account’s Library folder” (Magnet, 2020). The majority of web browser artifacts are either SQLite databases or property list (plist) format. The exception

to this is the web browser cache, composed of several files and stored using undocumented file types.

User artifacts from the Safari browser are located in /Users/<user>/Library/Safari. Starting with macOS 10.10, Safari moved away from using a plist file to store browsing history. The current history file, History.db, is stored in SQLite format. In addition to the history file, several other files within the Safari folder provide web browsing evidence, including Favicons.db, WebpageIcons.db, Bookmarks.plist, Downloads.plist, LastSession.plist, RecentlyClosedTabs.plist, and the browser cache files. Safari cookies are stored separately, as Binary Cookies, in /Users/<user>/Library/Cookies. As cixtor explains, "Binary Cookies are binary files containing several pieces of data that together form an array of objects representing persistent web cookies for different applications in the macOS and iOS application ecosystem" (cixtor, 2020).

Google Chrome artifacts are located within /Users/<user>/Library/Application Support/Google/Chrome. The main artifacts of interest, Cookies, Favicons, History, Media History, Shortcuts, and Top Sites, are SQLite database files located within /Users/<user>/Library/Application Support/Google/Chrome/Default. Chrome's browser cache is located within the subfolder Cache/Index and like most browsers, these files are stored in a proprietary, undocumented format.

Although the file formats and file locations vary between web browsers, there should be a certain level of uniformity when analyzing the artifacts. Regardless of the file format or the tool used to parse the data, there should be a consistency in the results. While examining evidence from a web browsing session, analysts should expect to find a list of URLs visited, timestamps, visit counts, and other metadata, as shown below. The browser cache should contain evidentiary artifacts such as image and video files from the websites visited.



URL	Title	Date Last Visited	Date Visited	Visit Count	Visited From
http://www.nhl.com/	Official Site of the National Hocke...	2021-01-03 18:26:42 (UTC)	2021-01-03 18:26:42 (UTC)	1	
https://www.nhl.com/	Official Site of the National Hocke...	2021-01-03 18:27:23 (UTC)	2021-01-03 18:26:42 (UTC)	2	http://www.nl
https://www.nhl.com/video	NHL Videos and Highlights | NHL.c...	2021-01-03 18:26:55 (UTC)	2021-01-03 18:26:55 (UTC)	1	https://www.r
https://www.nhl.com/video/top-5-of-2019-20-bo-hor...	Top 5 of 2019-20: Bo Horvat | NHL...	2021-01-03 18:27:21 (UTC)	2021-01-03 18:26:56 (UTC)	2	https://www.r
http://malkin71.com/	HELLO - malkin71	2021-01-03 18:27:11 (UTC)	2021-01-03 18:27:11 (UTC)	1	
https://www.nhl.com/video/top-5-of-2019-20-bo-hor...	Top 5 of 2019-20: Bo Horvat | NHL...	2021-01-03 18:27:21 (UTC)	2021-01-03 18:27:21 (UTC)	2	https://www.r
https://www.nhl.com/	Official Site of the National Hocke...	2021-01-03 18:27:23 (UTC)	2021-01-03 18:27:23 (UTC)	2	
https://www.nhl.com/news/minnesota-wild-name-jare...	5 things to watch in semifinals of ...	2021-01-03 18:28:54 (UTC)	2021-01-03 18:27:27 (UTC)	3	https://www.r
https://www.nhl.com/news/minnesota-wild-name-jare...	5 things to watch in semifinals of ...	2021-01-03 18:28:54 (UTC)	2021-01-03 18:27:28 (UTC)	3	https://www.r
https://www.nhl.com/news/nhl-2020-21-training-cam...	NHL training camp more critical th...	2021-01-03 18:28:40 (UTC)	2021-01-03 18:27:38 (UTC)	3	https://www.r
https://www.nhl.com/news/5-things-to-watch-world-j...	Marino signs 6-year extension wit...	2021-01-03 18:28:57 (UTC)	2021-01-03 18:27:40 (UTC)	2	https://www.r
https://www.nhl.com/news/nhl-2020-21-training-cam...	NHL training camp more critical th...	2021-01-03 18:28:40 (UTC)	2021-01-03 18:27:43 (UTC)	3	https://www.r
https://www.nhl.com/news/pittsburgh-penguins-john-...	Marino signs 6-year extension wit...	2021-01-03 18:28:59 (UTC)	2021-01-03 18:27:55 (UTC)	2	https://www.r
https://www.nhl.com/news/los-angeles-kings-2020-2...	Kings season preview: Face decisi...	2021-01-03 18:28:10 (UTC)	2021-01-03 18:28:10 (UTC)	1	https://www.r
https://www.nhl.com/schedule	Schedule | Jan 13, 2021 ET | NHL.c...	2021-01-03 18:28:26 (UTC)	2021-01-03 18:28:26 (UTC)	1	https://www.r

Figure 4: Cellebrite BlackLight's analysis of normal web browsing

4.1. Apple Safari: Normal Browsing vs Private Browsing

The web browsing sessions that occurred as part of this research lasted approximately 35 minutes. During those browsing sessions, images were viewed, videos were watched, web pages were scrolled, and links were clicked. Some of the links also caused pop-ups and the launching of new tabs. As expected, this produced a lot of evidentiary artifacts on the test systems.

Using a keyword list, Magnet Axiom discovered over 700 pieces of forensic evidence from the 35 minute browsing session. Most of the evidence recovered resided within the Safari history file, RecentlyClosedTabs.plist, KnowledgeC.db, and LocalStorage files. As stated by Mati Goldberg, "The KnowledgeC database stores an event log of multiple processes that run within an Apple device ranging from application usage to speaker output switching" (Goldberg, 2019). A log of Safari browsing history is stored in KnowledgeC.db. LocalStorage files are SQLite databases used by browsers that adhere to the WebKit format. These files may contain browser settings, plug-ins, and cached data (FileInfo, 2019). An additional 3,500 items were discovered by manually searching through the Safari browser cache. Surprisingly, all of these files were images. Axiom was unable to identify any video files, or partial video files, from the browsing session. Additional manual analysis of Safari artifacts produced significantly more evidence. The Favicons.db file, used to store the image associated with specific websites and shown below, contained evidence of all websites from the browsing session. The CacheSettings.plist file, used to configure advanced settings for the content cache, also

showed evidence from the browsing session. The total number of evidentiary artifacts identified using Magnet Axiom was 4,222. The additional evidence demonstrates the importance of performing manual analysis to double-check the findings from your tools.

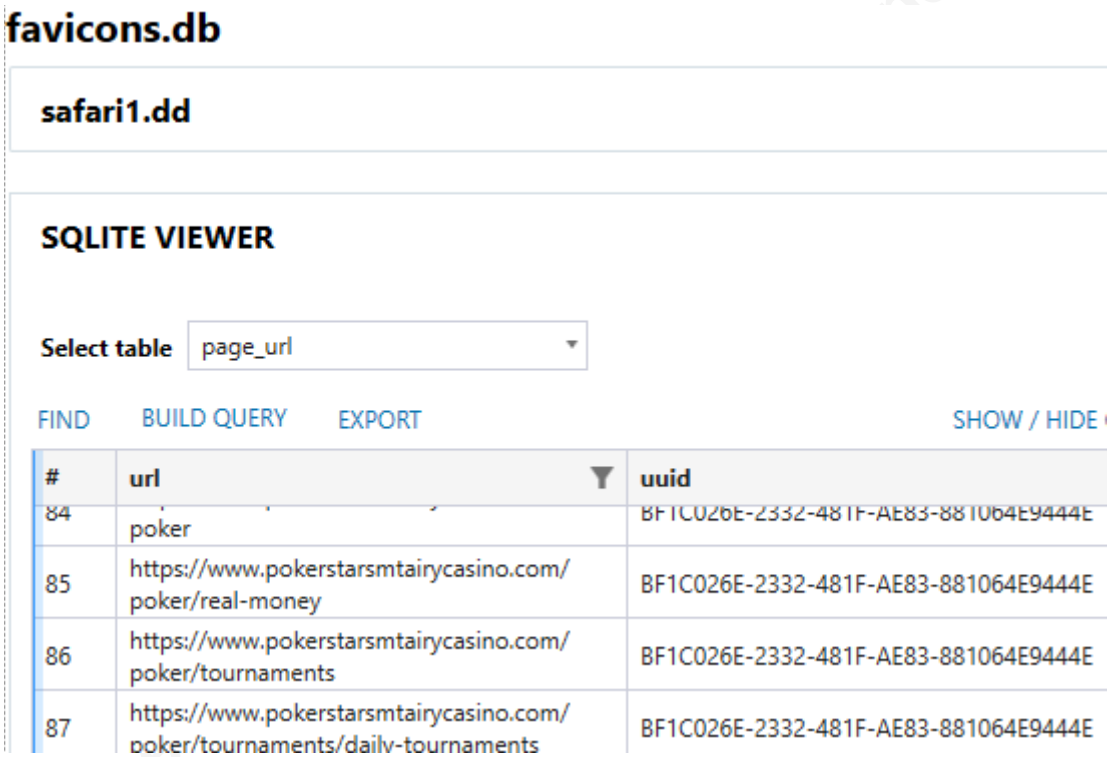


Figure 5: Favicons.db

The Safari browsing session was analyzed by Cellebrite BlackLight using the same keyword list as Magnet Axiom. One of the most notable differences between the Axiom and BlackLight was the amount of time it took to process the evidence. Although the hardware from the two systems was different, both workstations were built in the last 12 months. Axiom processed the images files in approximately two hours, while BlackLight required a minimum of eight hours. Performing content searches within the two tools also produced different results. Axiom searches were complete in under a minute, while BlackLight searches lasted over 45 minutes. BlackLight identified 4,445 hits from the keyword list, 61 of which were false positives. Similar to the Axiom analysis, much of the evidence was discovered within the Safari artifacts. Evidence was discovered within the history file, CacheSettings.plist, RecentlyClosedTabs.plist, Favicons.db, and browser cache files. Although BlackLight took much longer to process

the image file, it parsed the browser cache and identified several images and text files from the browsing session. As shown below, the tool also rebuilt several webpages.

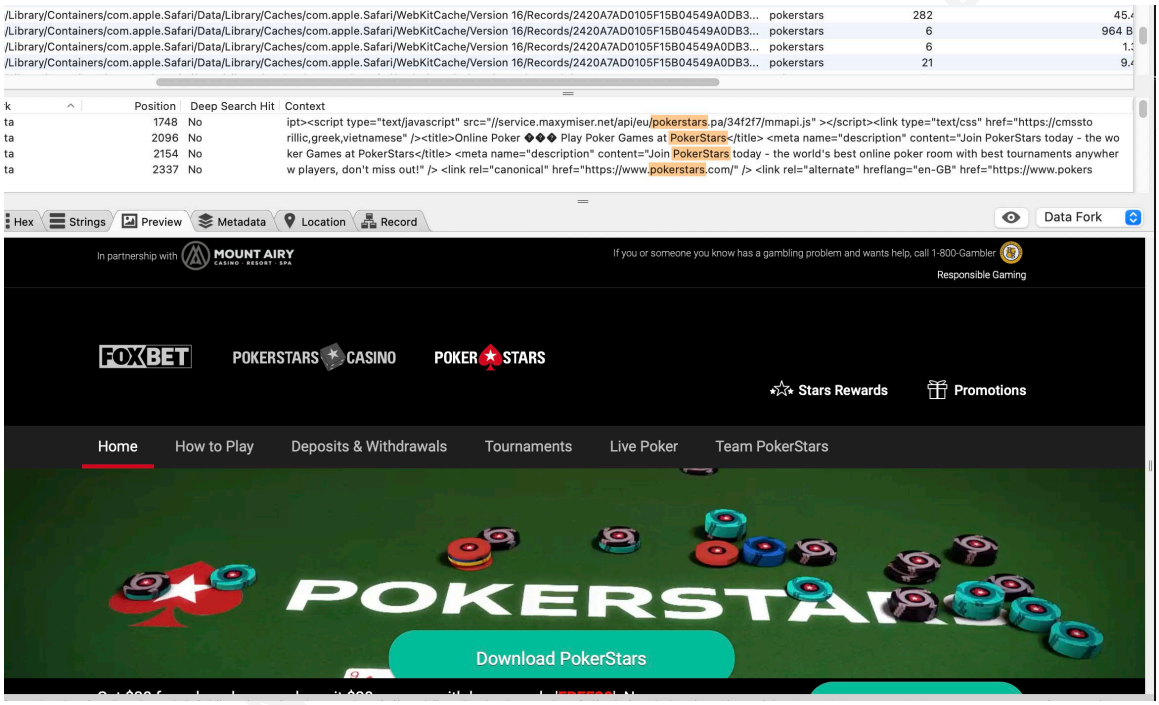


Figure 6: The Pokerstars website rebuilt by BlackLight

BlackLight also parsed Safari's binary cookies file, Cookies.BinaryCookies, and identified cookies from each of the websites visited during the browsing session. While parsing Safari's Tab Snapshot feature, BlackLight discovered evidence from three of the websites visited in Metadata.db. The extra time spent processing the image file resulted in the discovery of additional evidence.

Axiom's analysis of Safari's private browsing session was not as successful at uncovering forensic evidence of the browsing session. The same keyword list used to identify evidence from the normal browsing session did not generate any hits from the private browsing session. Further analysis of the web browsing artifacts and image and video files from the system, using Axiom, did not uncover any additional evidence. None of the plist files or SQLite databases showed any evidence from the private browsing session.

BlackLight's analysis of the Safari private browsing session could not find any evidence of the websites visited. The tool identified 33 hits from the keyword list, all of which were all false positives. Manual analysis, using BlackLight, of the previously

identified artifacts produced the same results. None of the SQLite databases, plists, or log files retained any evidence from the private browsing session.

The commercial tools could not find any evidence from the private browsing session. In order to discover evidence from the browsing session, manual analysis of the web browser and operating system artifacts was required. After exporting the browser artifacts from the image file, DB Browser for SQLite examined the relevant database files, including History.db, Favicons.db, PerSitePreferences.db, Metadata.db, and Cache.db. None of the SQLite database files contained any evidence of the private browsing session. Next, plist files, such as LastSession, Bookmarks, TopSites, and CacheSettings, were analyzed using PlistEdit Pro. The plist files did not contain any evidence from the private browsing session.

After failing to discover evidence from the SQLite and plist files, mac_apt, by Yogesh Khatri, was run against the image file. Mac_apt "is a Python based framework, which has plug-ins to process individual artifacts such as Safari internet history, Network interfaces, recently accessed files & volumes" (Khatri, 2021). After providing the tool with the image file's location and the desired output, the data was processed and the results were exported in SQLite format. DB Browser for SQLite queried the database tables and displayed evidence of the private browsing session. Evidence from one of the nine websites visited was identified. The UnifiedLogs database table contained ten references to the website, found within two tracev3 files. Unified logging is Apple's current log format. It was introduced in 2016 with the release of macOS Sierra (Hoakley, 2017). As explained by Hoackley, "Log contents are stored as tracev3 files – an undocumented compressed binary format – in /var/db/diagnostics/Persist/ and /var/db/diagnostics/Special/. Other folders in /var/db/diagnostics/ and /var/db/uuidtext/ contain ancillary information for those logs" (Hoakley, 2017). The evidence from the browsing session was written to the unified logs by the com.apple.WebKit.WebContent process, used by Safari to display web content (Degtiarenko, 2020). The entries in the unified logs were the result of dropped frames while playing video files. As shown in the image below, the log entries provide plenty of metadata, including timestamps.

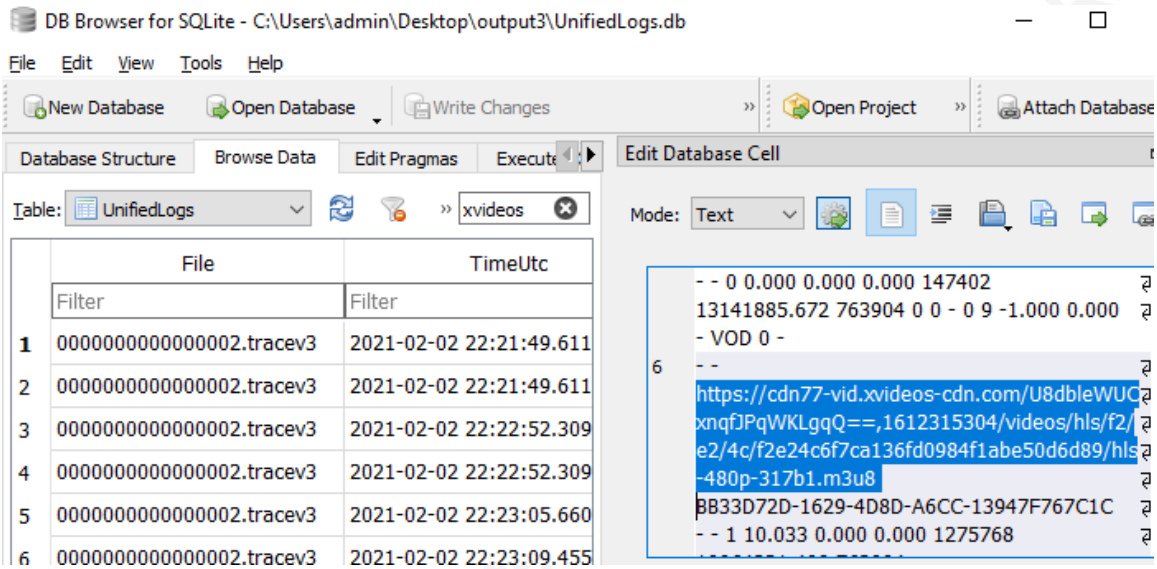


Figure 7: Evidence of private browsing in unified logs

The chart below summarizes the findings from the Safari browsing sessions. The first column identifies the name of the browsing session. The next three columns indicate the analysis methodology. The numbers below the methodologies identify the number of evidentiary artifacts discovered.

Browsing Session	Axiom	BlackLight	Manual Analysis
Safari normal	4222	4384	1582
Safari private	0	0	10

Table 2: Summary of findings from Safari normal browsing and private browsing

4.2. Google Chrome: Normal Browsing vs Incognito Browsing

Magnet Axiom's analysis of normal web browsing in Google Chrome produced 1,335 findings using the keyword list. Most of the evidence discovered by Axiom was within the primary Chrome artifacts. Parsing the Chrome history file showed the URLs and timestamps from the browsing session. Axiom also parsed the Chrome Cookies, Favicons, and Shortcuts files. Evidence from the browsing session was also carved from unallocated clusters and local storage files. Manual searches performed with Axiom identified additional evidence. Chrome's Preferences file contained evidence of all websites visited. Additional evidence was also discovered within Chrome's History Provider Cache, Quota Manager, and Media History. Thousands of images and hundreds of videos from the browsing session were discovered in the Chrome cache files. Image and video files from the Safari browsing session also went undiscovered by Axiom.

Rick Schroeder, rschroeder6687@gmail.com

However, the media files from the Chrome session did not include metadata such as timestamps. Timestamps are a critical piece of evidence. They are especially valuable when proving who was behind the keyboard.

Analysis of a normal browsing session using Cellebrite BlackLight produced similar results. The tool identified over 7,000 evidentiary artifacts from the keyword list, although approximately 500 were false positives. In addition to the primary web artifacts of the history, cookies, and browser cache files, BlackLight discovered evidence within several of Chrome's SQLite database files, including Preferences, Favicons, Network Action Predictor, and Shortcuts. The Google Chrome Code Cache directory contained cached JavaScript files containing evidence of all the websites visited. Additional evidence from the browsing session was carved from unallocated space.

Magnet Axiom's analysis of Chrome's Incognito mode browsing session was identical to the tool's analysis of the Safari private browsing session. Axiom was unable to identify any hits from the keyword list. Manual examination of the Chrome and operating system artifacts was also unsuccessful.

BlackLight's analysis of the Chrome Incognito Mode browsing session produced 48 hits from the keyword list. Of those 48 hits, 46 were false positives. The tool successfully identified two evidentiary artifacts from within a unified logging tracev3 file. As shown below, BlackLight was able to identify text from two of the URLs visited during the browsing session. However, Blacklight was unable to parse the tracev3 file. Manual analysis of the image file using BlackLight did not result in any additional evidence.

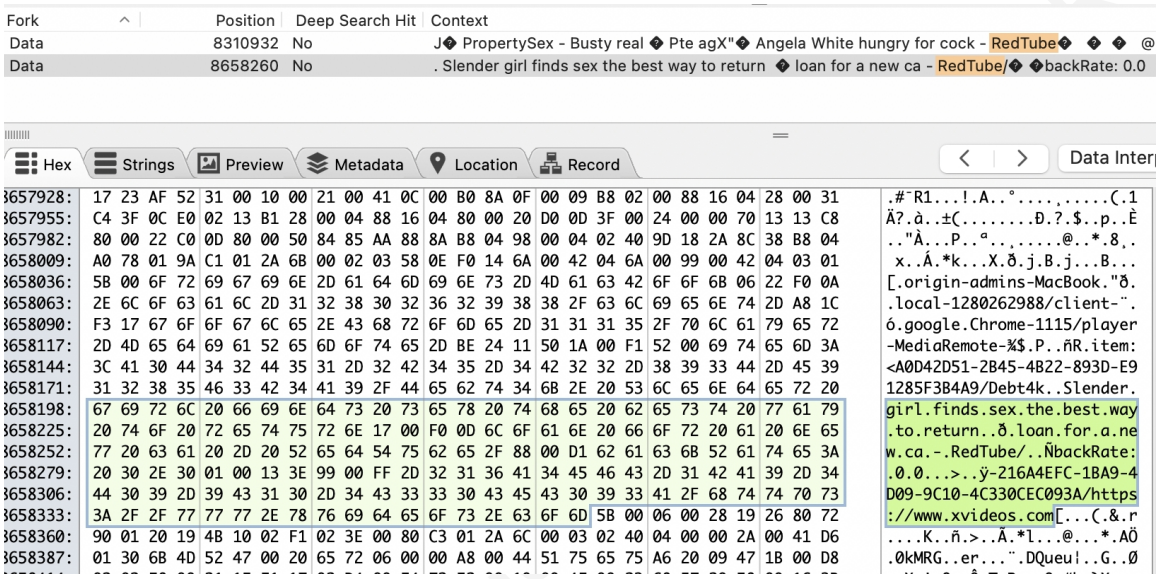


Figure 8: BlackLight's analysis of a macOS tracev3 file

Manual analysis of Chrome Incognito Mode browsing began the same way as the Safari Private browsing session's manual analysis. DB Browser for SQLite and Liya, could not find any evidence from the private browsing session. PlistEdit Pro did not find any evidence in the plist files. However, BlackLight already discovered evidence from the browsing session, providing a great starting point for manual analysis. Yogesh Khatri's mac_apt tool parsed the tracev3 files from Apple's unified logging. The Python-based tool found evidence of two of the websites visited. The data was written to the unified log files by the MediaRemote framework due to problems experienced while playing video files. In total, mac_apt found six evidentiary artifacts from one website and three from another.

The chart below summarizes the findings from the Chrome browsing sessions. The first column shows the name of the browsing session and the next three columns identify the analysis method. The number of evidentiary artifacts discovered is shown in the boxes below each methodology.

Browsing Session	Axiom	BlackLight	Manual Analysis
Chrome normal	4835	6502	1726
Chrome private	0	2	6

Table 3: Summary of findings from Chrome browsing sessions

Rick Schroeder, rschroeder6687@gmail.com

5. The Impact of Disk Cleanup Utilities

Tools such as Disk Drill, CCleaner, CleanMyMac X, and MacClean are gaining popularity among Apple users (Morelo, 2021). The software companies developing these applications refer to them as Mac cleaners, disk cleanup utilities, and browser history cleaners. The digital forensic and incident response analysts that discover the tools in investigations refer to them as anti-forensics or counter forensics tools. These terms refer to actions taken by attackers to remove or alter forensic artifacts with the intention of negatively impacting a forensic investigation (Kuntal, 2020). Although the reasons for running these tools can vary greatly, the impact they have on forensic analysis does not change. Critical evidence has been altered or deleted. This requires analysts to find secondary artifacts to support their case.

5.1. Apple Safari: Normal Browsing and Disk Cleanup Tools

Although Magnet Axiom did not find any evidence from the private browsing sessions, it discovered evidence from the Safari browsing session followed by CCleaner. Using the keyword list, Axiom found 165 evidentiary artifacts. The evidence was found in two locations. Axiom carved 94 items from unallocated space and the remaining 71 items were identified in the KnowledgeC database. The evidence in KnowledgeC and 12 items carved from unallocated space contained timestamps. Manual analysis, using Axiom, uncovered additional evidence. Favicons.db contained evidence of all the websites visited during the browsing session. The CacheSettings.plist file held evidence from two of the websites. Cached data from three more websites was discovered in separate local storage files.

BlackLight's analysis of Safari browsing and CCleaner use identified 422 evidentiary artifacts. Of the 422 items found, 44 were false positives, and 327 were carved from unallocated space. The remaining 51 items were discovered within KnowledgeC.db and Safari artifacts such as Favicons.db, CacheSettings.plist, and Observations.db, a SQLite database used "to manage the data that websites can store in the client file system like databases or caches" (WebKitGTK, 2019).

The analysis performed by Axiom and BlackLight of the Safari browsing and CCleaner use provided a starting point for the manual analysis. The commercial tools

already identified several SQLite databases and plist files containing evidence. The evidence within those files was confirmed using DB Browser for SQLite and Liya. As expected, those tools did not discover any evidence from the Safari history file or binary cookies. Cached information from all of the websites visited was also identified within Safari local storage files using mac_apt. Analysis of the unified logs, using mac_apt and UnifiedLogParser, identified evidence from one of the sites browsed. As shown below, the event was written to the log file by the com.apple.WebKit.Networking process, used by Safari and other web browsers for file uploads (McAfee, 2020).

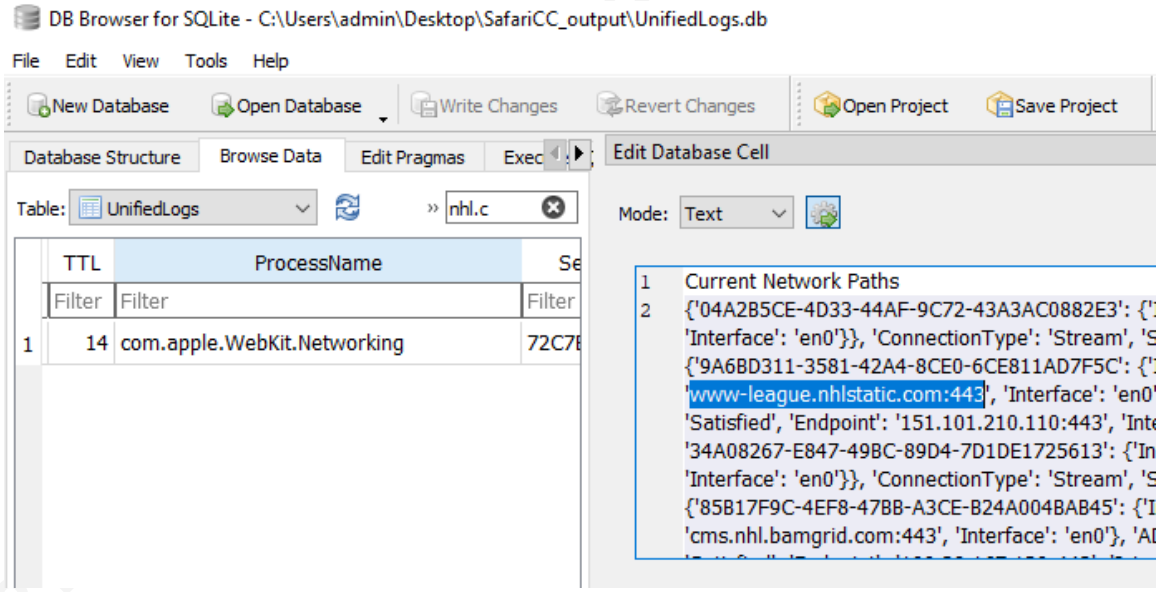


Figure 9: SQLite analysis of unified logs parsed by mac_apt

5.2. Google Chrome: Normal Browsing and Disk Cleanup Tools

Magnet Axiom's analysis of the Google Chrome browsing session and CCleaner use identified 283 evidentiary artifacts. The evidence resided within three files. Evidence of all nine websites was discovered in the Chrome Shortcuts file. Cached data from five of the websites, and timestamps, were carved from Chrome artifacts. The remaining 218 items, carved from unallocated space, did not contain timestamps. Manual analysis, using Magnet Axiom, identified 49 image files from the browsing session.

BlackLight's analysis of the same image file produced 148 hits from the keyword list. Although Axiom identified more evidence, BlackLight identified better evidence. The evidence identified by BlackLight included valuable metadata such as timestamps.

Rick Schroeder, rschroeder6687@gmail.com

Most of the evidence discovered by Axiom resided within unallocated space and lacked valuable metadata such as timestamps. Of the 148 items found by BlackLight, 20 were false positives, and 51 were carved from unallocated space. Chrome artifacts such as Favicons, Preferences, Shortcuts, Local Storage, and QuotaManager contained the remaining items. Manual analysis with BlackLight did not identify any additional evidence.

Much like the manual analysis of the Safari browsing session and CCleaner use, the commercial tools provided a great starting point. The manual analysis confirmed the findings of the commercial tools. Evidence was discovered within Chrome artifacts such as Favicons, Preferences, Shortcuts, and QuotaManager. No evidence was discovered from the Google Chrome History or Cookies files. Analysis of the unified logs identified additional evidence from two of the websites visited. The information was written to the unified logs by the MediaRemote framework. The MediaRemote framework manages content and communicates with remote media servers (Apple, 2017).

The chart below summarizes the findings from the Safari and Chrome browsing sessions followed by CCleaner. The first column identifies the name of the browsing session. The following three columns describe the analysis methodology. The numbers below the methodologies identify the number of evidentiary artifacts discovered.

Browsing Session	Axiom	BlackLight	Manual Analysis
Safari CCleaner	263	367	124
Chrome CCleaner	332	148	96

Table 4: Summary of findings from normal browsing and CCleaner

6. Combining Private Browsing and Disk Cleanup Tools

Cybersecurity professionals follow a Defense-in-Depth (DiD), or layered, approach towards protecting their assets. The redundancy provides better protection. End users follow a similar process. Instead of layering security products to protect their assets, they are combining private web browsing and disk cleaning utilities to increase their chances of removing data.

Rick Schroeder, rschroeder6687@gmail.com

After acquiring forensic images, the laptops were rebooted. CCleaner was downloaded, installed, and run. No changes were made to CCleaner's default settings. After running CCleaner, the laptops were shut down, and another image was acquired. Magnet Axiom was unable to identify any evidence from either of the private browsing sessions. It should come as no surprise that it was unable to find evidence after CCleaner ran on the same system.

BlackLight's analysis of the Safari private browsing session and CCleaner use failed to identify any evidence from the browsing session. Manual analysis of the data using BlackLight was unable to identify any evidence. Cellebrite BlackLight's analysis of the Chrome Incognito browsing with CCleaner identified evidence in two tracev3 files. These were the same evidentiary artifacts the tool previously discovered from the Chrome Incognito browsing session. The tracev3 files, part of Apple's unified logging, referenced two websites that experienced problems playing video files.

The manual analysis of the two private browsing sessions with CCleaner use was similar to the commercial tool findings. Analysis of the SQLite databases, using DB Browser for SQLite and Liya, failed to identify any evidence from the browsing sessions. PlistEdit Pro experienced the same results when tasked with analyzing plist files. The only remaining source of evidence from the two browsing sessions was Apple unified logs. The unified logs were parsed using mac_apt and UnifiedLogReader, and the output was exported in SQLite database format. As shown in the image below, Liya displayed the data from the unified logs. As previously documented, both browsing sessions contained unified log entries for issues experienced regarding video playback on websites.

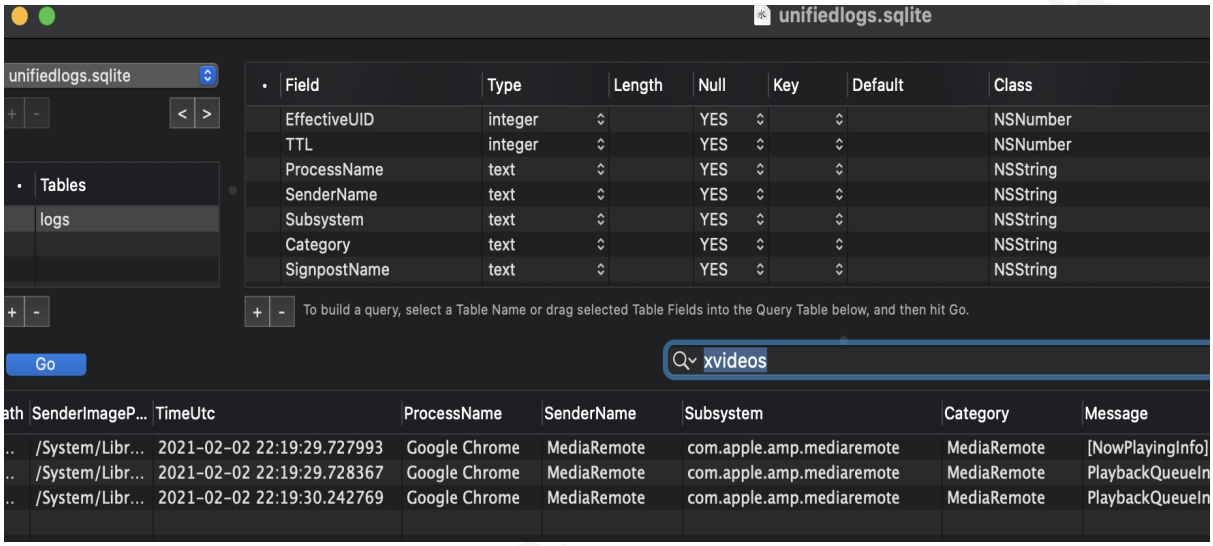


Figure 10: Liya displaying evidence from unified logs

The chart below shows the findings from the Safari and Chrome private browsing sessions followed by CCleaner. The first column identifies the name of the browsing session and the last three display the analysis methodology.

Browsing Session	Axiom	BlackLight	Manual Analysis
Safari both	0	0	10
Chrome both	0	2	6

Figure 11: Summary of findings from private browsing and CCleaner

7. Conclusion

Private web browsing does not write any information from the browsing session to the hard drive, thus enhancing the privacy of its users. Disk cleaning utilities remove evidence of web browsing from the primary web browser artifacts. Private web browsing and disk cleanup utilities are becoming more popular. Analysis of secondary artifacts is critical when private browsing and disk cleaning utilities are used. The tracev3 files used by Apple's unified logs contain a tremendous amount of information. Unified logging is Apple's central logging mechanism. It is the single location where all logs are stored. Forensic analysis of Apple's unified logs can be critical to an investigation and may be the only source of essential evidence. Although Apple's closed, proprietary log format adds a level of complexity to the analysis of macOS artifacts, several tools are capable of parsing the data.

Rick Schroeder, rschroeder6687@gmail.com

References

Apple. (2017, June 28). *Remote Command Center Events*. Retrieved from Apple Developer: https://developer.apple.com/documentation/mediaplayer/remote_command_center_events

Benson, R. (2019, August 8). *Deciphering Browser Hieroglyphics: FileSystem (Part 3)*. Retrieved from DFIR blog: https://dfir.blog/deciphering-browser-hieroglyphics-leveldb-filesystem/

Caithness, A. (2020, September 23). *Hang on! That's not SQLite! Chrome, Electron and LevelDB*. Retrieved from CCL Solutions Group: https://www.cclsolutionsgroup.com/post/hang-on-thats-not-sqlite-chrome-electron-and-leveldb

CCleaner. (2020, June 23). *How to fix 3 common Mac problems: a quick guide*. Retrieved from CCleaner: https://www.ccleaner.com/knowledge/how-to-fix-3-common-mac-problems-a-quick-guide

CCleaner. (2020). *Introducing CCleaner: What it can and can't do*. Retrieved from CCleaner: https://www.ccleaner.com/docs/ccleaner/introducing-ccleaner/what-it-can-and-cant-do

Cellebrite. (2020). *Cellebrite BlackLight*. Retrieved from Cellebrite: https://www.cellebrite.com/en/blacklight/

Center for Internet Security (CIS). (2019, October). *Cybersecurity Spotlight – Defense in Depth (DiD)*. Retrieved from Center for Internet Security: https://www.cisecurity.org/spotlight/cybersecurity-spotlight-defense-in-depth-did/

cixtor. (2020, March 3). *cixtor/binarycookies*. Retrieved from Github: https://github.com/cixtor/binarycookies

Cole, A. (2020, October 25). *CCleaner for Mac Review – It's Time to Clean Up Your Mac*. Retrieved from Clever: https://www.cleverfiles.com/howto/ccleaner-mac.html

darkdefender. (2019, April 12). *Brief Introduction to MacOS Forensics*. Retrieved from Medium.com: https://darkdefender.medium.com/brief-introduction-to-macos-forensics-f817c9c83609

Rick Schroeder, rschroeder6687@gmail.com

Degtiarenko, I. (2020, May 21). *What to do when Safari Web Content quits unexpectedly*. Retrieved from MacPaw: https://macpaw.com/how-to/safari-web-content-quit-unexpectedly

Edwards, S. (2016, November 13). *New macOS Sierra (10.12) Forensic Artifacts – Introducing Unified Logging*. Retrieved from mac4n6: https://www.mac4n6.com/blog/2016/11/13/new-macos-sierra-1012-forensic-artifacts-introducing-unified-logging

Epoch Converter. (2020). *Convert WebKit/Chrome timestamps to human-readable date & Unix time*. Retrieved from Epoch Converter: https://www.epochconverter.com/webkit

FileInfo. (2019, October 9). *.LOCALSTORAGE File Extension*. Retrieved from FileInfo: https://fileinfo.com/extension/localstorage

Goldberg, M. (2019, June 13). *How a Suspect's Pattern-of-life Analysis is Enhanced with KnowledgeC Data*. Retrieved from Cellebrite: https://www.cellebrite.com/en/how-a-suspects-pattern-of-life-analysis-is-enhanced-with-knowledgec-data/

Hernandez, A. (2020, August 12). *Top 3 Features to Try in Cellebrite BlackLight*. Retrieved from Cellebrite: https://www.cellebrite.com/en/top-3-features-to-try-in-cellebrite-blacklight-2019-r1/

hoakley. (2017, October 10). *Inside the macOS log: logd and the files that it manages*. Retrieved from The Eclectic Light Company: https://eclecticlight.co/2017/10/10/inside-the-macos-log-logd-and-the-files-that-it-manages/

Hunter, B. (2020, April 24). *How to Add Unified Logs to Cellebrite BlackLight*. Retrieved from Cellebrite: https://www.cellebrite.com/en/adding-unified-logs-to-cellebrite-blacklight/

John. (2021, January). *Best Mac Cleaner Software 2021*. Retrieved from TechsViewer: https://techsviewer.com/best-mac-cleaner-software/

Khatri, Y. (2021, January 17). *mac_apt macOS Artifact Parsing Tool*. Retrieved from github: https://github.com/ydkhatri/mac_apt

Rick Schroeder, rschroeder6687@gmail.com

Kingpin. (2019, December 19). *Top 5 computer privacy issues and how to avoid them*. Retrieved from Kingpin: https://kingpinbrowser.com/blog/computer-privacy-issues/

Kingpin. (2020). *10 Best browser history and cache cleaners for 2020*. Retrieved from Kingpin: https://kingpinbrowser.com/blog/best-browser-cleaners/

Kuntal, A. S. (2020, April 29). *An Introduction to Anti-Forensic Techniques*. Retrieved from Hawk Eye Forensic: https://hawkeyeforensic.com/2020/04/29/an-introduction-to-anti-forensics-techniques/

Magnet Forensics. (2020). *Magnet Axiom macOS Examinations (AX350).* Waterloo: Magnet Forensics.

Martin, J. M. (2020, August 25). *Finding Waldo: Leveraging the Apple Unified Log for Incident Response*. Retrieved from Crowdstrike: https://www.crowdstrike.com/blog/how-to-leverage-apple-unified-log-for-incident-response/

McAfee. (2020, October 6). *How to block classified file access by Safari using Data Loss Prevention Endpoint*. Retrieved from McAfee Knowledge Center: https://kc.mcafee.com/corporate/index?page=content&id=KB93496&locale=en_US

Moreau, S. (2018, June 6). *The evolution of macOS (and Mac OS X)*. Retrieved from Computer World: https://www.computerworld.com/article/2983507/the-evolution-of-macos-and-mac-os-x.html

Morelo, d. (2021, February 9). *10 Best FREE Mac Cleaners to Remove Junk from Your Mac*. Retrieved from Macgasm: https://www.macgasm.net/news/reviews/best-free-mac-cleaners/

Rafter, D. (2021, January 23). *How to protect your privacy online*. Retrieved from Norton: https://us.norton.com/internetsecurity-privacy-protecting-your-privacy-online.html

StatCounter. (2021, January). *Desktop Operating System Market Share Worldwide*. Retrieved from Statcounter: https://gs.statcounter.com/os-market-share/desktop/worldwide

Rick Schroeder, rschroeder6687@gmail.com

WebKitGTK. (2019). *WebKitWebsiteDataManager*. Retrieved from WebKitGTK Reference Manual: https://webkitgtk.org/reference/webkit2gtk/stable/WebKitWebsiteDataManager.html