CAL POLY

California Cybersecurity Institute

Computer Forensics CCIC Training

Chapter 10: Internet History

Lauren Pixley, Cassidy Elwell, and James Poirier

May 2019 (Version 2)

10

Internet History

Introduction

Internet history is an important aspect in many cases. You can find out what sites your suspect visited, what they were searching for, and if they downloaded any data. Earlier in the Craig Tucker case, you found files in his Downloads folder. There was a RAR file and two ZIP files that contained several coupons. Where did the suspect download these files from? Some of Craig's email messages also mentioned a "4chan site". What is the 4chan site, and why did Craig visit it? By the end of this section, you will be able to answer these questions and you will have a better understanding of Internet history.

Cookies

Cookies are small pieces of text which is sent to your browser by a website the user visits. The information a cookie stores helps the visited website remember any settings or preferences you specified so that returning to the website will be easier. While companies use cookies to remember your preferences, count visitors, and make relevant ads, investigators can use such information as one way to track the user's browser activity. The following data is stored in the browser's cookies:

Name	The name of the cookie
Content/Value	The value of the cookie **Note:** This is often a string which often represents a session id used by the visited website to recover your session from a larger session state.
Domain	The domain of the cookie
Accessible to script	Yes if Https, No if HttpOnly
Created	The date/time the cookie was created
Expires	The date/time the cookie will expire (typically 1 year from Created) **Note:** If a date/time is not specified then this cookie will remain in the browser until the user deletes it.

When looking at cookies within a browser, the user sees a view similar to this:

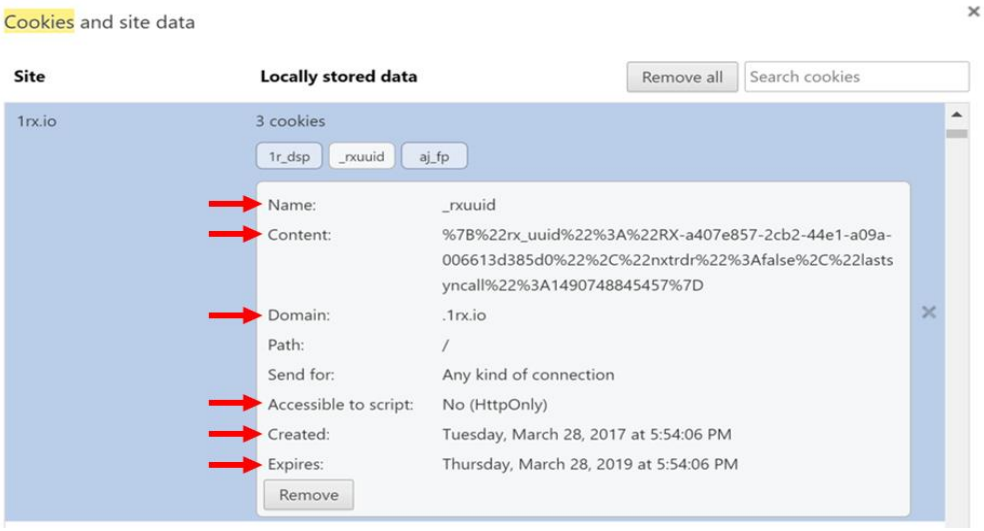

Figure 10-1 – Browser View of Cookies

History

The History SQLite database stores a user's past activity which can be divided into Downloads, History, and Searches.

History	URL	Full URL that was visited by the user
	Date Accessed	Date/time the URL was last visited
	Title	The title of the website visited (ie. Welcome to Facebook)
Downloads	Path	Location of file when downloaded **Note:** This provides you with the downloaded file's name and possible location within the image.
	URL	Full url that was visited by the user to accomplish download
	Date Accessed	Date/time of the download
Searches	Domain	URL where the search was made (ie. google.com, bing.com)
	Text	Text exactly as searched by the user
	Date Accessed	Date/time of the web search

Chrome

Chrome is one of the most commonly used open source web browsers. The browser automatically saves all user activity in all versions of Windows at:

`C:\Users\[username]\AppData\Local\Google\Chrome\User Data\Default`

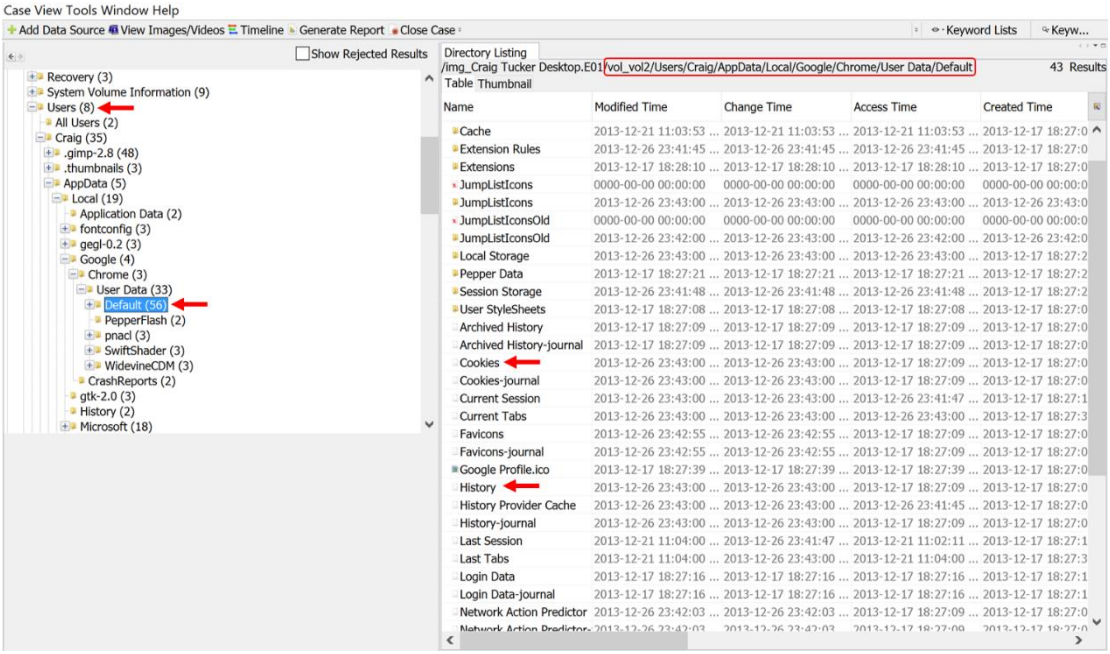

Figure 10-2 – Chrome Cookies and History Database

Internet Explorer

Internet Explorer is another popular web browser and is also the automatic default for Windows computers before Version 10. Being a Windows default, the browser's data is stored within:

`C:\Users\[username]\AppData\Local\Microsoft\Windows`

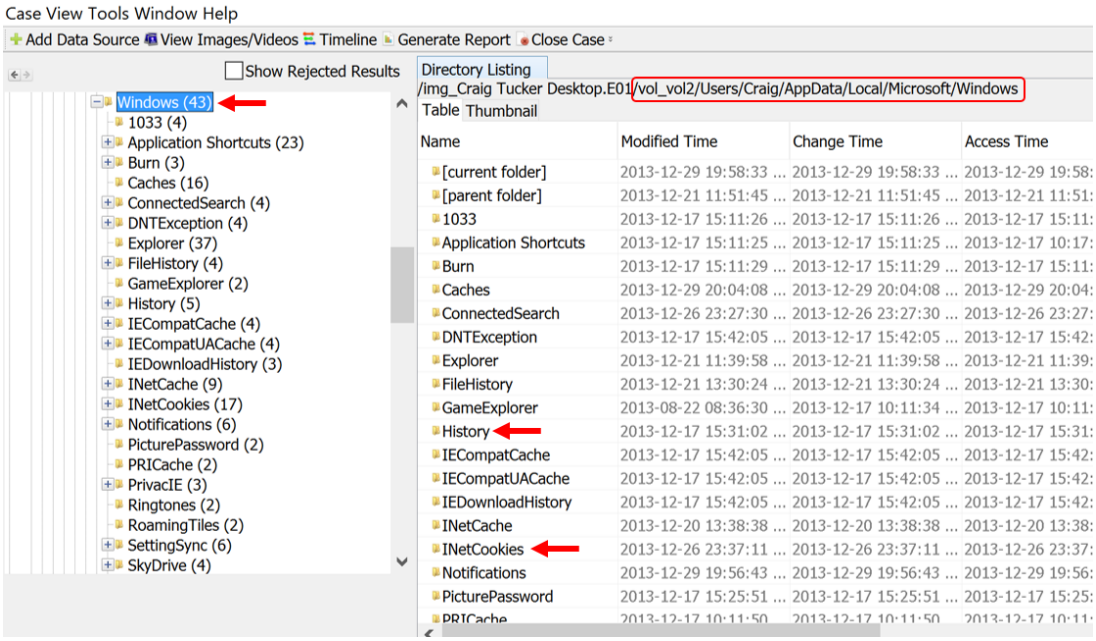

Figure 10-3 – Internet Explorer History and Cookies

SQLite View Example

Next, we will look at the SQLite information you can use to analyze a user's browser activity and how Autopsy makes investigations even easier with the "Extracted Content" window.

In Autopsy, you can view the data stored in SQLite databases by opening the Results view and using the arrows to move between entries. In bold text, at the top of each entry, you will see the word "Web" followed by either "Cookies", "History", "Downloads", or "Search". This tells you of which category the data is considered under (see Figure 10-4).

Note: The same procedure is followed for both Chrome and Internet Explorer browsers. However, this version of Autopsy is not pulling the Internet Explorer history into the Results view. You should always make sure to validate your software and see if it is pulling all the browser history information and determine if the user is using multiple browsers.

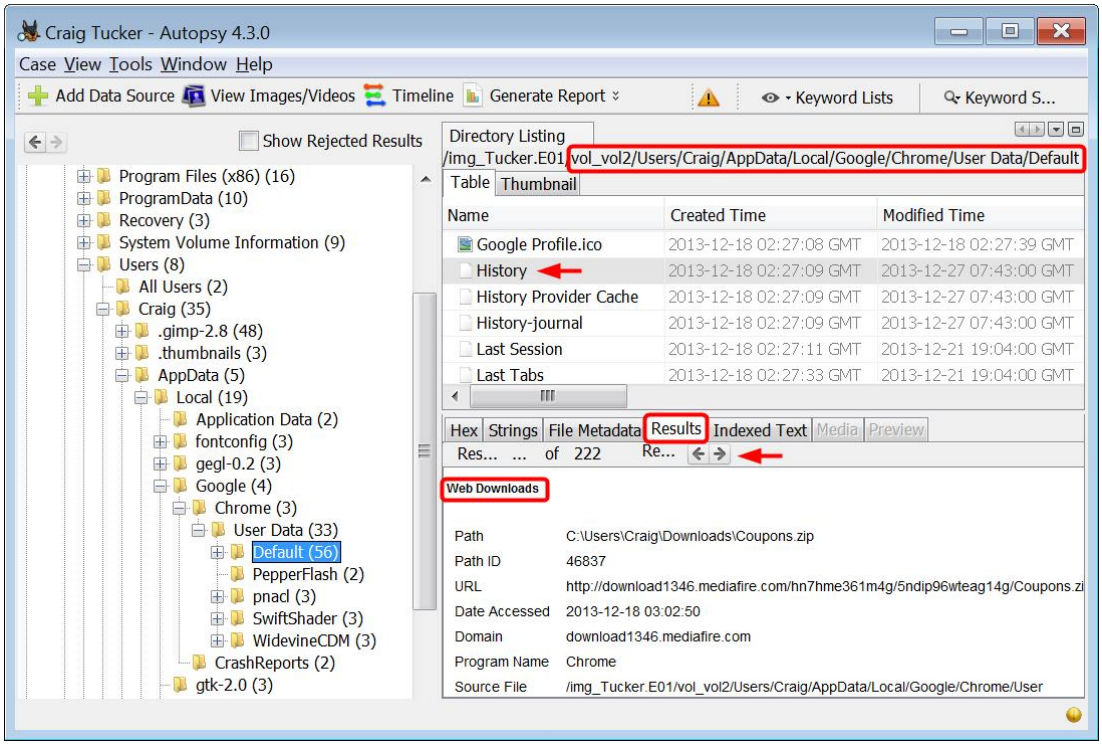

Figure 10-4 – Use Arrows in Results View for Chrome History

The Date/Time shown by Autopsy represents the Created date and time for Cookies as seen below. The Expired data and time are not stored along with whether the Cookie is Accessible to script.

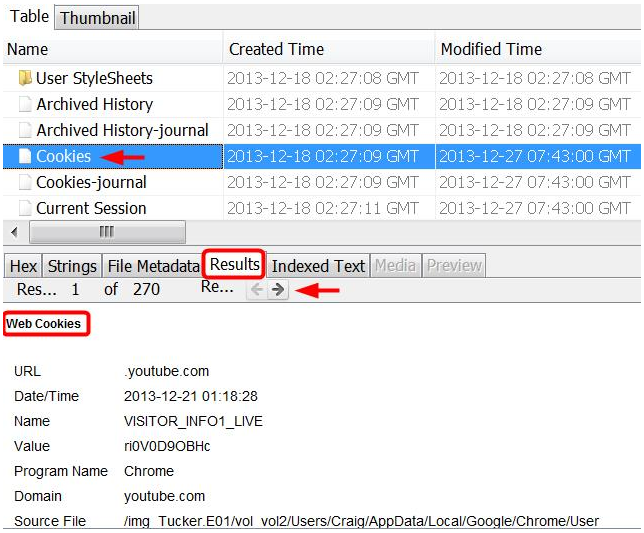

Figure 10-5 – Use Arrows in Results View for Chrome Cookies

Extracted Content View Example

Another way to view the SQLite data in Autopsy is through the Results\Extracted Content window, provided by the program. This window separates each entry into its own "Source File" and then places it within its category of "Web Cookies", "Web Downloads", "Web History", or "Web Search".

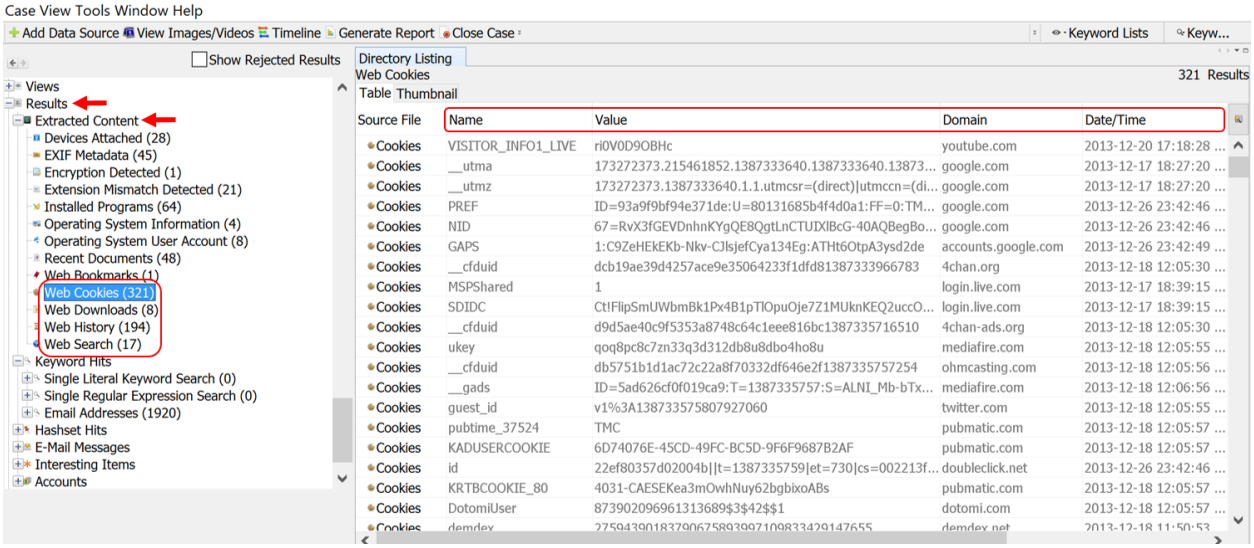

Figure 10-6 – Extracted Content View for Web Cookies, Downloads, History, and Search

Note: Under web history, you will see several entries for the website 4chan. People go to this site to post data anonymously to different boards. There are many boards where people will post inappropriate data, but also many fake coupons. People will post their fake coupons to this site so more people will use them and it will be harder to track down who created the coupons and all the people that use the coupons.