



Browser Forensics

Natan Eliezer
Chief Research Officer
Digital Forensics Association
Champlain College

Agenda



POSSIBLE
ARTIFACTS



POPULAR
BROWSERS



POWERFUL
TOOLS



INCOGNITO
MODE

Why care about browsers?

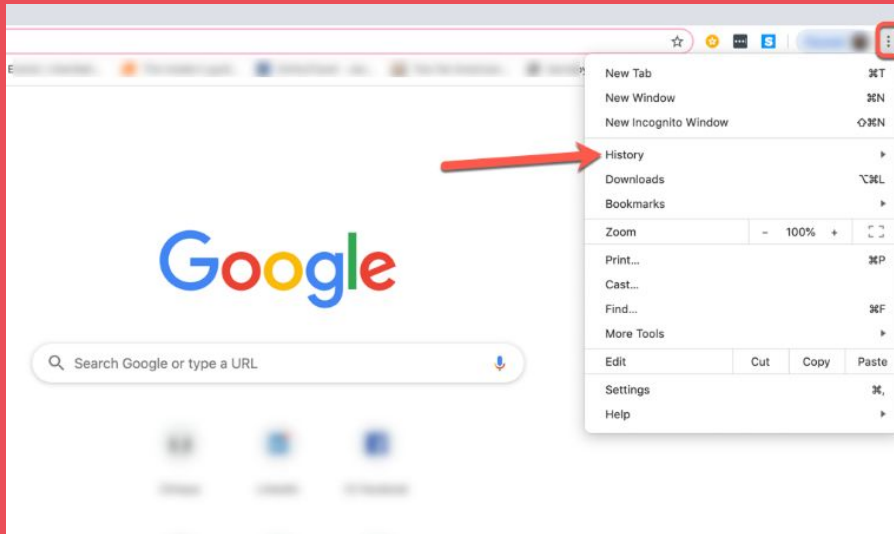
- It's how most people access the internet
- Used to establish common user activity
- TON of information within it





Common Artifacts

Browsing History

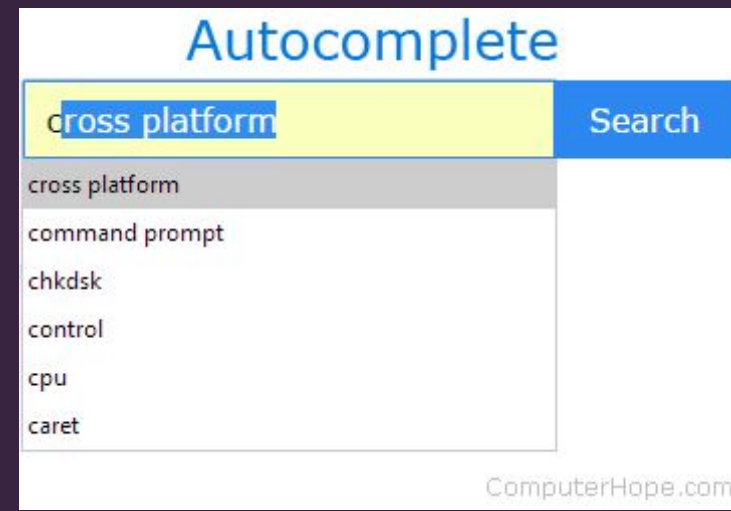


- Navigation History of a user
- Can be used to build a usage pattern of user
- Evidence a user visited a specific website
- Could be used to establish intent

Autocomplete Data

Search Autocomplete

- Information the browser suggests
- Based on common searches
- Commonly used with Browsing History



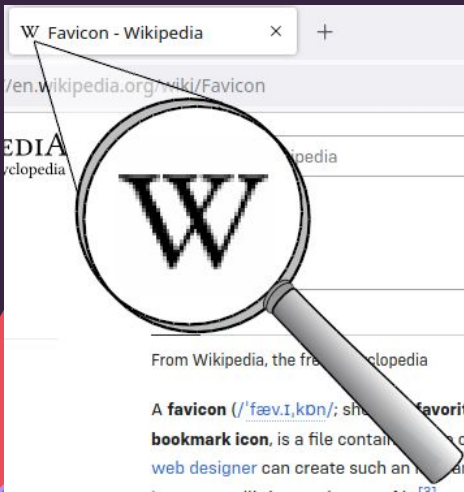
Form Autocomplete

- Data that is entered into forms
- Can be Name, Address, Phone number, etc



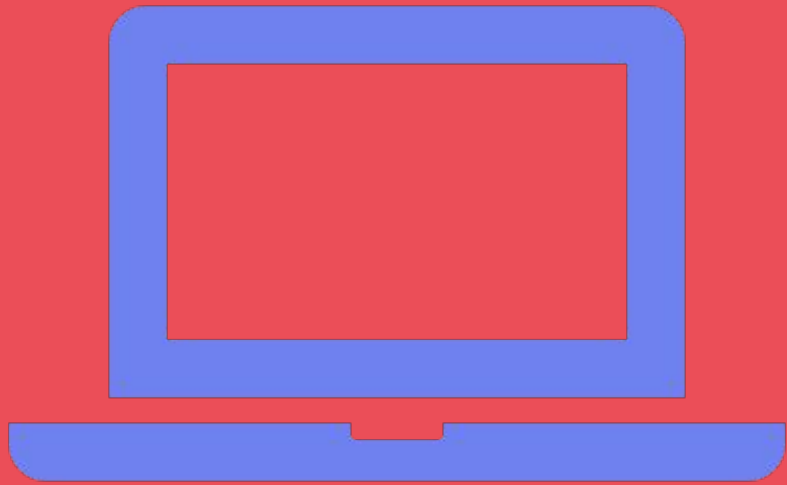
Cache

- Browsing data that is stored in memory
- Contains images, javascript files, etc
- Faster to load a webpage
-



Additional Artifacts

- Bookmarks
- Logins
- Downloads
- Extensions/Addons
- Browsing Sessions
- Thumbnails
- Favicons
- Custom Dictionary



Commonly used Browsers

Google Chrome



C:\Users\ %userprofile%\AppData\Local\Google\Chrome\User Data\

- Most data located in Default\ or ChromeDefaultData\
 - History
 - Cookies
 - Cache
 - Bookmarks
 - Web Data
 - Favicons
 - Login Data
 - Current Session/Current Tabs
 - Extensions
 - Thumbnails
 - Preferences
 - Downloads

Firefox

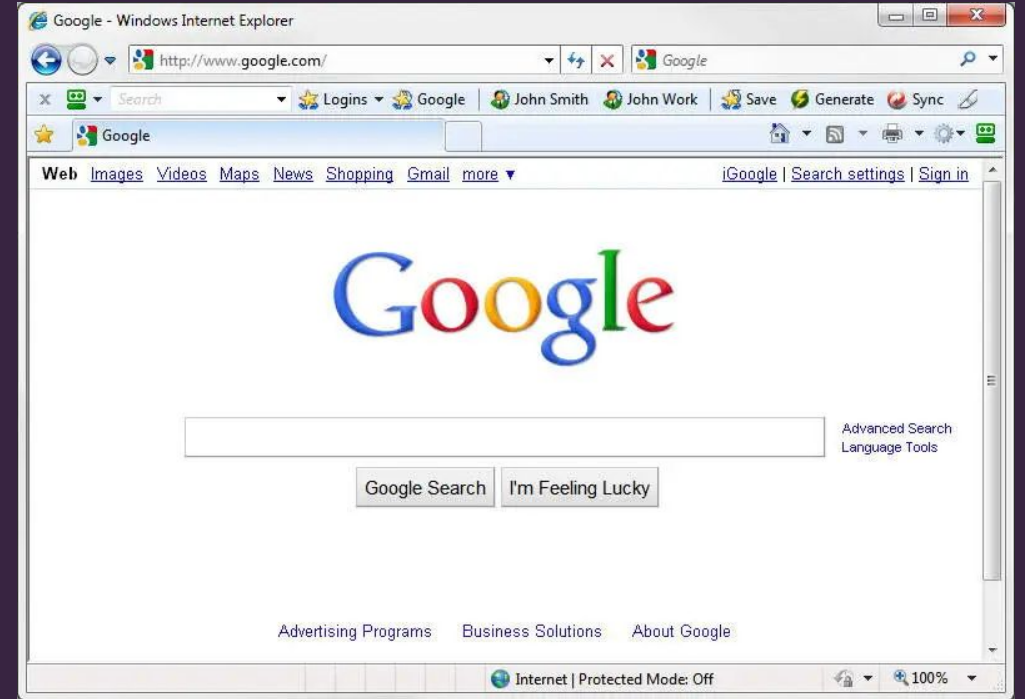


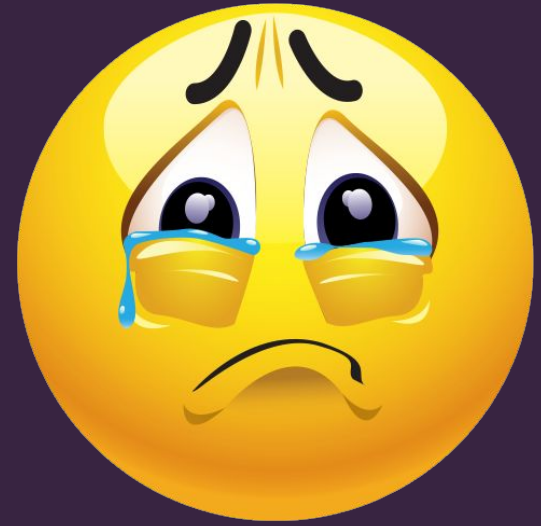
%userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\

- Places.sqlite
- Bookmarkbackups/
- Formhistory.sqlite
- Handlers.json
- Persdict.dat
- Addons.json/extensions.sqlite
- Cache2/entries or startupCache
- Favicons.sqlite
- Prefs.js
- Downloads.sqlite
- Thumbnails/
- Logins.json



Internet Explorer...







Moving on to Edge!

Microsoft Edge

- Based off Chromium
- Two locations
- C:\Users\<username>\AppData\Local\Microsoft\Edge\User Data\Default
- C:\Users\<username>\AppData\Local\Microsoft\Edge\User Data\Default\Cache

Format of Edge

JSON files


- Bookmarks
- Preferences
 - Site Settings

SQLITE

- Cookies
- Favicons
- Logins
- Thumbnails
 - 'Top sites'
- 'History'
 - 'Downloads'
 - Searches



Tools

- 
- BrowsingHistoryView
 - MZCookiesView
 - MozillaCacheView
 - SQLparse
 - Web Browser pass view
 - Hindsight

- ChromeHistoryView
- ChromeCookiesView
- ChromeCacheView
- Minitool data recovery

Many many more!





Incognito mode

How private is private browsing?



How does it work?

- Browsing data is “not saved” once session is closed
- Most data was stored in temporary files
- These files were deleted after the browser was closed
- Internet explorer, and Firefox both had evidence that could be investigated



What if I cleared my browsing
history?

You can still find data...

- Google chrome has a feature to sync history across multiple devices
- Browsers like Chrome and Firefox use sqlite databases to store history
 - There are ways to recover data from these types of files
- DNS cache
 - ipconfig /displaydns



Now for a demonstration!

(time permitting)



Sources

- <https://forensafe.com/blogs/microsoftedge.html>
- <https://usa.kaspersky.com/resource-center/definitions/cookies>
- <https://www.eastbaylawpractice.com/blog/2021/november/can-internet-search-history-be-used-against-you-/#:~:text=Your%20search%20history%20could%20also,to%20search%20your%20home%20computer.>
- https://www.nirsoft.net/web_browser_tools.html
- <https://focusinfotech.com/blog/browser-forensics/>
- <https://book.hacktricks.xyz/generic-methodologies-and-resources/basic-forensic-methodology/specific-software-file-type-tricks/browser-artifacts>
- <https://resources.infosecinstitute.com/topics/digital-forensics/browser-forensics-google-chrome/>
- <https://nasbench.medium.com/web-browsers-forensics-7e99940c579a>