

Building a Chrome Extension to Track Websites Visited

John Mikos, Iqra Rehman, Laura Adams, Eric Chan-Tin
Department of Computer Science, Loyola University Chicago

Abstract

Anonymity tools such as VPNs and Tor protect what you are browsing on the Internet. However, attackers can still see the packet sizes, which can then be used to predict the website. We created a web browser extension to record what websites users are visiting (both in regular HTTPS and using VPN/Tor) to see whether the website can be de-anonymized. We gained basic knowledge in JavaScript, jQuery, and the fundamentals of running and saving to a database. This project's aim is to collect data that can lead to better methods for anonymity on the web.

Motivation

- Packets are the information sent between computers that tell computers what to do.
- By tracing the size of packets, a previous study found that with one website's packet size information, you can predict the site correctly with more than 90% accuracy.
- Our group created a Google chrome extension that records the timestamp (in milliseconds), URL and tabID of multiple websites that are visited or closed.

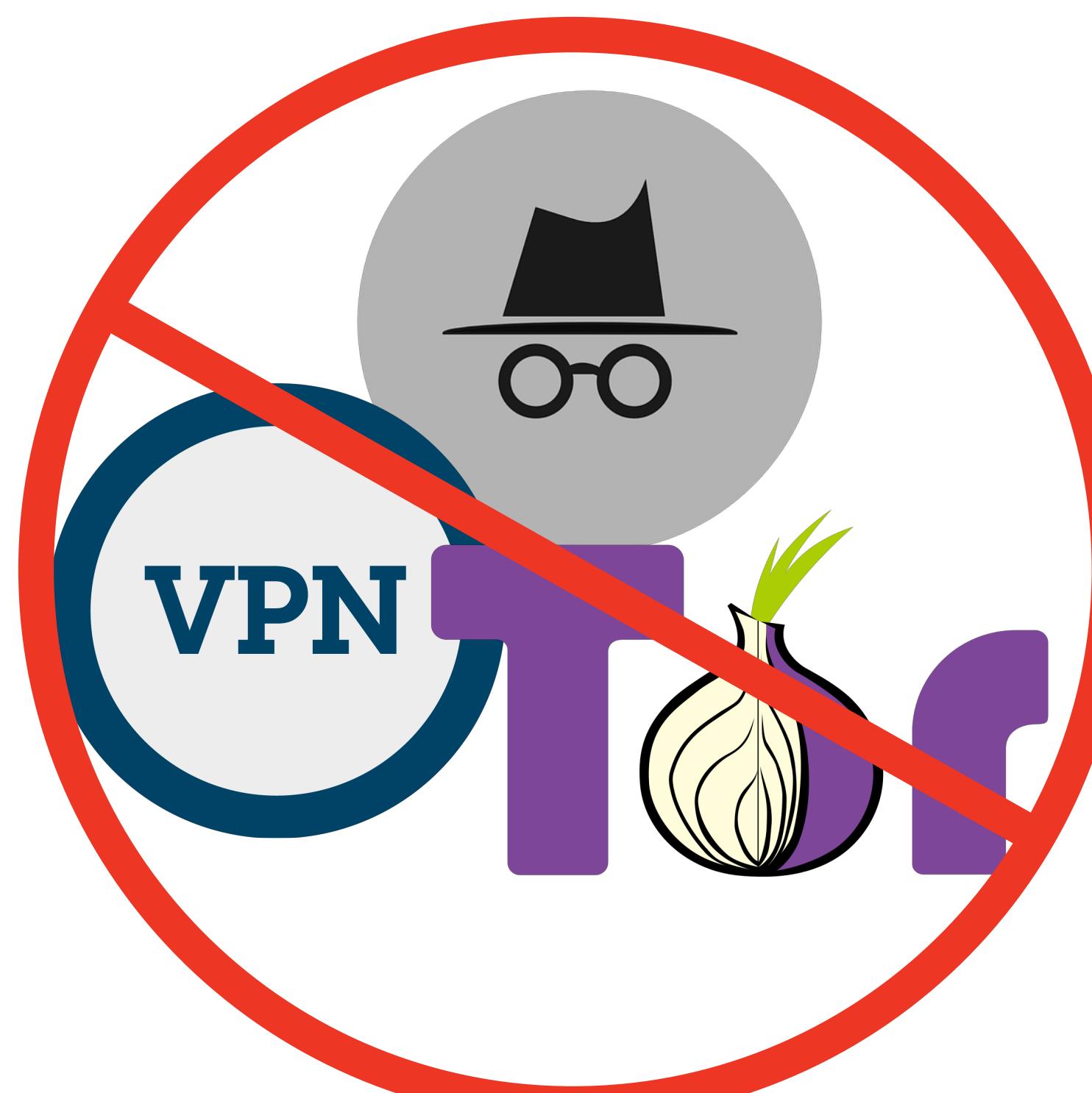


Fig 1. As long as you are on the web, **anyone** can track your activity... even if you are in 'incognito mode', have a VPN enabled, or are using a Tor anonymity network.

Think you're safe? **WT**
Think again.

Tracker in Progress

Web Tracker On

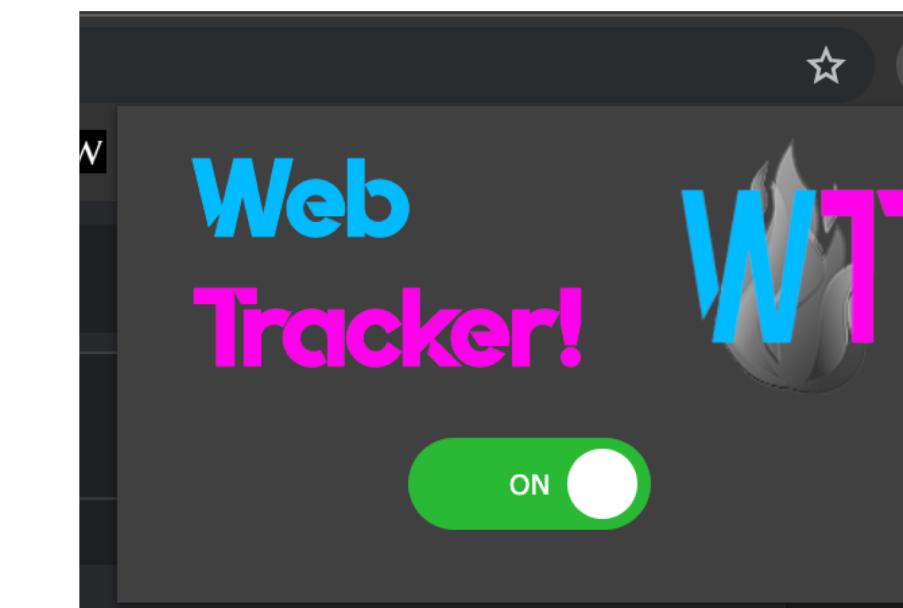


Fig 2. The extension is on and recording the user's data.

Web Tracker Off

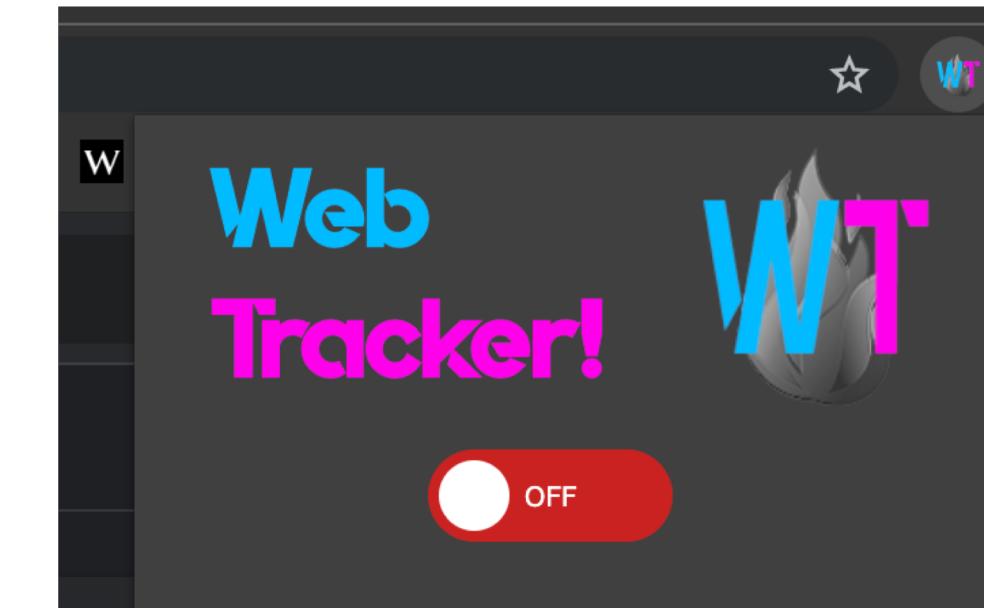


Fig 3. The extension is off and not recording the user's data.

Alert for website change

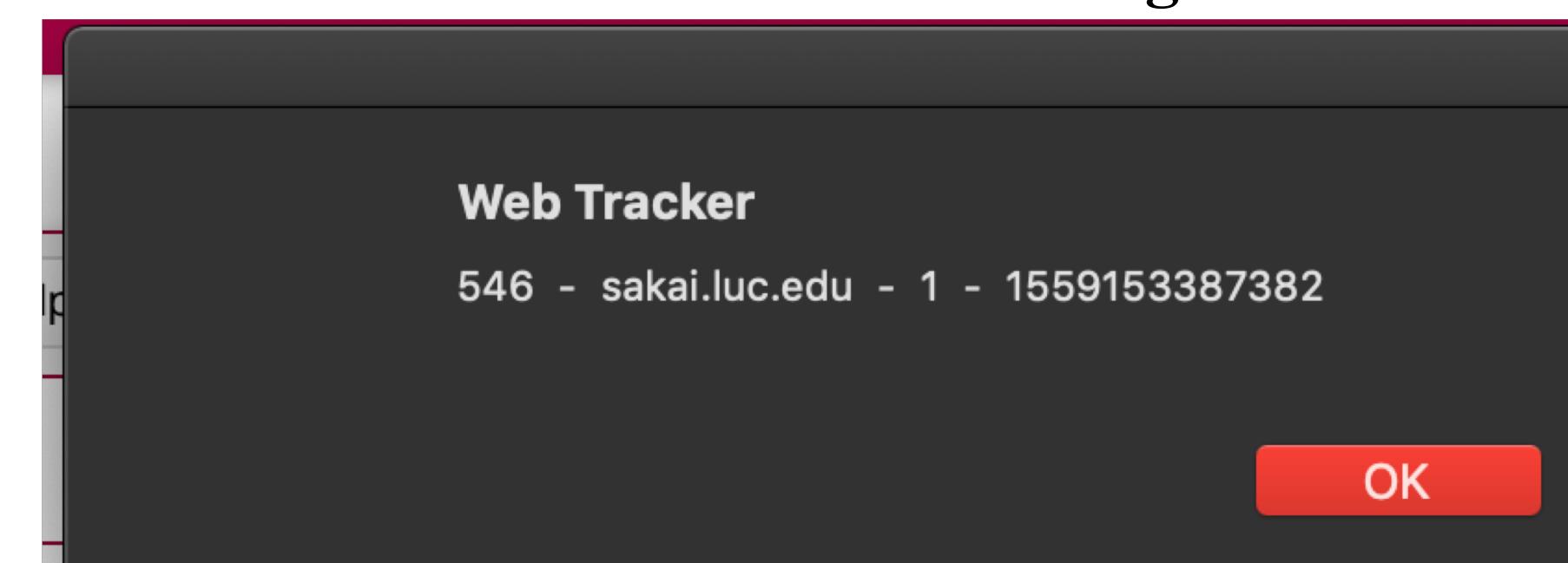


Fig 4. The user has changed websites and an alert has been issued with the following information: tabID – URL – open – Timestamp

Resources



Chrome's APIs were used to create browser extension to track data.



Used Linux to set up our database for data storage.



PHP was used to send the data to the server.



MySQL allowed us to store and access information.



jQuery for the data tracking switch.



HTML was used for structure and extension layout.

CSS for styling and friendly user interface. JavaScript was used to execute the extension and for data tracking.

Going Forward

In the future, we would like to use software to collect data on packet sizes and their distribution to analyze whether we can determine someone's activity across multiple sites on the web, which will later be used to deanonymize the data

Saving to Database

The goal of our group was to record the timestamp, URL, and tabID's of multiple websites that are visited once the tracker is turned on. The data was saved to a csv file using a database.

MySQL Database

Fig 5. Data saved to MySQL database using PHP

csv File

	A
1	796,youtube.com,1,1559140864539
2	802,youtube.com,1,1559140971727
3	796,youtube.com,0,1559141008560
4	796,google.com,1,15591410042341
5	

Fig 6. Exported saved data to an excel csv file

References

- Panchenko, A., Lanze, F., Zinnen, A., Henze, M., Pennekamp, J., Wehrle, K., and Engel, T. (2019). *Website Fingerprinting at Internet Scale*. [online] Research Gate. Available at: https://www.researchgate.net/publication/306097739_Website_Fingerprinting_at_Internet_Scale [Accessed 13 May 2019].
- MDN Web Docs. (2019). *Browser Extensions*. [online] Available at: <https://developer.mozilla.org/en-US/docs/Mozilla/Add-ons/WebExtensions> [Accessed 15 May 2019].
- Developer.chrome.com. (2019). *Chrome APIs - Google Chrome*. [online] Available at: https://developer.chrome.com/extensions/api_index [Accessed 13 May 2019].