Lucerne University of Applied Sciences – Computer Science
Scientific Writing & Research Methods (WSFM)
Fall 2025

Research Proposal

Website Fingerprinting in the Tor Network: Reproduction and Evaluation under Simulated Laboratory Conditions

Oliver LASTNAME
Group 2

Supervisor:

February 20, 2026

Contents

1 Background, Problem Statement, and Objectives

When browsing the internet, user traffic is typically encrypted through HTTPS. However, Internet Service Providers (ISPs) can still observe the IP addresses of connection attempts, thereby identifying which websites and services a user accesses. Furthermore the websites themselves can see what IP addresses are accessing them. To mitigate this visibility, several privacy-enhancing technologies exist, one of them is Tor.

The Tor Network is a decentralized communication service anonymizing internet traffic by encapsulating traffic in onion like layered packages. The traffic is then routed through three nodes which all peel off / decrypt one layer of the package. Therefore the nodes will never know both the sender and the target of the package. (TorNews, 2025)

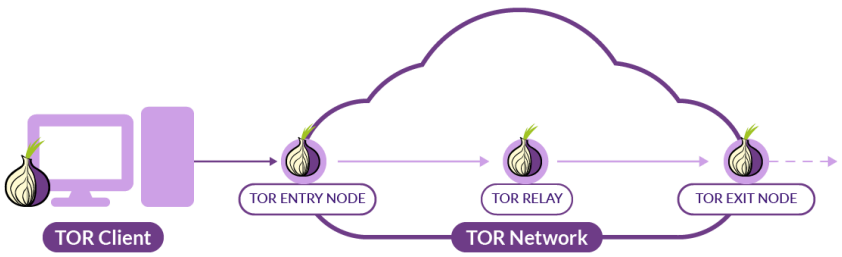

Figure 1: Overview of the Tor network architecture (Sysdig, 2024)

The Tor Network is used by journalists, whistleblowers and activists to circumnavigate censorship and surveillance. However it is also used by criminals of all sort to avoid the justice system. (TorNews, 2025)

As a result several techniques have been developed to deanomyze Tor Network users. One of them is called Website Fingerprinter or FW. The Objective of this Paper is to describe the process and the working of FW.

2 Research Questions and Methods

To what extent can the Deep Fingerprinting attack be reproduced in a Shadow-simulated Tor network, and how does classification accuracy compare to results reported on live Tor traffic?

3 Personal Reflection

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aeque doleamus animo, cum corpore dolemus, fieri tamen permagna accessio potest, si aliquod aeternum et infinitum impendere malum nobis opinemur. Quod idem licet transferre in voluptatem, ut postea variari voluptas distinguique possit, augeri amplificarique non possit. At.

4 Literature Review

4.1 Deep Fingerprinting (Sirinam et al., 2018)

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aeque doleamus animo, cum corpore dolemus, fieri tamen permagna accessio potest, si aliquod aeternum et infinitum impendere malum nobis opinemur. Quod idem licet transferre in voluptatem, ut postea variari voluptas distinguique possit, augeri amplificarique non possit. At.

4.2 Data-Explainable Website Fingerprinting (Jansen et al., 2023)

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aeque doleamus animo, cum corpore dolemus, fieri tamen permagna accessio potest, si aliquod aeternum et infinitum impendere malum nobis opinemur. Quod idem licet transferre in voluptatem, ut postea variari voluptas distinguique possit, augeri amplificarique non possit. At.

4.3 Research Methods Literature

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aeque doleamus animo, cum corpore dolemus, fieri tamen permagna accessio potest, si aliquod aeternum et infinitum impendere malum nobis opinemur. Quod idem licet transferre in voluptatem, ut postea variari voluptas distinguique possit, augeri amplificarique non possit. At.

Bibliography

Sysdig. (2024,). *Detect Tor Network Connection with Falco*. https://www.sysdig.com/blog/detect-tor-network-connection-falco

TorNews. (2025,). *What is Onion Routing? The Complete 2026 Guide - TorNews*. https://tornews.com/deep-web/guides/what-is-onion-routing/

References

Appendix: Assignment