Lucerne University of Applied Sciences and Arts

Practical De-Anonymization in the Tor Network

Timing Leaks, Traffic Correlation, and Website Fingerprinting

Bachelor Thesis

Study Program: Information & Cyber Security

Oliver TODO
Zürich (Switzerland)

Defense Date: TODO
Defense Location: Rotkreuz

Supervisor: TODO
External Expert: TODO
Industry Partner: TODO

2026

Abstract

The content of your thesis in brief.

Contents

1 Problem Statement, Research Questions, and Vision

1.1 Problem Statement

The Tor network is widely considered secure, yet theoretical studies demonstrate that timing analyses and traffic correlation attacks can compromise user anonymity. However, practical investigations under controlled, local conditions remain scarce.

1.2 Research Questions

1. Can Website Fingerprinting attacks successfully de-anonymize Tor users in a locally simulated Shadow network?
2. To what extent do Tor's built-in circuit padding mechanisms reduce detection accuracy of such attacks?
3. What bandwidth and latency overhead do these defenses introduce?

1.3 Vision

2 State of Research

2.1 The Tor Network

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 have been developed, one of them being Tor.

The Tor Network is a decentralized communication service anonymizing internet traffic by encapsulating traffic in onion like encrypted layers. The traffic is then routed through three nodes which all decrypt one layer of the package. Therefore no single node learns both the origin and the destinationnd of the package. (TorNews, 2025)

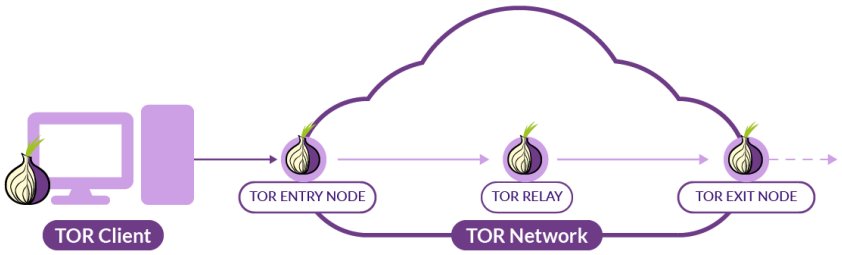

Figure 1: Overview of the Tor network architecture (Sysdig, 2024)

The Tor Network is used by journalists, whistleblowers and activists to circumvent censorship and surveillance. However it is also used by malicious actors of all sort to evade law enforcement. (TorNews, 2025)

As a result several techniques have been developed to de-anonymize Tor Network users. One of them is called Website Fingerprinter or WF.

In a WF attack, a passive observer — such as an ISP or a compromised entry node — analyses patterns in the encrypted traffic from the user, and compares against pre-recorded fingerprints from known webistes.(Juarez et al., 2014). Some of the compared patterns include

such as packet sizes, timing, and direction, to infer which website a Tor user is visiting. Over the past decade, various WF approaches have been proposed,

ranging from statistical classifiers to deep learning models, with varying degrees of success. This proposal aims to survey these approaches and compare them with respect to the traffic features they exploit and the classification accuracy they achieve.

This chapter reviews existing research on Tor anonymization, website fingerprinting attacks, traffic analysis techniques, and circuit padding defenses.

2.2 WF Attack

3 Ideas and Concepts

4 Method(s)

4.1 Phase 1: Shadow Network Setup

Tor network simulation using Shadow/tornettools, Wikipedia mirror cloning, and wget2-based client configuration.

4.2 Phase 2: Baseline Data Collection

Packet capture and feature extraction from client nodes; training and evaluation of WF classifiers (e.g.
Deep Fingerprinting CNN).

4.3 Phase 3: Circuit Padding Activation

Configuration of Tor's built-in padding mechanisms at various levels and corresponding data collection.

4.4 Phase 4: Comparison and Analysis

Comparative analysis of detection rates with and without padding, overhead measurement, and trade-off quantification.

5 Implementation

5.1 Baseline WF Attack Results

5.2 Circuit Padding Configuration

6 Validation and Evaluation

6.1 Performance Overhead

6.2 Limitations

7 Outlook

7.1 Ethical Considerations

Reflection on ethical aspects of the research.

7.2 Future Work

8 Appendices

8.1 Task Description

8.2 Project Management

9 Lists of Abbreviations, Figures, Tables, AI Tools, and Formulas

9.1 List of Abbreviations

HSLU — Lucerne University of Applied Sciences and Arts
Tor — The Onion Router
WF — Website Fingerprinting
ISP — Internet Service Provider
NN — Neural Network
IDS — Intrusion Detection System

9.2 List of Figures

9.3 List of Tables

9.4 AI Tools Declaration

10 Bibliography

Juarez, M., Afroz, S., Acar, G., Diaz, C., & Greenstadt, R. (2014). A critical evaluation of website fingerprinting attacks. *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 263–274. https://dl.acm.org/doi/pdf/10.1145/2660267.2660368

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/