|  |
| --- |
| **Ime: Klemen**  **Priimek: Jeršin**  **Vpisna št: 6419023**  **Datum: 21.12.2022** |

**Odjemalec Tor in delovanje sistema**

# Namen

Namen vaje je spoznati delovanje sistema Tor za anonimen dostop do spleta. Omrežje Tor je prekrivno omrežje (angl. Ovelay network), ki ga sestavljajo vozlišča Tor (relay) in odjemalske aplikacije (Tor browser). Z rabo odjemalca Tor prek omrežja Tor se prikrije naslov IP, s katerim spletni odjemalec komunicira s spletnim strežnikom. Na ta način Tor omogoča anonimnost oz. zasebnost pri dostopu do spletnih storitev.

Pri vaji se bomo seznanili s protokolom Onion routing, preučili arhitekturo (odjemalci, relay, bridge, exit relay) in topologijo omrežja Tor ter preverili, kakšen vpliv na omrežno povezljivost ima raba Tor za dostop do interneta.

# Potek vaje

Pred začetkom vaje namestite aktualno inačico spletnega brskalnika Tor z naslova [https://www.torproject.org/download/download-easy.html.en.](https://www.torproject.org/download/download-easy.html.en)

## 1.1 Usmerjanje prometa

V navadnem spletnem brskalniku (ne Tor!) odprite spletno stra[n http://www.yougetsignal.com/whatis-my-ip-address/](http://www.yougetsignal.com/what-is-my-ip-address/) in preverite spletni naslov, s katerim se predstavljate spletnim strežnikom.

Nato z ukazom tracert (ukazna vrstica) določite usmerjevalnike na poti med vašim in računalnikom na naslovu [www.yougetsignal.com.](http://www.yougetsignal.com/) Z geo-lokacijo (preslikava naslova IP v približno lokacijo) določite okvirne lokacije in pot prerišite v priloženi zemljevid.

Spletno stran <http://www.yougetsignal.com/what-is-my-ip-address/>odprite še v brskalniku Tor in preverite spletni naslov, s katerim se sedaj predstavljate spletnim strežnikom.

Kaj lahko ugotovite glede izvornih IP naslovov v enem in drugem primeru?

|  |
| --- |
|  |

S klikom na ikono preverite sekvenco vozlišč (angl. Circuit) v prekrivnem (overlay) omrežju Tor, prek katerih trenutno tunelirate svoj dostop do spleta. Približno pot (geolokacije vozlišč Tor in povezave med njimi) za to spletno sejo vrišite v zemljevid (zadnja stran).

Slika, ki vsebuje besede besedilo

Opis je samodejno ustvarjen

## 1.2 Topologija omrežja Tor

Na stran[i https://check.torproject.org/ p](https://check.torproject.org/)reverite naslov IP trenutnega izhodnega vozlišča in prek orodij na <https://metrics.torproject.org/rs.html> preverite njegove podrobnosti. Kateri podatki se vam zdijo pomembni za ocenjevanje zanesljivosti nekega vozlišča v Tor?

|  |
| --- |
| Pomembna podatka sta Advertised Bandwidth in Flags. |

S podatki na straneh <https://metrics.torproject.org/networksize.html>si oglejte podatke o aktualnem številu vozlišč Tor. Poiščite še podatek o približnem številu usmerjevalnikov v Internetnem omrežju IP in primerjajte števili obeh omrežnih elementov.

|  |
| --- |
| Releyev je veliko več kot bridgov |

Kakšna je razlika med vozlišči (internal) relay, exit relay in bridge relay.

|  |
| --- |
| Internal relay povezuje vozlišča med seboj, exit relay je končno vozlišče pred uporabnikom,  Bridge relay so vstopna vozlišča z neznanim IP naslovom. |

## 1.3 Sekvence vozlišč (angl. Circuit)

Kaj povzroči izvedba ukaza »New Tor Circuit for this Site? Primerjajte in komentirajte sekvenci za dve različni spletni strani, ki jih odprete v brskalniku Tor.

|  |
| --- |
| Tor browser nam dodeli nam nova vozlišča, pri čemer Guard večinoma ostane isti. |

## 1.4 Analiza prometa Tor

Z orodjem Wireshark zajemite promet, ki pripada HTTP zahtevi in odgovoru ob dostopanju do strani [http://test.ltfe.org,](http://test.ltfe.org/) ter zabeležite podate o vseh vozliščih v sekvenci vozlišč, kot jih podaja brskalnik Tor.

|  |
| --- |
|  |

Iz podatkov v sledi prometa Wireshark ugotovite, s katerim naslovom IP si pri dostopu do te spletne strani datagrame dejansko izmenjuje vaš računalnik.

Nastavite prikazovalni fliter v Wiresharku tako, da prikazuje le promet do ugotovljenega računalnika:

|  |
| --- |
| ip.dst == 192.168.1.6 |

Zapišite, katere aplikacijske protokole pri tem uporablja, in pojasnite opažanja.

|  |  |
| --- | --- |
| Uporablja TLSv1.2 in TCP protokola. TLSv1.2 protokol skrbi za enkripcijo povezave, kar je tudi glavna funkcija TOR brskalnika oziroma omrežja. |  |

## 1.5 Ocena zakasnitve pri rabi Tor

Ocenite velikost dodatne zakasnitev (ali RTT), ki jo v komunikacijo vnesemo na račun rabe omrežja Tor. Primerjamo seveda zakasnitve end-to-end, torej med našim računalnikom in izbranim ciljnim.

Oceno opravite tako, da iste spletne strani odpirate v navadnem in brskalniku Tor. Čas, ki ga potrebujete za izvedbo celotnega HTTP zahtevka in dostavo vsebine odjemalcu pa ugotovite s pomočjo razvijalskih orodij v obeh brskalnikih:

 Web Developer > Network

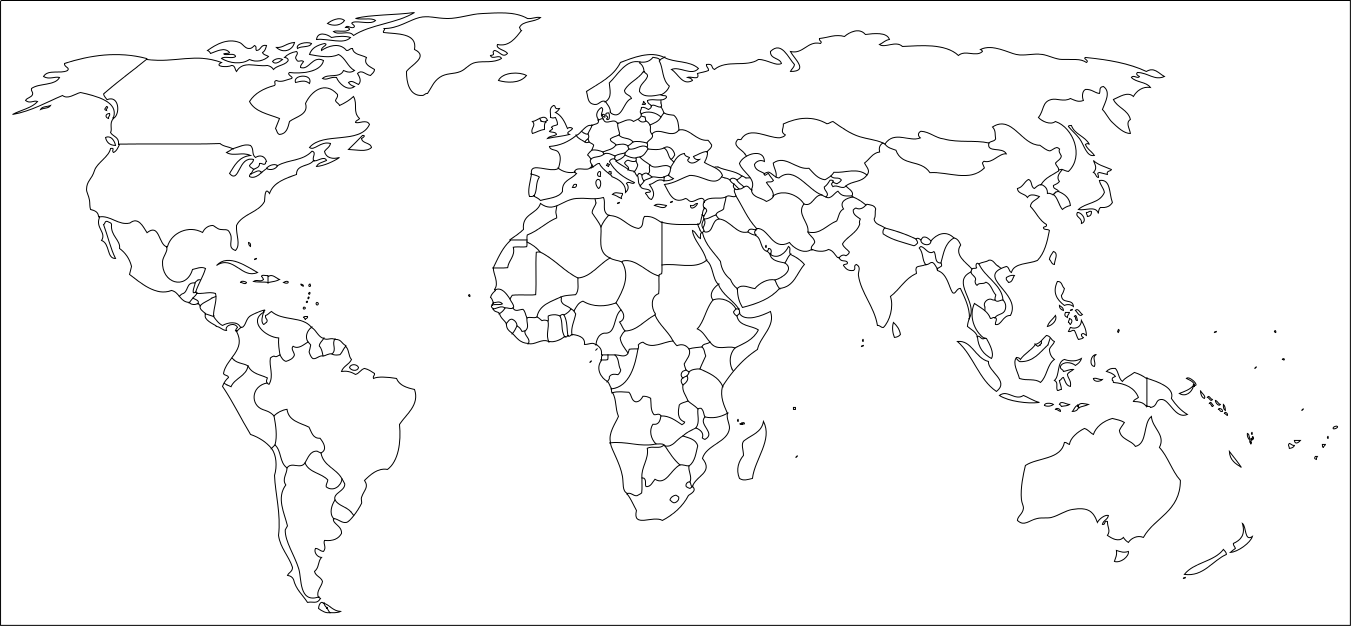
Meritev opravite za dve različni spletni strani, pri treh različnih sekvencah vozlišč in jo v vsakem primeru ponovite trikrat.

Tabela: Primerjava in ocena celotnih zakasnitve pri rabi Tor

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **URL 1:**  **test.ltfe.org** |  | **URL 2: www.google.com** |  |
| **Tor** | **Firefox** | **Tor** | **Firefox** |
| **Circuit 1** | 1589ms | 25ms | 2010ms | 148ms |
| 2725ms | 39ms | 2210ms | 154ms |
| 1504ms | 44ms | 1980ms | 208ms |
| **Povprečje [ms]:** | 1939 | 36 | 2066 | 170 |
| **Circuit 2** | 588ms |  | 2760ms |  |
| 2178ms |  | 2777ms |  |
| 1344ms |  | 2560ms |  |
| **Povprečje [ms]:** | 1370 |  | 2699 |  |

Komentirajte rezultate:

|  |
| --- |
| Tor ima pričakovano višje zakasnitve kot navaden brskalnik, saj morajo podatki čez vse relay-e. |





5