

# **Text laboratórnej úlohy**

Laboratórna úloha č. 11

## **ANONYMIZAČNÉ SIETE**

# Úvod k laboratórnej úlohe

Cieľom laboratórnej úlohy je oboznámiť študentov s použitím anonymizačných sietí, ich významom v oblasti ochrany súkromia a bezpečnosti online komunikácie a ozrejmiť im základné princípy ich fungovania, pričom hlavná pozornosť bude venovaná **anonymizačnej sieti Tor** (z angl. *The Onion Routing*), ktorá využíva pre zaistenie dôvernosti, anonymity užívateľov a utajenia komunikácie medzi účastníkmi techniku tzv. cibulového smerovania (*onion routing*). V rámci laboratórnej úlohy budú preto vysvetlené základné princípy fungovania a účel použitia anonymizačných sietí, ďalej bude predstavený hlavný koncept celosvetovo známej anonymizačnej siete Tor a taktiež bude objasnené použitie vrstvomého smerovania v tomto type sietí.

V praktickej časti sa študenti budú venovať inštalácii a konfigurácii nástroja Tor v prostredí Kali Linux, prehliadaniu internetu prostredníctvom Tor siete a analýze sieťovej komunikácie pomocou nástroja Wireshark. Študenti tak nadobudnú praktické zručnosti v oblasti anonymizácie internetovej komunikácie a naučia sa analyzovať tok dát v prostredí anonymizačných sietí.

## Požiadavky pre vypracovanie úlohy:

- software: VMware Workstation Player pre virtualizáciu staníc,
- virtuálne stroje: dva, resp. tri virtuálne stroje s Kali Linux.

## 1. Teoretický úvod

V tejto laboratórnej úlohe venovanej problematike anonymizačných sietí sa zoznámite so základnými princípmi fungovania anonymizačných sietí, ich základnou štruktúrou a tiež s procesom tzv. viacvrstvomého („cibulového“) šifrovania, ktoré je typické práve pre dosiahnutie anonymity klientov, resp. komunikujúcich koncových zariadení prostredníctvom anonymizačných sietí.

### 1.1. Anonymizačné siete

**Anonymizačné siete** predstavujú pokročilejšie bezpečnostné technológie navrhnuté a používané za účelom **ochrany identity používateľov a ich súkromia** v digitálnom prostredí dnešných počítačových sietí. Jedná sa o špeciálne typy sietí navrhnuté za účelom ochrany identity a polohy používateľov, ktoré umožňujú prostredníctvom šifrovania informácií obsiahnutých v prenášaných dátových jednotkách **zaistiť anonymné prehliadanie internetu**, resp. komunikáciu, a tým i **ukrytie identity** prístupujúcich užívateľov (resp. zariadení) naprieč rozsiahlym konglomerátom vzájomne prepojených sietí. Ich cieľom je minimalizovať možnosť sledovania zdrojovej IP adresy, lokalizácie či iných identifikačných údajov používateľa. Medzi najznámejšie

anonymizačné siete patria napríklad **Tor**, **I2P**, **Freenet** a i. V tejto úlohe bude najväčšia pozornosť venovaná primárne anonymizačnej sieti Tor (*The Onion Router*).

## 1.2. Tor (The Onion Router)

Tor predstavuje projekt vyvíjaný s cieľom poskytnúť užívateľom možnosti anonymného vystupovania a komunikácie v digitálnom prostredí internetu. Je založený na **princípe tzv. „cibuľového“ smerovania (*onion routing*)**, kde komunikácia medzi klientom a cieľovým serverom prebieha cez sériu náhodne vybraných sprostredkovateľov nazývaných „Tor relé“ (typicky sa jedná o medziľahlé smerovače na prenosovej trase). Každý takýto medziľahlý uzol pozná len bezprostredne predchádzajúci a ďalší nasledujúci bod komunikácie, vďaka čomu je možné zamedziť úplné sledovanie priebehu celej komunikácie, a to vrátane informácií o koncových bodoch. Anonymizačná sieť Tor je navrhnutá tak, aby bolo možné:

- zabezpečiť anonymitu klienta voči cieľovej službe,
- napr. v prípade tzv. skrytých služieb zabezpečiť taktiež anonymitu cieľa voči klientovi,
- zamedziť tretím stranám (napr. poskytovateľom internetového pripojenia, prevádzkovateľom Wi-Fi sietí apod.) získať prehľad o tom, aké stránky používateľ navštevuje alebo s kým pri prístupe do siete komunikuje.

### Architektúra Tor siete

Pre ďalší popis a vysvetlenie princípov tzv. „cibuľového“ smerovania sú dôležité dva základné pojmy: **vrstvy a uzly**. Pri smerovaní dátových jednotiek (tzv. buniek) smerom k adresátovi s využitím „cibuľového“ smerovania každý medziľahlý uzol podieľajúci sa na komunikácii (resp. smerovaní) vždy dešifruje len jednu „vrstvu“ aplikovaného šifrovania. Po dešifrovaní, t. j. odstránení vonkajšej vrstvy sa odhalí ďalšia nasledujúca adresa na trase k príjemcovi dátovej jednotky, iné však zostávajú stále chránené, utajené šifrovaním, čo predstavuje základný mechanizmus pre zaistenie anonymity užívateľov (resp. jednotlivých uzlov, zariadení).

Typická sieť Tor pozostáva z nasledujúcich **základných komponentov (uzlov)**:

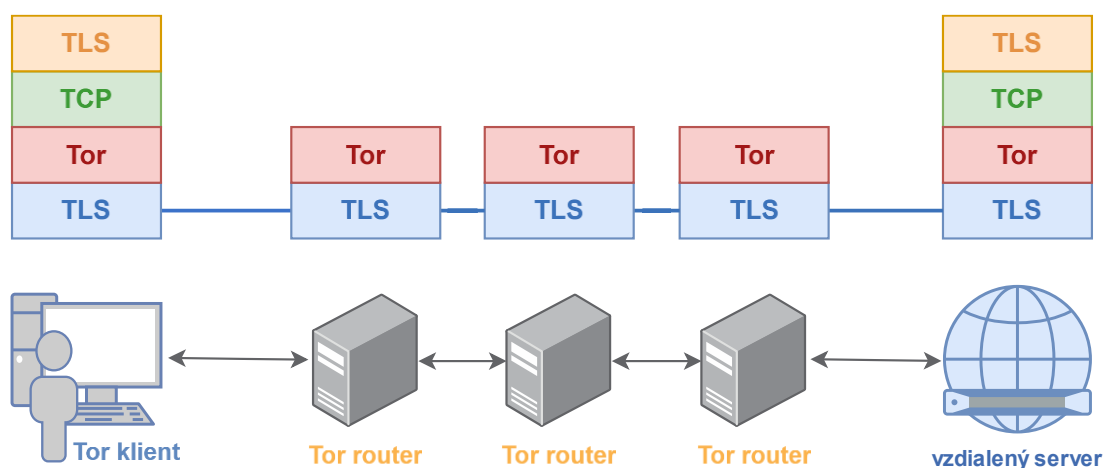
- **Tor klient** – aplikačné rozhranie na strane používateľa využívajúceho možnosti anonymného prehliadania, typicky v podobe Tor prehliadača alebo systémového démona **tor**.
- **Tor smerovače (*Tor relays, onion routers*)** – medziľahlé uzly (spravidla smerovače), ktorých úlohou je smerovanie dátových jednotiek (buniek) v Tor sieti. Rozlišujeme:
  - **vstupný uzol (*Entry Node*)** – prvý bod (uzol) v komunikačnej sieti, kde po prvýkrát dochádza k šifrovaniu prenášaných dát;

- **relé uzly (*Relay Nodes*)** – medziľahlé<sup>1</sup> uzly, ktoré prenášajú šifrované dáta, resp. postupne ich (de)šifrujú pomocou svojich kľúčov pre šifrovanie, resp. dešifrovanie;
- **výstupný uzol (*Exit Node*)** – posledný bod v sieti, kde sú dáta dešifrované a odoslané na cieľovú adresu (prijemcovi);
- **Adresárové servery** – centrálné uzly, ktoré spravujú zoznam dôveryhodných Tor smerovačov a poskytujú informácie o dostupných uzloch ostatným prvkom v Tor sieti.

### Princíp šifrovania v anonymizačnej sieti

Mechanizmy siete Tor používané pre zaistenie anonymity používateľov sú aplikované na úrovni sieťovej vrstvy, ako ju poznáme zo sieťového modelu TCP/IP. Celková architektúra siete Tor pozostáva z nasledujúcich vrstiev:

- **Linková vrstva** – je realizovaná TLS spojmami medzi jednotlivými prvkami Tor siete, kde protokol TLS zohráva zásadnú úlohu pri autentizácii prvkov a pri ochrane dôvernosti a integrity prenosov. Každý individuálny úsek komunikácie medzi dvoma susednými uzlami (napr. klient ↔ OR1) je zabezpečený samostatným TLS tunelom.
- **Sieťová vrstva** – je realizovaná protokolom Tor, ktorý zaisťuje vytváranie a následný prenos a smerovanie buniek, vrátane ich šifrovania.
- **Transportná vrstva** – za účelom spoľahlivosti prenosu a možnosti šifrovania pomocou TLS využíva spojovo orientovaný a spoľahlivý protokol TCP.
- **Aplikačná vrstva** – pozostáva z klientskych aplikácií na strane koncového používateľa využívajúcich transportný protokol TCP (napr. HTTP, FTP).



Obrázok 1.1 Vrstvová architektúra siete Tor<sup>2</sup>.

<sup>1</sup> Tieto medziľahlé *relay* uzly sú sprostredkovateľmi prenosu šifrovanej dátovej komunikácie medzi odosielateľom a prijemcom využívajúcich anonymizačnú sieť Tor.

<sup>2</sup> Prevzaté z oficiálnych výučbových materiálov k prednáškam predmetu MPC-NSB – vypracoval garant predmetu a prednášajúcim doc. Karel Burda, CSs. (viď tiež E-learning predmetu).

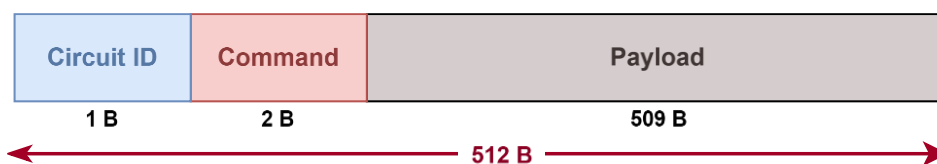
V sieti Tor prebieha komunikácia vo forme **buniek (cells)**, ktoré predstavujú základnú jednotku prenosu dát medzi klientom a uzlami v sieti. Každá bunka má **fixnú veľkosť 512 bajtov**. Nemenná veľkosť bunky umožňuje minimalizovať možnosť analýzy komunikácie na základe veľkosti prenášaných dátových jednotiek. Všetky správy, bez ohľadu na ich skutočný obsah alebo dĺžku, sú preto zapuzdrené do rovnako veľkých buniek, čím sa znižuje riziko, že by pozorovateľ (typicky útočník) mohol identifikovať vzorce komunikácie alebo konkrétny typ dát.

Tor bunky možno rozdeliť podľa účelu ich použitia na viacero typov. Napríklad:

- **Bunky typu CREATE a CREATED** sa používajú pri vytváraní šifrovaného okruhu medzi klientom a jednotlivými uzlami (resp. medzi dvojicou susedných uzlov v Tor sieti).
- **Bunky označené ako RELAY, RELAY\_EXTEND, RELAY\_DATA** apod. slúžia k prenosu šifrovaných dát cez jednotlivé uzly v rámci okruhu.
- Na ukončenie okruhu sa používa **bunka typu DESTROY**, ktorá signalizuje, že daný komunikačný okruh má byť okamžite zrušený a všetky naviazané šifrovacie kľúče zneplatnené.

Každá Tor bunka má pevne daný formát a obsahuje viacero polí, ktoré slúžia na identifikáciu, správu prenosu a prenos samotných dát. Presný obsah bunky sa môže mierne líšiť v závislosti od jej typu. Štruktúra štandardnej Tor bunky je znázornená na obr. 1.2, význam príslušných polí je nasledovný:

- **Circuit ID** – identifikátor okruhu, ku ktorému bunka patrí. Umožňuje multiplexovanie viacerých okruhov cez jedno TCP spojenie.
- **Command** – určuje typ bunky (napr. CREATE, RELAY, DESTROY, atď.).
- **Payload** – telo bunky, ktoré je počas prenosu v Tor sieti šifrované. Jeho obsah sa líši podľa konkrétneho typu bunky.



Obrázok 1.2 Schematické znázornenie štruktúry Tor bunky<sup>3</sup>.

<sup>3</sup> Prevzaté z oficiálnych výučbových materiálov k prednáškam predmetu MPC-NSB – vypracoval garant predmetu a prednášajúcim doc. Karel Burda, CSs. (viď tiež E-learning predmetu).

## Vytváranie okruhov a princíp cibul'ového smerovania v sieti Tor

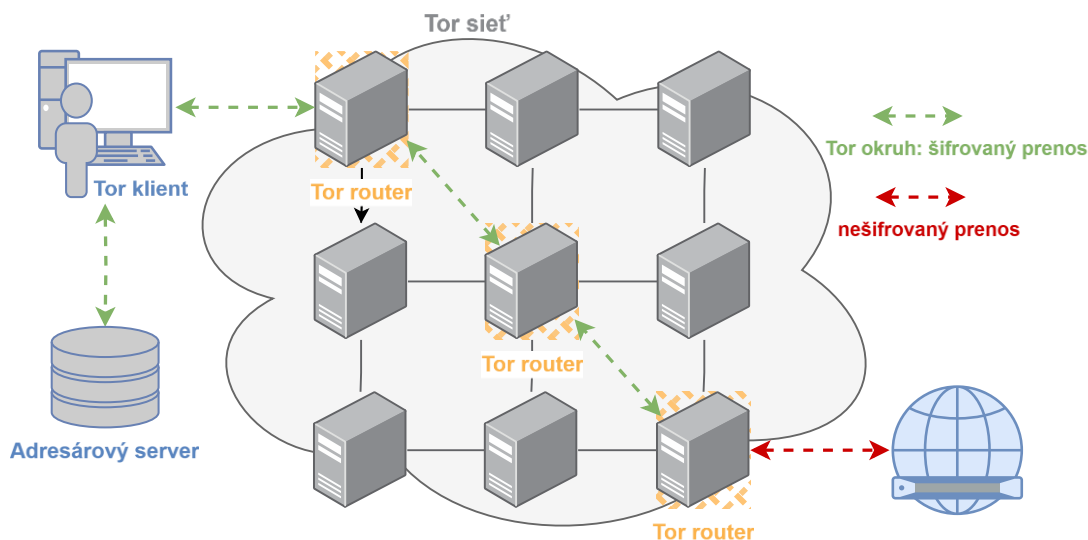
Kľúčovým mechanizmom zabezpečenia anonymity je vytváranie tzv. okruhov (*circuits*) a používanie techniky viacvrstvového šifrovania, známeho aj ako *onion routing*.

Tor vytvára medzi klientom a cieľovým serverom viacvrstvový (tzv. „cibul'ový“<sup>4</sup>) šifrovaný kanál, prostredníctvom ktorého sú údaje, resp. dátové pakety presmerované cez niekoľko náhodne vybraných uzlov v Tor sieti. Jednotlivé uzly poznajú len odosielateľa a prijímateľa ich časti trasy, nemajú znalosť o iných uzloch, ktoré boli alebo budú zapojené do celej komunikácie potrebnej pre zaistenie doručenia danej dátovej jednotky (bunky) od jej odosielateľa až k vybranému príjemcovi, čo zabezpečuje anonymitu.

Proces vytvárania okruhu prebieha v niekoľkých etapách:

1. **Výber uzlov:** klient si zo zverejneného zoznamu vyberie náhodne vhodné Tor uzly. Výber prebieha podľa špecifických pravidiel – napríklad vstupné uzly musia byť stabilné a dôveryhodné.
2. **Dohoda na kľúčoch:** pomocou protokolu podobného Diffie-Hellmanovej výmene kľúčov si klient postupne vytvorí s každým uzlom samostatný šifrovací kľúč. Všetky tieto výmeny prebiehajú cez vstupný uzol, pričom klient nadväzuje spojenie s ďalšími uzlami „cez“ predchádzajúce (šifrované).
3. **Postupné rozšírenie okruhu:** najskôr sa vytvorí šifrované spojenie klienta so vstupným uzlom (pomocou CREATE a CREATED buniek), následne sa cez tento uzol vytvorí šifrovaný tunel postupne ku všetkým nasledujúcim uzlom až nakoniec k výstupnému uzlu.

Takto vytvorený okruh slúži ako trasa, po ktorej sú ďalej prenášané šifrované dáta.



Obrázok 1.3 Komponenty Tor siete a znázornenie vytvoreného okruhu<sup>5</sup>.

<sup>4</sup> Označenie je prevzaté z prekladu angl. slova *onion*, ktoré značí cibuľu. Princíp šifrovania, resp. dešifrovania paketov odosielaných cez Tor sieť sa podobá vrstveniu cibule – a práve na základe tejto podobnosti bol vytvorený aj jej názov.

<sup>5</sup> Prevzaté z [5].

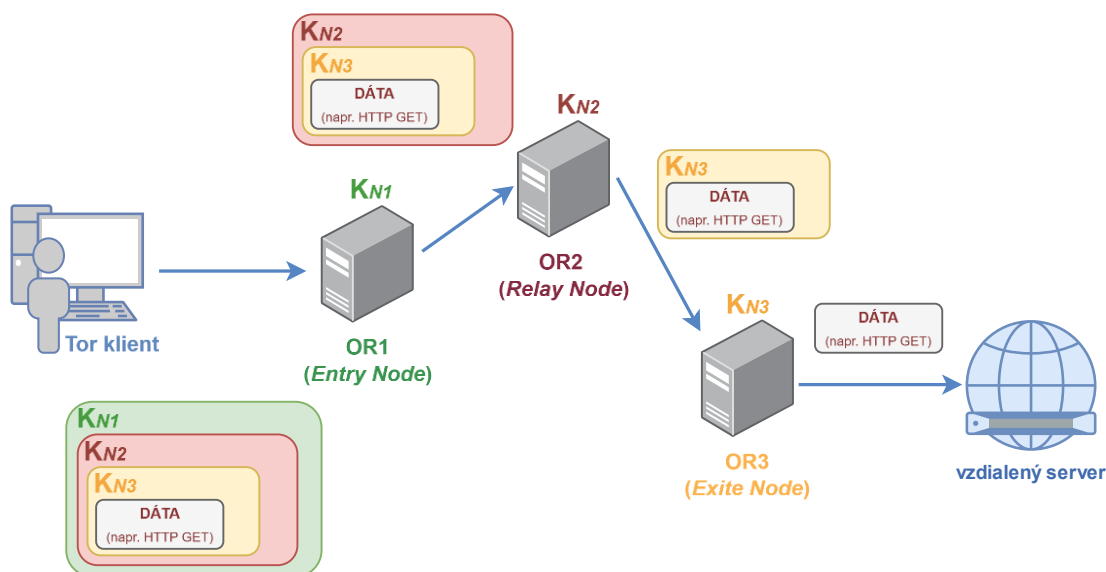
Po vytvorení kompletného okruhu od odosielateľa až cieľovému príjemcovi je možné zahájiť dátový prenos, ktorý je podrobený „cibuľovému smerovaniu“. Mechanizmus tohto viacvrstvého šifrovania funguje nasledovne:

1. Klient si najprv pripraví dátovú jednotku (napr. požiadavku HTTP), ktorú chce doručiť na cieľový server.
2. Túto jednotku následne **viacnásobne šifruje** – každá vrstva je určená jednému uzlu v poradí od výstupného po vstupný:
  - najprv pre výstupný uzol (vnútorná vrstva),
  - potom pre stredný uzol,
  - napokon pre vstupný uzol (vonkajšia vrstva).
3. Keď šifrovaná správa dorazí do vstupného uzla, ten v procese dešifrovania odstráni iba svoju vrstvu (vonkajšiu) a odošle jej obsah, ktorý je zašifrovaný pomocou kľúča pre ďalší medziľahlý uzol v poradí, ďalej smerom k ďalšiemu uzlu vo vytvorenom okruhu.
4. Nasledujúci uzol opäť odstráni svoju vrstvu a odošle zašifrovaný ďalej.
5. Proces sa opakuje, až kým bunka nedorazí k výstupnému uzlu. Ten dešifruje poslednú vrstvu a odosiela pôvodnú požiadavku vytvorenú klientom, resp. odosielateľom na cieľový server na internete (napr. webovú stránku).
6. Pri spätnej odpovedi sa postupuje obdobne, akurát sa jednotlivé šifrovacie kľúče aplikujú pri vytváraní vrstiev v opačnom poradí – výstupný uzol odpoveď zašifruje a pošle späť cez ten istý okruh, pričom každý uzol dešifruje iba svoju časť, až sa odpoveď dostane k pôvodnému klientovi.

Aplikácia viacvrstvého šifrovania na prenášané dáta je schematicky znázornená na obr. 1.4. Popísaný mechanizmus zaručí, že žiaden z uzlov nemá úplnú znalosť o celej komunikácii. Vstupný uzol pozná IP klienta, ale nie cieľový server. Výstupný uzol naopak pozná cieľ, ale nie klienta. Všetky medziľahlé uzly poznajú len svojich bezprostredných susedov.

Použitie anonymizačných sietí prináša množstvo výhod, medzi ktoré nepochybne patrí ukrytie IP adresy používateľov, čo je tiež jeden zo základných predpokladov pre ochranu pred nežiadúcim sledovaním a profilovaním. Na druhej strane, prenos dát prostredníctvom anonymizačnej siete môže byť znateľne pomalší, nakoľko nutnosť prenosu dát cez viaceré medziľahlé uzly, kedy dochádza navyše k šifrovaniu (resp. dešifrovaniu) týchto dát, môže mať za následok výsledné spomalenie internetového pripojenia. Medzi ďalšie nevýhody a riziká anonymizačných sietí možno zaradiť i možnosť kompromitácie výstupného uzla smerom k príjemcovi dát (*exit node*) a tiež skutočnosť, že použitie anonymizačných sietí nezaručí kompletnú ochranu pred všetkými formami sledovania komunikácie v počítačových sieťach, akou môže byť napr. sledovanie časových korelácií medzi dátovými prenosmi s ich následnou analýzou, a tak isto neposkytuje ochranu pred inými typmi sieťových útokov či útokov na koncové zariadenia, napr. prostredníctvom škodlivého kódu (malware) na strane užívateľa apod.

Viac informácií o koncepte anonymizačných sietí a o samotnej sieti Tor je možné nájsť v publikáciách [1], [2], [3], [4].



Obrázok 1.4 Schematické znázornenie vrstveného šifrovania v Tor sieti<sup>6</sup>.

### 1.3. Použité nástroje

#### Tor v Kali Linux

Tor predstavuje jednoduchý softvérový nástroj umožňujúci **anonymné prehliadanie internetu cez Tor sieť**. Vytvorenie, resp. simuláciu vlastnej anonymizačnej siete založenej na využití služby Tor je možné uskutočniť i v prostredí systému Kali Linux, a to jej inštaláciou priamo prostredníctvom príkazového riadku (terminálu) pomocou príkazov:

```
sudo apt update  
sudo apt install tor
```

Po úspešnej inštalácii nasleduje spustenie služby Tor:

```
sudo systemctl start tor  
sudo systemctl enable tor
```

Overenie, či je služba aktívna, je možné pomocou príkazu:

```
sudo systemctl status tor
```

<sup>6</sup> Prevzaté z [6].



Pre overenie pripojenia na Tor sieť možno použiť napr. nižšie uvedený príkaz:

```
curl --socks5-hostname 127.0.0.1:9050  
https://check.torproject.org/
```

Uvedený príkaz spustí odoslanie jednoduchkej HTTP GET požiadavky na stránku <https://check.torproject.org><sup>7</sup> cez vytvorenú Tor sieť. Pozn.: TCP port 9050 je predvolený pre Tor klienta, ktorý beží na Kali Linux. Sieť Tor v tomto prípade funguje ako proxy server, resp. sprostredkovateľ komunikácie medzi klientom na vašom zariadení a dotazovaným cieľovým serverom – všetka komunikácia je teda presmerovaná práve cez Tor sieť.

Po odoslaní požiadavky server **check.torproject.org** analyzuje vašu IP adresu a vráti odpoveď, či komunikácia prebieha cez Tor, alebo nie. Pokiaľ je použitie siete Tor správne nastavené, na výstupe v termináli sa zobrazí hláška:

**"Congratulations. This browser is configured to use Tor."**

## Tor Browser

Jedná sa o upravenú verziu webového prehliadača nakonfigurovanú pre anonymné používanie využívajúc práve sieť Tor pre **zabezpečenie súkromia a anonymity jeho užívateľov** v online prostredí. Tor Browser je navrhnutý tak, aby bolo s jeho použitím možné ukrytie nielen samotnej identity užívateľa, ale tiež jeho polohy a aktivity na internete.

**Tor Browser** realizuje šifrovanie prenášaných užívateľských dát v niekoľkých vrstvách. Dátové prenosy sú kompletne šifrované a odosielané cez Tor sieť, ktorá pozostáva z veľkého množstva (typicky tisícov) *relay* uzlov sprostredkujúcich prenos zabezpečenej šifrovanej komunikácie. Každý *relay* uzol na ceste prenosu dát smerom k príjemcovi vždy dešifruje len jednu (vonkajšiu) vrstvu, čím nikdy nezíska úplnú, kompletnú informáciu o danom prenose, vďaka čomu anonymita komunikujúcich strán zostáva zachovaná.

## Wireshark

Wireshark je sieťový analyzátor, ktorý umožňuje sledovať dátové prenosy. V prípade Tor je možné zachytiť šifrované pakety a analyzovať ich štruktúru, no obsah zostáva chránený šifrovaním.

Použitie nástroja Wireshark ste si prakticky vyskúšali už v rámci niekoľkých predošlých laboratórnych úloh, takže jeho bližší popis nebude už ďalej podrobne uvádzaný.

---

<sup>7</sup> Viac o filozofii a štruktúre projektu Tor, ktorého cieľom je poskytovanie špecializovaného Tor Browser prehliadača pre anonymné prehliadanie, je možné nájsť na oficiálnych stránkach: [7].

## 2. Praktická časť

V rámci praktickej časti úlohy si vyskúšate **anonymné prehliadanie prostredníctvom anonymizačného webového prehliadača Tor Browser**. Následne budete analyzovať zachytený tok dát v anonymizačnej sieti pomocou nástroja Wireshark, na základe čoho získate prehľad o výhodách, nevýhodách, a rizikách spojených s použitím prostriedkov pre anonymizáciu v dnešných počítačových sieťach.

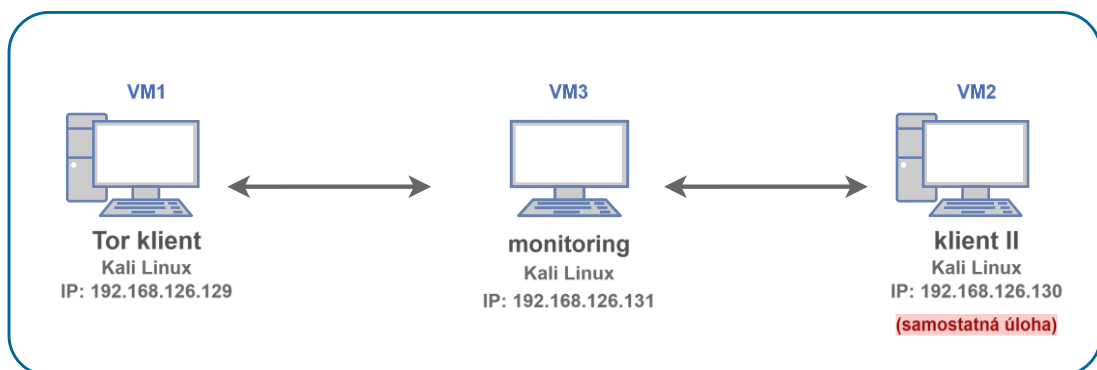
### 2.1. Topológia virtuálnej siete a nastavenie virtuálnych strojov

Vytvorená sieť bude pozostávať z troch virtuálnych strojov:

- **klient pre anonymné prehliadanie** a prístup na internet cez Tor sieť,
- **klient II** – simulácia klasického pripojenia, t. j. bežné pripojenie bez použitia Tor (využitie v časti **Samostatná úloha**),
- **monitorovacie zariadenie**, ktoré bude slúžiť pre účely sledovania a následnej analýzy prebiehajúcej komunikácie v sieti.

Sieťová konfigurácia:

- Tor klient (VM1): 192.168.126.129
- klient II (VM2): 192.168.126.130
- monitorovacie zariadenie (VM3): 192.168.126.131



Obrázok 2.1 Topológia siete laboratórnej úlohy.

### 2.2. Zoznámenie sa s použitými nástrojmi

Prehľad základných príkazov pre jednotlivé používané nástroje

- Uvedenie základných príkazov pre prácu so službou Tor na klientskom zariadení a pre inštaláciu a následné **použitie prehliadača Tor Browser** pre anonymné prehliadanie na internete bolo súčasťou teoretického úvodu, a z toho dôvodu ich opakovaný prehľad nie je ďalej uvádzaný. Všetky potrebné príkazy budú uvedené následne v praktickej časti v jednotlivých krokoch pre vypracovanie laboratórnej úlohy.

## Použitie Wiresharku pre analýzu komunikáciu cez sieť Tor

- V rámci analýzy zaznamenatej komunikácie je vhodné použiť filter:

```
tcp.port == 9050
```

Použitie uvedeného filtra zaručí zobrazenie TCP komunikácie na príslušnom porte, t. j. 9050 – čo je port využitý na strane klienta pre komunikáciu so SOCKS proxy pre jej ďalšie presmerovanie cez anonymizovanú Tor sieť.

## 2.3. Postup pre vypracovanie laboratórnej úlohy

### A) Príprava prostredia

#### Spustenie virtuálnych strojov:

- Otvorte VMware Workstation Pro (umiestnený na ploche).
- Spustite postupne všetky tri virtuálne stroje s Kali Linux.
- Uistite sa, že všetky VMs sú pripojené do rovnakej virtuálnej siete (napr. režim Host-only alebo NAT).
- Prihláste sa do prostredia Kali Linux na jednotlivých VMs.

VM „Tor klient“ – prihlasovacie údaje: **Username:** klient, **Password:** kali

VM „Klient II“ – prihlasovacie údaje: **Username:** server, **Password:** kali

VM „monitoring“ – prihlasovacie údaje: **Username:** kali, **Password:** kali

- Skontrolujte sieťovú konektivitu medzi strojmi (pomocou príkazu **ping**).

### B) Príprava klienta pre využitie anonymizovanej siete

#### Inštalácia Tor na klientskom VM:

- Na jednom z VMs, ktorý bude v simulovanej sieti zastávať úlohu klienta, otvorte terminál kliknutím na ikonu umiestnenú v záhlaví hlavného pracovného okna alebo v menu zvolíte **Applications > System Tools > Terminal**. Otvorí sa okno s príkazovým riadkom.
- Aktualizujte balíčky Kali Linux príkazom:

```
sudo apt update && sudo apt upgrade -y
```

- Pomocou nasledujúcich príkazov nainštalujte službu Tor:

```
sudo apt update  
sudo apt install tor
```

*Po úspešnej inštalácii služba Tor beží automaticky na pozadí systému.*

## Inštalácia Tor Browseru

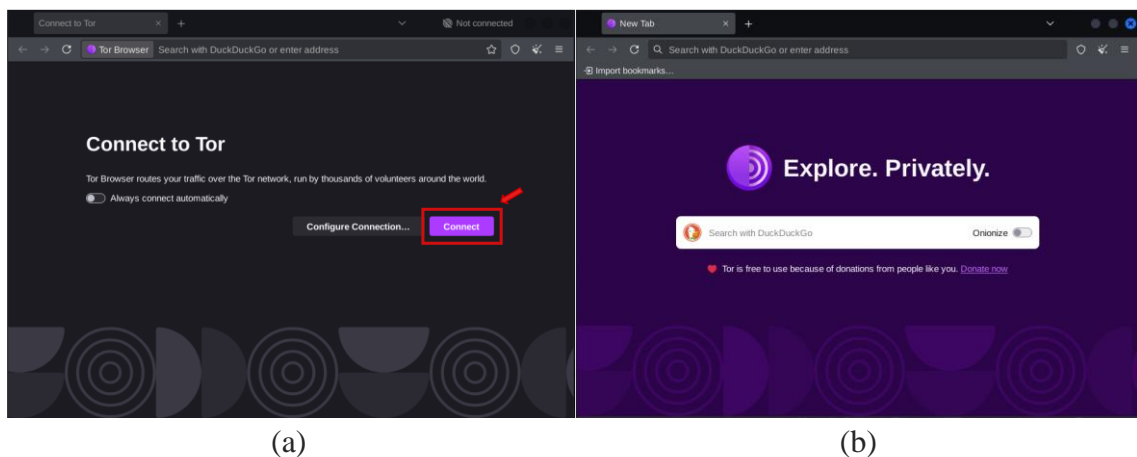
- Stiahnite inštalačný balík Tor Browser zo stránok projektu:

```
sudo apt install torbrowser-launcher -y
```

- Po stiahnutí spustíte Tor Browser zadáním nižšie uvedeného príkazu do terminálu (alebo v menu: **Applications** → **Internet** → **Tor Browser Launcher**):

```
torbrowser-launcher
```

- Po spustení akceptujte podmienky, potvrdíte a nechajte prebehnúť aktualizáciu, ak je dostupná, a následne kliknite na **Connect**.
- Po úspešnom pripojení sa otvorí anonymné prehliadacie okno, čo značí, že **Tor Browser** je pripravený na anonymné prehliadanie.



Obrázok 2.2 Pripojenie k prehliadaču Tor Browser (a), načítanie úvodnej domovskej stránky (b).

## Pripojenie k Tor sieti a overenie funkčnosti

- Po spustení Tor Browseru by sa automaticky mala otvoriť stránka (viď obr. 2.3): <https://check.torproject.org/>
- V prípade úspešného pripojenia sa objaví hláška: "Congratulations. This browser is configured to use Tor."
- Ak nedôjde k automatickému načítaniu stránky, skúste kliknúť na možnosť **Connect** alebo reštartujte Tor Browser.

## C) Sledovanie sieťovej prevádzky

### Sledovanie prichádzajúcej komunikácie vo Wiresharku na VM3

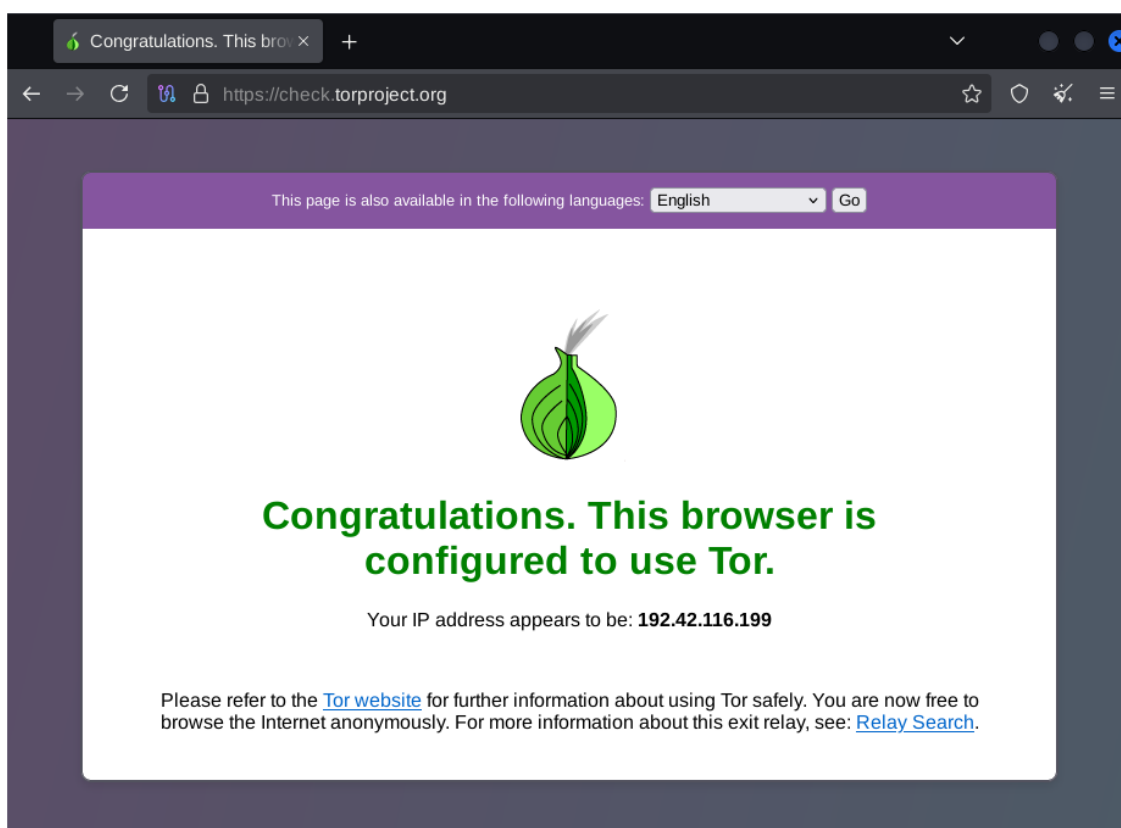
- Prejdite na VM3.
- Otvorte nové terminálové okno a spustíte nástroj Wireshark:

```
sudo wireshark &
```

- Vyberte správne sieťové rozhranie (napr. `eth0`).
- Aplikujte vhodný filter pre zachytávanie komunikácie prechádzajúcej cez sieť Tor, napr.:

```
tcp.port == 9001 || tcp.port == 443
```

- Spustite zachytávanie sieťovej komunikácie na zvolenom rozhraní kliknutím na **Start Capturing**.

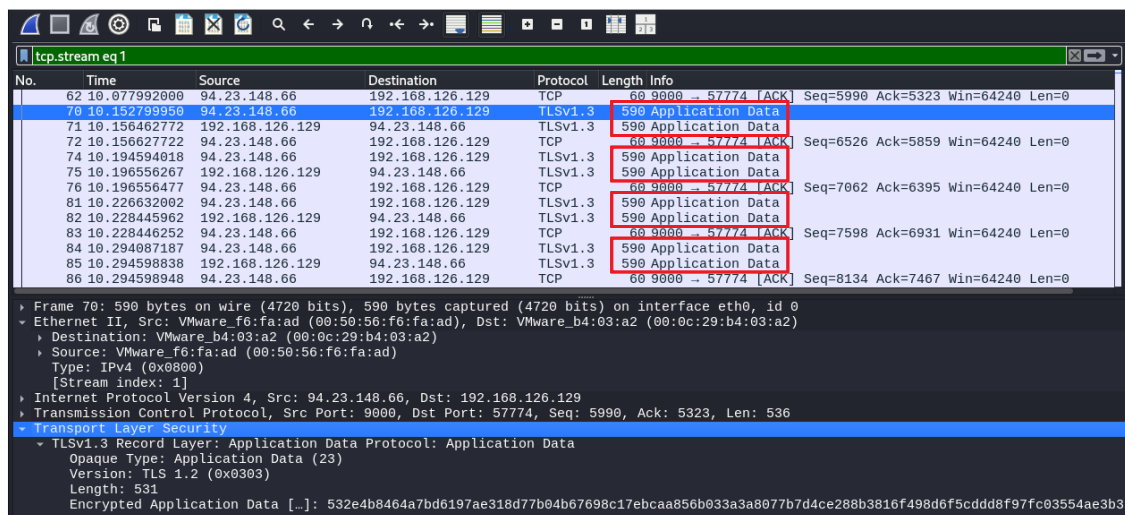


Obrázok 2.3 Úvodná stránka – potvrdenie úspešného pripojenia.

- V spustenom Tor Browseri na klientovi (VM1) sa pokúste prístupit' na webovú stránku <https://whatismyipaddress.com> a sledujte priebeh zaznamenanej komunikácie vo Wiresharku na monitorovacom zariadení (VM3). **Zaznamenajte si IP adresu zobrazenú stránkou.**
- Výsledkom by mal byť záznam komunikácie, v ktorom je možné pozorovať veľké množstvo TCP spojení, kedy ale **nebude možné ďalej analyzovať prenášaný obsah**, a to konkrétne HTTP/HTTPS požiadavky v čitateľnej

podobe, nakoľko sa jedná o šifrovaný prenos skrz vytvorenú Tor sieť. Venujte pozornosť veľkosti dátových jednotiek.

*Pozn.: štandardná veľkosť Tor bunky je 512 B. Táto bunka sa však následne zapuzdruje do TLS záznamu (TLS record), ktorý obsahuje okrem dátovej časti (= Tor bunky) aj ďalšie riadiace informácie. Z toho dôvodu je možné vidieť v zázname komunikácie inú veľkosť dátovej jednotky (napr. 590 B), dôležitá je avšak jej nemennosť v priebehu komunikácie.*



No.	Time	Source	Destination	Protocol	Length	Info
62	10.077992000	94.23.148.66	192.168.126.129	TCP	60	9800 → 57774 [ACK] Seq=5990 Ack=5323 Win=64240 Len=0
70	10.152799950	94.23.148.66	192.168.126.129	TLSv1.3	590	Application Data
71	10.156462772	192.168.126.129	94.23.148.66	TLSv1.3	590	Application Data
72	10.156627722	94.23.148.66	192.168.126.129	TCP	60	9800 → 57774 [ACK] Seq=6526 Ack=5859 Win=64240 Len=0
74	10.194594018	94.23.148.66	192.168.126.129	TLSv1.3	590	Application Data
75	10.196556267	192.168.126.129	94.23.148.66	TLSv1.3	590	Application Data
76	10.196556477	94.23.148.66	192.168.126.129	TCP	60	9800 → 57774 [ACK] Seq=7062 Ack=6395 Win=64240 Len=0
81	10.226632002	94.23.148.66	192.168.126.129	TLSv1.3	590	Application Data
82	10.228445962	192.168.126.129	94.23.148.66	TLSv1.3	590	Application Data
83	10.228446252	94.23.148.66	192.168.126.129	TCP	60	9800 → 57774 [ACK] Seq=7598 Ack=6931 Win=64240 Len=0
84	10.294087187	94.23.148.66	192.168.126.129	TLSv1.3	590	Application Data
85	10.294598838	192.168.126.129	94.23.148.66	TLSv1.3	590	Application Data
86	10.294598948	94.23.148.66	192.168.126.129	TCP	60	9800 → 57774 [ACK] Seq=8134 Ack=7467 Win=64240 Len=0

Frame 70: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface eth0, id 0  
 Ethernet II, Src: VMware\_f6:fa:ad (00:50:56:f6:fa:ad), Dst: VMware\_b4:03:a2 (00:0c:29:b4:03:a2)  
 Destination: VMware\_b4:03:a2 (00:0c:29:b4:03:a2)  
 Source: VMware\_f6:fa:ad (00:50:56:f6:fa:ad)  
 Type: IPv4 (0x0800)  
 [Stream index: 1]  
 Internet Protocol Version 4, Src: 94.23.148.66, Dst: 192.168.126.129  
 Transmission Control Protocol, Src Port: 9800, Dst Port: 57774, Seq: 5990, Ack: 5323, Len: 536  
 Transport Layer Security  
 TLSv1.3 Record Layer: Application Data Protocol: Application Data  
 Opaque Type: Application Data (23)  
 Version: TLS 1.2 (0x0303)  
 Length: 531  
 Encrypted Application Data [...]: 532e4b8464a7bd6197ae318d77b04b67698c17ebcaa856b033a3a8077b7d4ce288b3816f498d6f5cdd8f97fc03554ae3b3

Obrázok 2.4 Ukážka zachytenej komunikácie: využitie Tor Browser pre anonymné prehliadanie<sup>8</sup>.

- K overeniu informácií o pridelennej IP adrese<sup>9</sup> použite službu whois a analyzujte zistené informácie:

```
whois 193.189.100.201
```

IP adresa, ktorú uvidíte na stránke ako napr. [whatismyipaddress.com](http://whatismyipaddress.com), je **IP adresa výstupného Tor uzla**, ktorý kontaktuje cieľový server na konci vytvoreného Tor okruhu. Cieľový server tak nemá vedomosť o tom, aký konkrétny klient ho so svojou požiadavkou kontaktov, čo názorne demonštruje spôsob, akým Tor umožňuje zaistiť anonymitu klientov.

<sup>8</sup> Vo výstupe môžete vidieť komunikáciu klienta s uzlom s IP adresou 94.23.148.66 – jedná sa o IP adresu, ktorá pravdepodobne patrí jednému z uzlov siete Tor. Komunikácia na porte 9000 je pre túto sieť typická. Tor štandardne pre medzifahlé uzly (*relays*) využíva porty ako 9001, 9003 apod., avšak vzhľadom k tomu, že Tor sieť je dynamická a uzly sa môžu meniť, je bežné, že klient nadviaže spojenie s rôznymi IP adresami na rôznych portoch, ako napríklad práve 9000, 9001 alebo 9003.

<sup>9</sup> Pri zadávaní príkazu do terminálového okna použite IP adresu pridelenú Vášmu klientovi na VM1.

Time	192.168.126.129	94.23.148.66	Comment
9.748423723	57774	57774 → 9000 [SYN] Seq=0 Win=0 Len=0	TCP: 57774 → 9000 [SYN] Seq=0 Win=64240 Len=0 MSS
9.768111029	57774	9000 → 57774 [SYN, ACK] Seq=0 Ack=1 Win=64240	TCP: 9000 → 57774 [SYN, ACK] Seq=0 Ack=1 Win=64240
9.768456270	57774	57774 → 9000 [ACK] Seq=1 Ack=1 Win=64240 Len=0	TCP: 57774 → 9000 [ACK] Seq=1 Ack=1 Win=64240 Len=0
9.781625301	57774	Client Hello (SNI=www.f2neitsb6y5wljbagwz.co)	TLSv1.3: Client Hello (SNI=www.f2neitsb6y5wljbagwz.co)
9.781625351	57774	9000 → 57774 [ACK] Seq=1 Ack=518 Win=64240 Len=0	TCP: 9000 → 57774 [ACK] Seq=1 Ack=518 Win=64240 Len=0
9.803170438	57774	Server Hello, Change Cipher Spec, Application Data	TLSv1.3: Server Hello, Change Cipher Spec, Application Data
9.803452035	57774	57774 → 9000 [ACK] Seq=518 Ack=1169 Win=65535 Len=0	TCP: 57774 → 9000 [ACK] Seq=518 Ack=1169 Win=65535
9.810071096	57774	Change Cipher Spec, Application Data	TLSv1.3: Change Cipher Spec, Application Data
9.810140880	57774	9000 → 57774 [ACK] Seq=1169 Ack=598 Win=64240 Len=0	TCP: 9000 → 57774 [ACK] Seq=1169 Ack=598 Win=64240
9.810585387	57774	Application Data	TLSv1.3: Application Data
9.810585577	57774	9000 → 57774 [ACK] Seq=1169 Ack=631 Win=64240 Len=0	TCP: 9000 → 57774 [ACK] Seq=1169 Ack=631 Win=64240
9.829499085	57774	Application Data	TLSv1.3: Application Data
9.848758025	57774	Application Data	TLSv1.3: Application Data
9.849586326	57774	57774 → 9000 [ACK] Seq=631 Ack=1327 Win=65535 Len=0	TCP: 57774 → 9000 [ACK] Seq=631 Ack=1327 Win=65535
9.853747568	57774	9000 → 57774 [PSH, ACK] Seq=1327 Ack=631 Win=6 Len=0	TCP: 9000 → 57774 [PSH, ACK] Seq=1327 Ack=631 Win=6
9.873075962	57774	Application Data	TLSv1.3: Application Data

Obrázok 2.5 *Flow Graph*<sup>10</sup> komunikácie medzi Tor klientom a vzdialeným serverom.

The screenshot shows the homepage of WhatIsMyIPAddress.com. The user's IP address is displayed as IPv6: 2a0f:df00:0:255::201 and IPv4: 193.189.100.201. The location is identified as Stockholm, Sweden, with a map showing the city. A red box highlights the IPv4 address. A red button labeled 'HIDE MY IP ADDRESS NOW' is visible. The page also includes a search bar and navigation links like 'ABOUT', 'PRESS', 'PODCAST', and 'SUPPORT'.

Obrázok 2.6 Tor klient: ukážka výstupu po prístupe na webové stránky [whatismyipaddress.com](https://whatismyipaddress.com) (pridelenie IP adresy).

<sup>10</sup> Flow Graph záznamu komunikácie si môžete zobrazit' cez voľbu **Statistics > Flow Graph** v záhlaví panela nástrojov hlavného okna nástroja Wireshark.

- Po zistení IP adresy klienta s Tor (napr. pomocou [whatismyipaddress.com](https://whatismyipaddress.com) alebo z výpisu vo Wiresharku), overte, či táto pridelená IP adresa skutočne prislúcha niektorému z výstupných uzlov Tor siete pomocou niektorej zo stránok:
  - <https://www.dan.me.uk/tornodes> – webová stránka poskytuje aktuálny zoznam Tor výstupných (*exit*) uzlov vrátane ich IP adries, portov a krajín. Poskytujete možnosti filtrovania a vyhľadávania konkrétnych adries.
  - <https://www.netify.ai/resources/tor> – webová stránka obsahuje podrobné informácie o Tor sieti, vrátane jej štruktúry, identifikácie prevádzky a aktuálneho zoznamu výstupných uzlov.
- Ak sa pridelená IP adresa nachádza v niektorom zo zoznamov, jedná sa skutočne o výstupný uzol (*exit node*). Všimnite si aj ďalšie informácie, ako napr. krajinu, port a názov siete. Tieto informácie si zaznamenajte a porovnajte s výsledkom zisteným pomocou `whois`.
- Otestujte funkčnosť pripojenia na `.onion` adresu cez Tor Browser – tieto adresy predstavujú špeciálne domény určené pre webové služby dostupné iba cez anonymizovanú Tor sieť. Zabezpečujú anonymitu nielen používateľa, ale tiež cieľového servera. Ich cieľom je skryť fyzické umiestnenie služby a znemožniť bežné sledovanie prevádzky. V prehliadači na klientovi s Torom (VM1) otvorte nasledovný odkaz:
 

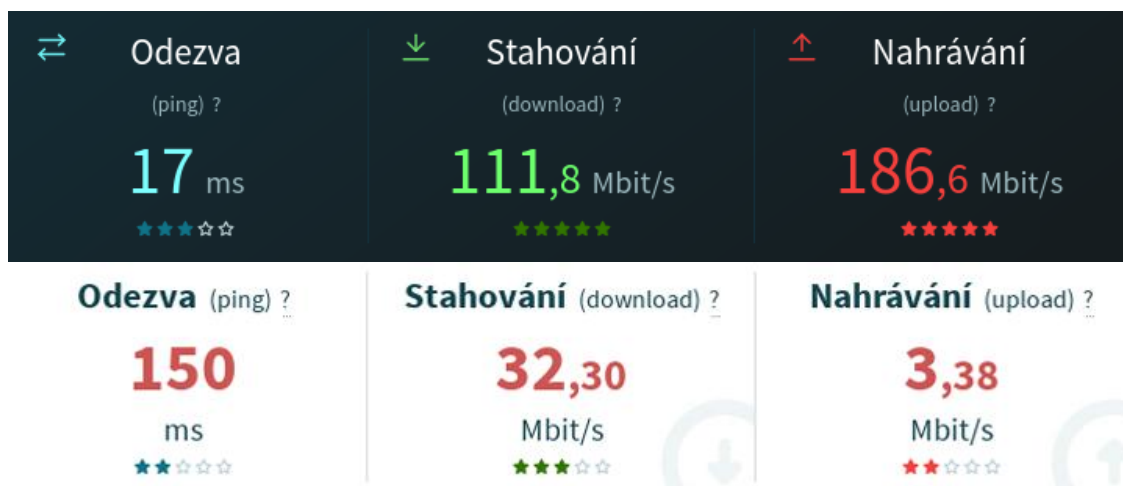
<https://duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion/>
- Jedná sa o špeciálnu verziu vyhľadávača DuckDuckGo pre Tor sieť. Vyskúšajte vyhľadať kľúčové slovo **"Tor exit node"** a sledujte, či sa načítajú výsledky. Môžete tiež porovnať rýchlosť, štruktúru a vzhľad stránky so štandardnou verziou DuckDuckGo.



## 2.4. Samostatná úloha

V poslednej časti laboratórnej úlohy realizujete porovnanie šifrovanej komunikácie, resp. prenosu dátových jednotiek štandardným spôsobom (t. j. s využitím aplikačného protokolu HTTPS) a prostredníctvom Tor siete. Na základe analýzy dátovej komunikácie vo Wiresharku porovnáte rozdiely medzi uvedenými možnosťami dátového prenosu.

- A) Cieľom vašej samostatnej práce bude s využitím VM2 (nového klienta) pristupovať na internet „klasicky“ (t. j. bez použitia siete Tor), kedy bude pre dátový prenos využitý protokol HTTP, resp. zabezpečený HTTPS, a následne porovnať zásadné rozdiely v anonymite, štruktúre prenosu, veľkosti dátových jednotiek a viditeľnosti dát pri použití Tor Browseru (Tor siete) a bežného prehliadača využívajúceho HTTPS pripojenie.
- B) Na základe záznamu komunikácie vo Wiresharku analyzujte hlavné rozdiely v zabezpečení identity pri použití Tor vs. klasického HTTPS pripojenia a porovnajte výhody, resp. nevýhody oboch prístupov. Taktiež analyzujte rozdiely v IP adresách, ktoré cieľový server prideli klientom na VM1 a VM2 (môžete využiť nástroj `whois`).
- C) Nakoniec uskutočnite meranie prenosovej rýchlosti a latencie oboch klientov. Doporučené je využiť stránku: <https://www.rychlost.cz>. Sledujte parametre rýchlosti sťahovania/odosielania a latenciu (dobu odozvy – ping), následne namerané výsledky oboch klientov vzájomne porovnajte.



Obrázok 2.7 Porovnanie výsledkov meraní prenosových parametrov: klient bez Tor (hore) vs. klient s Tor (dole).

### 3. Záver

V tejto laboratórnej úlohe ste sa oboznámili so základnými princípmi fungovania anonymizačných sietí a ich významom pre ochranu súkromia a zachovanie anonymity používateľov pri komunikácii na internete.

Prakticky ste si vyskúšali **inštaláciu Tor klienta** v systéme Kali Linux a tiež použitie **prehliadača Tor Browser** špeciálne prispôbeného pre anonymné prehliadanie, nadviazanie spojenia cez Tor sieť, ako aj prehliadanie internetu anonymným spôsobom. Súčasťou úlohy bola aj analýza zachytenej komunikácie pomocou nástroja Wireshark, kde ste mohli sledovať *handshake* fázu pre vytvorenie spojenia so sieťou Tor a následné šifrované dátové prenosy. Súčasťou samostatnej úlohy bolo taktiež **porovnanie priebehu šifrovanej komunikácie prostredníctvom protokolu HTTPS a komunikácie odosielanej práve cez anonymizačnú sieť Tor** a sledovanie významných rozdielov porovnaním oboch uvedených prístupov. V rámci vzájomného porovnania ste taktiež uskutočnili meranie prenosových parametrov, v priebehu ktorého ste mohli pozorovať dlhšiu dobu odozvy a nižšie prenosové rýchlosti v prípade použitia Tor.

#### 3.1. Kontrolné otázky

1. Čo je hlavným cieľom využívania anonymizačných sietí?
  - A) Dosiahnuť vysokú prenosovú rýchlosť komunikácie
  - B) Zamedziť identifikácii používateľa v celosvetovej sieti
  - C) Šifrovať komunikáciu a zabezpečiť dôvernosť prenosu medzi klientom a cieľovým serverom
  - D) Zaistiť anonymitu používateľa pri prístupe k internetu ☒
2. Na akom princípe funguje tzv. „cibuľové smerovanie“ (*onion routing*)?
  - A) Každý medziľahlý uzol na ceste od klienta k serveru pozná vždy celú trasu prenosu až k cieľu
  - B) Dáta sú šifrované v niekoľkých vrstvách a dešifrované postupne na každom uzle
  - C) Každý uzol na prenosovej trase musí poznať IP adresu cieľového servera
  - D) Dáta sú prenášané pomocou transportného protokolu UDP
3. Označte nesprávne tvrdenia o medziľahlých uzloch prenosu (*Tor Nodes*):
  - A) Vstupný Tor uzol (*Entry Node*) je prvým bodom kontaktu medzi klientom a Tor sieťou
  - B) Komunikujú medzi sebou s využitím transportného protokolu UDP
  - C) Každý uzol pozná IP adresu klienta
  - D) Tor Exit Node smeruje dáta na cieľový server a pozná IP adresu klienta

4. Ktoré z nasledujúcich charakteristík platia pre Tor bunky (*cells*)?
- A) Majú pevne stanovenú veľkosť 512 bajtov
  - B) Vždy obsahujú riadiace aj dátové informácie
  - C) Ich prenos na transportnej vrstve zabezpečuje protokol UDP
  - D) V záhlaví IP protokolu obsahujú zdrojovú IP adresu klienta
5. Aké rozdiely možno pozorovať medzi bežným HTTPS prístupom a prístupom cez Tor v nástroji Wireshark?
- A) V prípade použitia Tor sú IP adresy výstupných uzlov odlišné od zdrojovej IP adresy klienta
  - B) HTTPS nezahŕňa žiadne mechanizmy pre šifrovanie, Tor používa pre zaistenie dôverylosti prenosu TLS
  - C) Tor používa fixnú veľkosť buniek
  - D) Tor umožňuje sledovanie zdrojovej IP adresy klienta rovnako ako HTTPS
6. V čoho dôsledku je pripojenie cez Tor zvyčajne pomalšie než priame pripojenie k internetu?
- A) Dáta sa prenášajú cez niekoľko medziľahlých uzlov
  - B) Používateľ (klient) musí pred odoslaním dát tieto dáta najskôr elektronicky podpísať pomocou asymetrického kryptosystému
  - C) Tor používa zastaraný kryptografický algoritmus
  - D) Každý medziľahlý uzol musí uskutočniť viacnásobné operácie šifrovania (resp. dešifrovania)
7. Čo je .onion adresa?
- A) Doména bežne dostupná pri klasickom internetovom prehliadaní
  - B) IP adresa výstupného uzla Tor siete
  - C) Špeciálna adresa určená pre skryté služby v sieti Tor
  - D) Označuje cieľovú službu, ktorá je dostupná len pri znalosti IP adresy cieľového servera tejto služby
8. Na základe akých znakov je možné identifikovať vo Wiresharku, že komunikácie prebieha prostredníctvom Tor siete?
- A) Použitím filtra `tcp.port == 9001`
  - B) Vyhľadaním EAPoL správ
  - C) Identifikáciou TLS paketov s fixnou veľkosťou dát
  - D) Zhodou zdrojových a cieľových IP adries pre všetky pakety prislúchajúce k rovnakému dátovému toku

9. Vyberte správne tvrdenia o výstupnom uzle Tor siete (*Exit Node*):
- A) Je posledným uzlom vo vytvorenom Tor okruhu
  - B) Odosiela dešifrovanú komunikáciu na cieľovú službu
  - C) Ako jediný pozná IP adresu používateľa (klienta)
  - D) Zabezpečuje TLS šifrovanie medzi klientom a serverom
10. Čo je úlohou adresárového servera v sieti Tor?
- A) Zabezpečuje šifrovanie prenosu dát medzi uzlami v sieti
  - B) Poskytuje IP adresy užívateľov v sieti
  - C) Obsahuje informácie o dostupných Tor uzloch
  - D) Pridáva nové vrstvy šifrovania pre každú odoslanú Tor bunku
11. Aké zásadné rozdiely ste pozorovali pri meraní rýchlosti pripojenia cez anonymnú sieť Tor a bez použitia Tor?
- A) Vyššiu latenciu cez Tor
  - B) Prenosovú rýchlosť bola približne rovnaká
  - C) Nižšiu rýchlosť downloadu pri použití Tor
  - D) Nižšiu latenciu prenosu v prípade bežného pripojenia

## 4. Literatúra

- [1] Dingledine, Roger, Mathewson, Nick and Syverson, Paul *Tor: The Second Generation Onion Router*. In: Paul Syverson, vol. 13, 2004. Dostupné z: <https://ieeexplore.ieee.org/document/10330539> [cit. 2024-12-02].
- [2] Rahman, Mohammad Saidur and Diadamo, Stephen and Mehic, Miralem and Fleming, Charles. *Quantum Secure Anonymous Communication Networks*. 2024. [online]. Dostupné z: [https://www.researchgate.net/figure/Three-layer-encrypted-message-in-a-Tor-network\\_fig1\\_380600931](https://www.researchgate.net/figure/Three-layer-encrypted-message-in-a-Tor-network_fig1_380600931) [cit. 2024-12-02].
- [3] MURDOCH, Steven J. a George DANEZIS. *Low-cost traffic analysis of Tor*. In: Proceedings of the 2005 IEEE Symposium on Security and Privacy. IEEE, 2005, s. 183–195. ISBN 0-7695-2339-0. [cit. 2025-04-25].
- [4] DINGLEDINE, Roger, Nick MATHEWSON a Paul SYVERSON. *Tor: The second-generation onion router*. In: Proceedings of the 13th USENIX Security Symposium. San Diego: USENIX Association, 2004, s. 303–320. Dostupné tiež z: <https://www.usenix.org/legacy/events/sec04/tech/dingledine.html>
- [5] MYRA SECURITY. *What is the Tor Network?* [online]. Myra Security, [cit. 2025-05-04]. Dostupné z: <https://www.myrasecurity.com/en/knowledge-hub/tor-network/>
- [6] PALLOTTI, Massimo a KULSHRESTHA, Mayank. *Tor Traffic in Enterprise Networks: Risks and Realities* [online]. Unit 42 – Palo Alto Networks, 2023. [cit. 2025-05-04]. Dostupné z: <https://unit42.paloaltonetworks.com/tor-traffic-enterprise-networks/>
- [7] TOR PROJECT. *Anonymity Online*. [online]. 2025 [cit. 2024-12-07]. Dostupné z: <https://www.torproject.org/>