Možnosti komunikace klient-server v TOR sítích

Šimon Boškovič

Bakalářská práce
2018

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2017/2018

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Šimon Boškovič**
Osobní číslo:	**A14076**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Informační a řídicí technologie**
Forma studia:	**prezenční**
Téma práce:	**Možnosti komunikace klient-server v TOR sítích**
Téma anglicky:	**Client-server Communication Options in the TOR Network**

Zásady pro vypracování:

1. **Popište základní schéma TOR komunikace a principy anonymizace uživatelů.**
2. **Pomocí zachycené komunikace zhodnoťte, zda proces odpovídá principům popsaných v bodě 1.**
3. **Specifikujte slabé místa anonymizačního procesu.**
4. **Pomocí testů zjistěte stabilitu spojení.**
5. **Navrhněte další možnosti rozšíření anonymizace uživatelů.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **OREBAUGH, Angela. Wireshark a Ethereal: kompletní průvodce analýzou a diagnostikou sítí. Brno: Computer Press, 2008. ISBN 9788025120484.**
2. **Tor Project – online. Seattle, WA USA: The Tor Project, 2002 ,cit. 2017-11-19. Dostupné z: www.torproject.org ISBN 788025104170**
3. **PUŽMANOVÁ, Rita. Bezpečnost bezdrátové komunikace: jak zabezpečit wi-fi, bluetooth, GPRS či 3G. Brno: Computer Press, 2005. ISBN 9788025107911**
4. **BURDA, Karel. Úvod do kryptografie. Brno: Akademické nakladatelství CERM, 2015. ISBN 9788072049257**
5. **JIROUŠEK, Radim. Principy digitální komunikace. Voznice: Leda, 2006. ISBN 9788073350840**

Vedoucí bakalářské práce: **Ing. David Malaník, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání bakalářské práce: **15. prosince 2017**

Termín odevzdání bakalářské práce: **25. května 2018**

Ve Zlíně dne 15. prosince 2017

doc. Mgr. Milan Adámek, Ph.D.
děkan

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

prof. Ing. Vladimír Vašek, CSc.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 22.5.2018

.....
podpis diplomanta

ABSTRAKT

Bakalářská práce se zabývá možnostmi skrytí komunikace v síti Tor. Jsou popsány technické specifikace od skupiny The Tor Project, jejíž principy jsou následně prokázány v několika praktických testech. Kromě ověření bezpečnostní vrstvy byl dbán také důraz na zhodnocení kvality připojení a jeho stabilitu. V závěru práce jsou zmíněny také vylepšení, které by mohly zvýšit bezpečnost této anonymizační vrstvy a uživatelský komfort.

Klíčová slova: Síť Tor, Anonymní komunikace, Cibulové směrování, Analýza síťové komunikace, Asymetrické šifrování.

ABSTRACT

The Bachelor thesis is focused on possibilities of hiding communication in the Tor network. Technical specifications from The Tor Project are described, the principles of which are then demonstrated in several practical tests. In addition to verifying quality of security layer, emphasis was also placed on stability and bandwidth of the connection. At the end of this work are mentioned improvements, which could increase safety and user comfort of this anonymous layer.

Keywords: Tor network, Anonymous communication, Onion routing, Analysis of communication network, Asymmetric cryptography

Velké poděkování patří hlavně panu Ing. Davidu Malaníkovi Ph.D. za pomoc při zpracování bakalářské práce, cenné rády a bezproblémové jednání.

OBSAH

ÚVOD

V dnešní době rozvinutých informačních a komunikačních technologií si jen stěží dokážeme představit život bez internetu. Internet nám umožňuje každodenní přístup ke všem informacím, a také nám dává možnost komunikovat prostřednictvím sociálních sítí mezi sebou. Internet je dynamické místo, které se vyvíjí každým dnem, v případě jakéhokoliv konfliktu, války, nebo třeba živelné katastrofy se díky internetu dozvíme o nich téměř ihned. Internet se tedy může na první pohled jevit jako bezpečné místo, kde se shromažďují veškeré informace o aktuálním i předešlém dění ve světě. Mnoho lidí si ovšem neuvědomuje fakt, že po každém z nás zůstává na internetu spousta informací, které si může každý schopnější člověk, který se pohybuje na internetu, snadno dohledat.

Tato bakalářská práce se bude zabývat anonymitou uživatelů v prostředí sítě internet. Bude zkoumat, zda je opravdu síť TOR tak anonymní, jak je popisována.

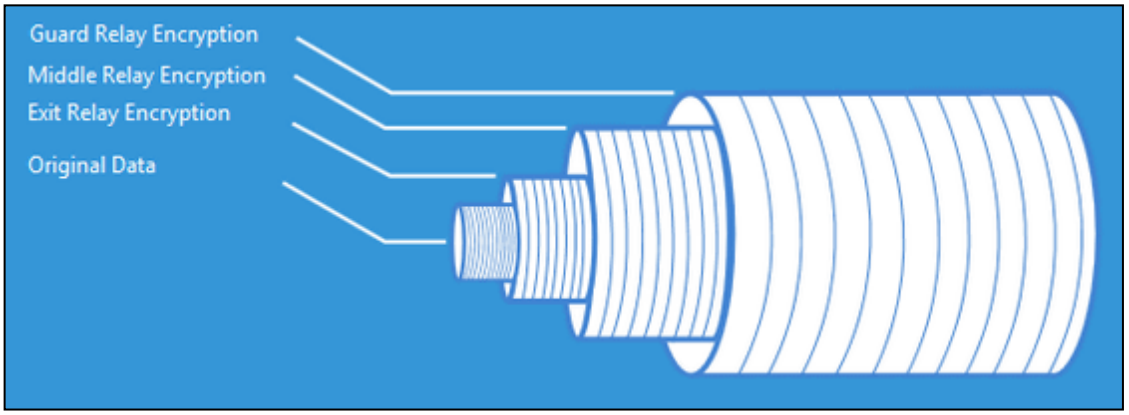
I. TEORETICKÁ ČÁST

1 ANONYMITA V INTERNETU

Slovo anonymita je v dnešní době dosti aktuální a diskutované téma. Doslovný překlad slova anonymita pochází z řeckého slova *anonymia* a v informačních technologiích je tento význam slova chápán jako vlastnost systému, která dovoluje použití služeb a zdrojů bez zjištění identity uživatele tohoto systému. Internet jako takový se může jevit jako bezpečné a anonymní místo. Člověku se může zdát, že je za monitorem obrazovky bezpečně ukryt před okolním světem, a že mu z internetu nic nehrozí. Lidé si ve svém osobním životě soukromé informace tají, nebo je sdělují jen těm lidem, kterým doopravdy věří. Ve světě internetu je tomu ovšem jinak, vývojem sociálních a jiných sítí se úroveň soukromí dramaticky zhoršila. Na sociálních sítích lidé vystupují pod reálnými jmény, přidávají fotografie svých aut, svého domu, velmi často sdílí svoji aktuální polohu, což může budoucímu útočníkovi nahrát do karet. [1]

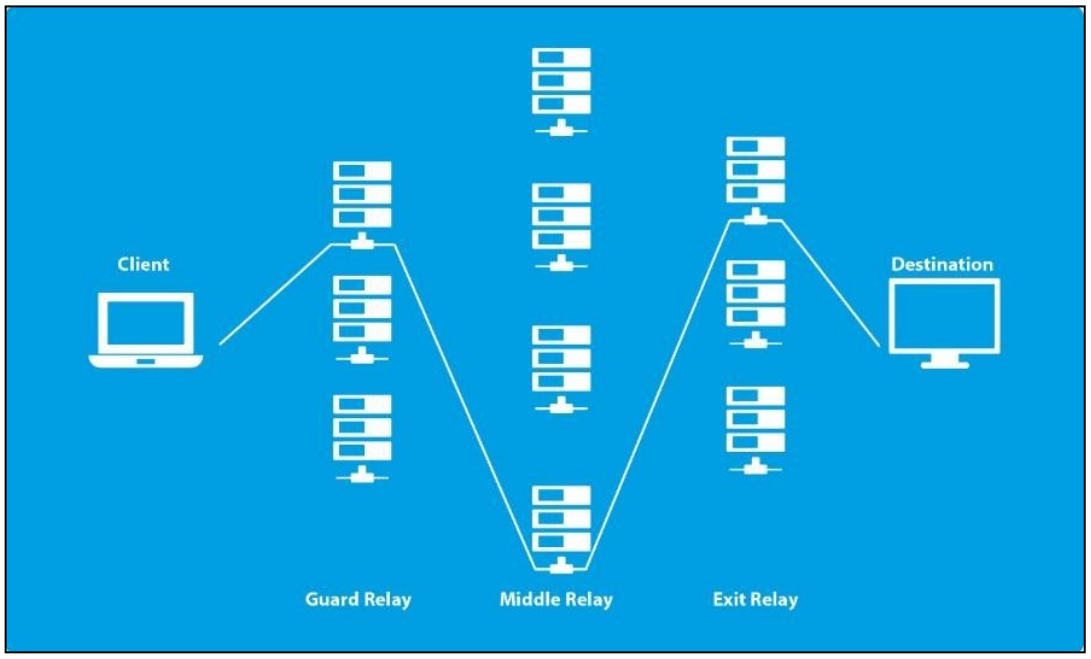
1.1 Onion Routing

Vznik TOR sítě se datuje v druhé polovině 90. let 20. století a jejím cílem bylo zabezpečit odposlech vládní a armádní komunikace ve Spojených státech amerických. Později se však tato komunikace rozšířila od americké armády k veřejnosti. Do sítě TOR se může připojit skutečně každý, je to naprosto bezplatné. Stačí si stáhnout webový prohlížeč ze stránek https://www.torproject.org/. Tento prohlížeč je navíc dostupný pro všechny systémové platformy, takže není problém s kompatibilitou. Na rozdíl od klasického směrování na internetu, které má za cíl najít tu nejlepší cestu pro doručení zprávy je Onion rauting navržen tak, že představuje obecné řešení anonymizace. Pokud ale používáme klasickou komunikaci postavenou na protokolu IP, pak pakety putující sítí, obsahují zdrojovou i cílovou IP adresu, což zcela vylučuje anonymitu. Pokud je komunikace na internetu zprostředkována mezi dvěma nebo více počítači, tak jsou jednotlivé zprávy přednášeny pomocí datagramů. Každý z datagramu obsahuje zdrojovou a cílovou IP adresu, z čehož plyne, že na libovolném uzlu, přes který prochází naše data, jde získat zdrojovou i cílovou IP adresu. Pokud si tedy chceme zajistit na síti anonymitu, bude zapotřebí použít některou s anonymizujících technik, která zabraňuje získávání IP adres. Tuto problematiku řeší síť Tor, která odeslané data zabaluje do jednotlivých slupek podobajících se cibuli (od toho název Onion).



Obrázek č. 1 - Zapouzdření dat v síti [3]

Celou síť tvoří skupina dobrovolníků, kteří představují v síti uzly, které buďto předávají data dále po síti, nebo se jedná o uzly, které zprostředkovávají komunikaci s vnějším internetem. Pokud se tedy připojíme do sítě, vytvoří se spojení, které obsahuje tři výchozí body, z nichž první dva uzly zprostředkovávají komunikaci mezi sebou, a poslední uzel komunikuje s výstupním serverem.



Obrázek č. 2 - Typy uzlů v Tor síti [3]

Pokud tedy odešleme požadavek na server, naše data se zašifrují a odešlou k prvnímu uzlu. Ten zná pouze naši IP adresu, ale obsah dat, který odesíláme, je šifrován. V dalším bodě dorazí naše data ke druhému uzlu, který již nezná ani naši IP adresu, ani obsah dat ale ví pouze, kam má data předat. Teprve až konečný uzel rozšifruje obsah zprávy, ovšem ten již nezná adresu odesilatele a pouze předá data do přístupného internetu. Tento princip činnosti

prakticky vylučuje jakýkoliv odposlech sítě, jelikož žádný z uzlů nevidí dále než před sebe tj. pouze ví, kam má data dále poslat, ale již neví, odkud data přišla. Jediná možnost je ta, že by případný útočník měl pod kontrolou všechny tři uzly, což je ale vzhledem k velikosti sítě velmi nepravděpodobné. [2] [3]

Jak již bylo řečeno, síť Tor používá ke své funkci takzvané uzly. V současné době je funkčních asi 6 000 uzlů, které jsou rozmístěny po celém světě. Samotné uzly představují lidé, kteří dobrovolně propůjčují svoji šířku internetového pásma jakožto uzel v sítí. Tyto uzly v síti nemají žádný speciální hardware, ale pouze konfigurační software přímo od Toru. Software, který Tor používá je volně dostupný včetně zdrojového kódu, takže je možno jej modifikovat dle svých potřeb. Celá síť se neustále rozrůstá, přibývají nové a nové uzly, což v praxi znamená, že bude daleko větší problém vystopovat jednotlivé uživatele, protože bude více cest, ze kterých si bude možnost vybrat. [4]

Obrázek č. 3 - Tor směrovače ve světě [21]

K šifrování dat se používá kryptografický protokol TLS (*Transport Layer Security*). Po navázání spojení mezi dvěma uzly si můžou navzájem prokázat totožnost druhé strany na základě certifikátu. Při vytváření spojovací cesty se používá asymetrické šifrování, které funguje na veřejném a soukromém klíči. Veřejný klíč je součástí certifikátu a používá se taky jako ověření identity stanice. Z principu asymetrického šifrování je zřejmé, že všechna

data jsou zašifrována veřejným klíčem a rozšifrována mohou být jen pomocí soukromého klíče druhé strany. Pokud nemáme odpovídající soukromý klíč k šifrované zprávě, tak je jakékoliv rozšifrování dat vyloučeno. [5] [6]

1.2 Prvky sítě Tor

Adresářový server (*directory servers*) V síti tor funguje více adresářových serverů z důvodu bezpečnosti a každý z nich má svůj podepisovací kryptologický systém. Adresářový systém udržuje seznam aktivních uzlů v síti a také obsahuje informace pro ostatní prvky sítě.

Směrovač sítě (*onion router*) Vytváří spojovací uzly v síti Tor a zároveň zprostředkovávají komunikaci na síti.

Skryté služby (*hidden services*) Cílem je, aby při komunikaci se serverem neznal klient IP adresu serveru a naopak. Pokud by klient znal IP adresu serveru, na kterou přistupuje, mohlo by docházet častěji k tzv. DDos útokům. Skrytou službu si lze představit jako intranet celé sítě. Můžete zde vytvářet vlastní webové stránky a další věci.

Mosty (*bridges*) Jedná se o směrovače, které nejsou uvedeny v hlavním adresáři Tor. V některých zemích můžou poskytovatelé internetového připojení záměrně blokovat hlavní směrovače sítě, ale nemohou blokovat tzv. mosty, o kterých dodnes neexistuje kompletní seznam. [7]

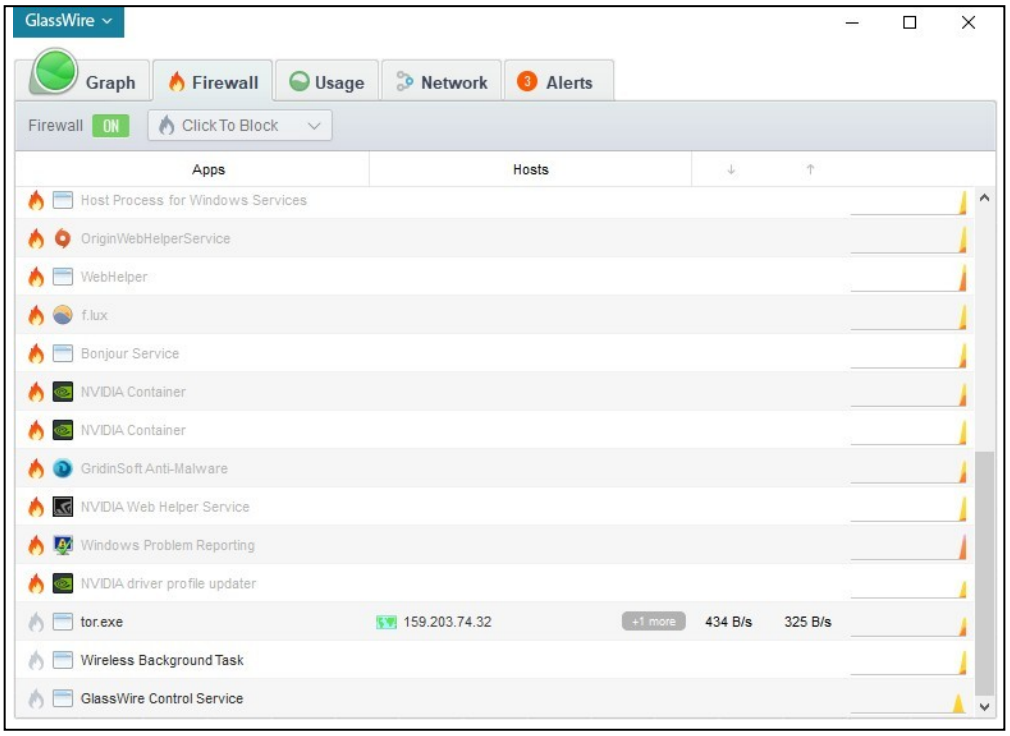
Vstupní strážci (*entry guards*) Může nastat situace, kdy útočník kontroluje směrovač, který jsme si vybrali pro vstup do sítě, a zároveň sleduje námi navštěvované stránky. Z tohoto důvodu se používají tzv. vstupní strážci, kteří fungují jako dlouho stabilní běžící uzly, ze kterých si klienti vybírají začáteční cestu v síti.

Maskování síťového provozu (*traffic morphing*) V případě odposlechu sítě lze zjistit, že TCP pakety v síti Tor mají nejčastější velikost 586 bytů, což by mohlo vést k odhalení provozu. Tor tedy používá tzv. transformace charakteristik síťového provozu, mezi které patří např. odlišná délka paketových mezer, změna rozložení délek, apod. [8] [9]

II. PRAKTICKÁ ČÁST

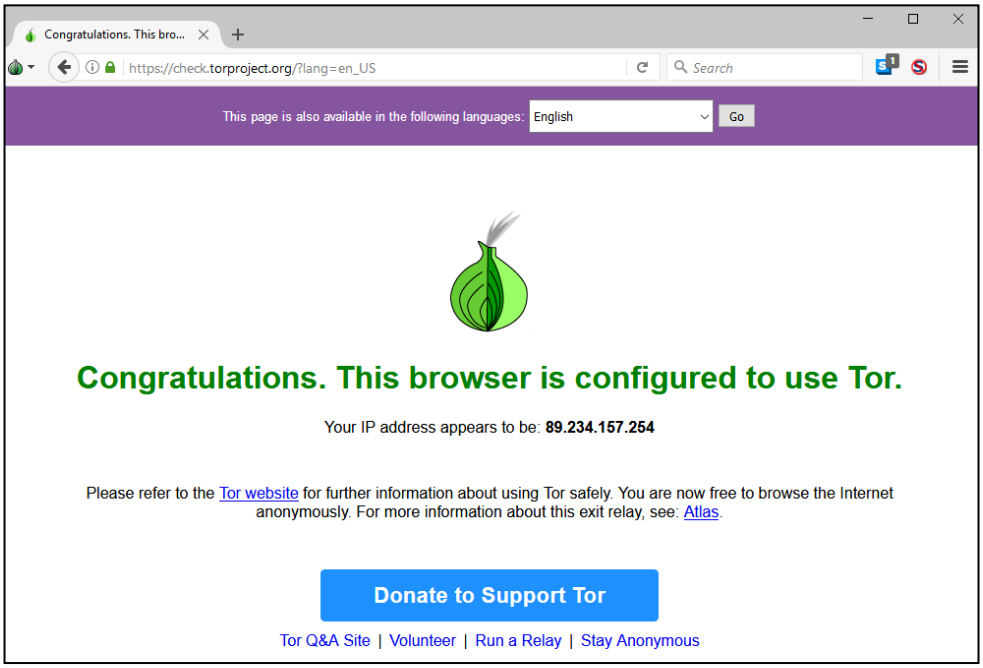
2 TESTOVÁNÍ OKRUHU SÍTĚ

Pro sledování komunikace, která na sítí probíhá, bude použit program WireShark, který patří mezi ty nejčastěji používané analyzátory a paketové sniffery. Podporuje více než 750 síťových protokolů a další jsou přidávány lidmi, kteří na projektu WireShark spolupracují. Po zapnutí programu a připojení do sítě, se zobrazí obrovské množství protokolů, mezi kterými je potřeba najít ty správné. Pro pomoc při filtrování bude použit program GlassWire, který obsahuje firewall, díky kterému je možno zablokovat veškerý síťový provoz všech spuštěných aplikací, které právě běží. Na obrázku č. 4 je možno vidět blokovaný provoz všech spuštěných aplikací. Vyfiltrované pakety přes WireShark mohou mít shodné přenosové protokoly, které používá Tor Browser, tudíž by bylo nutné mezi nimi hledat ty správné. Proto je lepší si datovou komunikaci programu na síti zablokovat a nechat povolené jen ty, které pochází s Toru. [10]



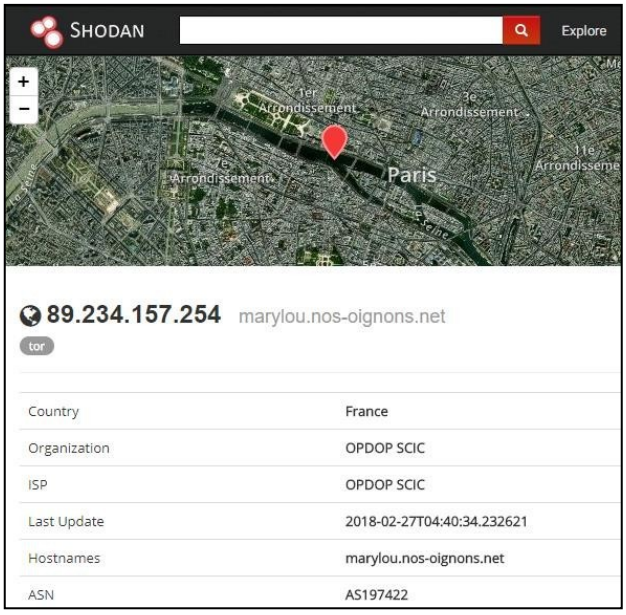
Obrázek č. 4 – Blokovaný síťový provoz programem GlassWire

Při zapnutí Tor Browseru je možnost pod tlačítkem *Test Tor Network Settings* otestovat, zda je prohlížeč správně nakonfigurován k použití sítě. Je zde uvedena i IP adresa, která ovšem jakkoliv nesouvisí s adresou konkrétního uživatele. A to proto, že pokud tuto IP adresu použijeme jakožto zdrojovou IP adresu v programu WireShark a jako cílovou nastavíme první uzel, přes který prochází komunikace, pak program nezaznamená žádný pohyb paketů po síti.



Obrázek č. 5 – Test internetového nastavení v prohlížeči Tor

Z několika testů, které byly provedeny, vyplynulo, že IP adresy, které Tor generuje, pochází z Paříže, nebo z jeho předměstí. Na obrázků č. 6 lze vidět lokalitu dané IP adresy, kterou Tor přidělil prohlížeči.

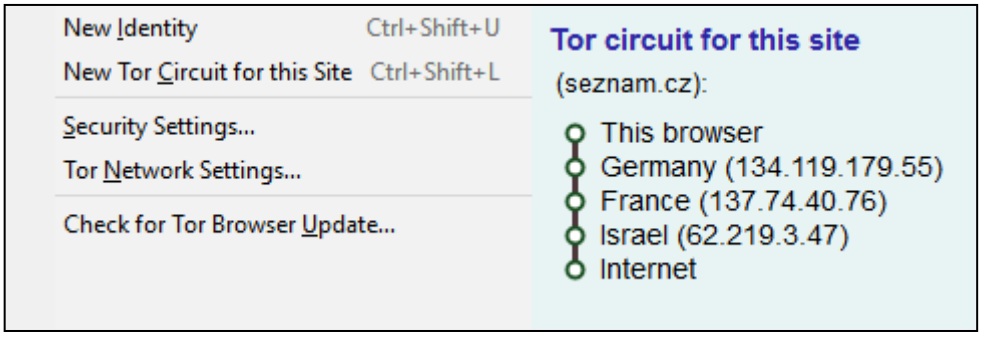


Obrázek č. 6 – Lokalita IP adresy [22]

Z principu činnosti celého systému, na kterém Tor pracuje, vyplývá, že by jednotlivé uzly neměly vidět dále, než před sebe a tedy, že komunikaci bude možno zaznamenat pouze mezi zdrojem a prvním uzlem tedy mezi *entry guard.* Komunikace mezi prvním a druhým uzlem, druhým a třetím uzlem, ani mezi prvním a třetím uzlem by teoreticky neměla být zjištěna.

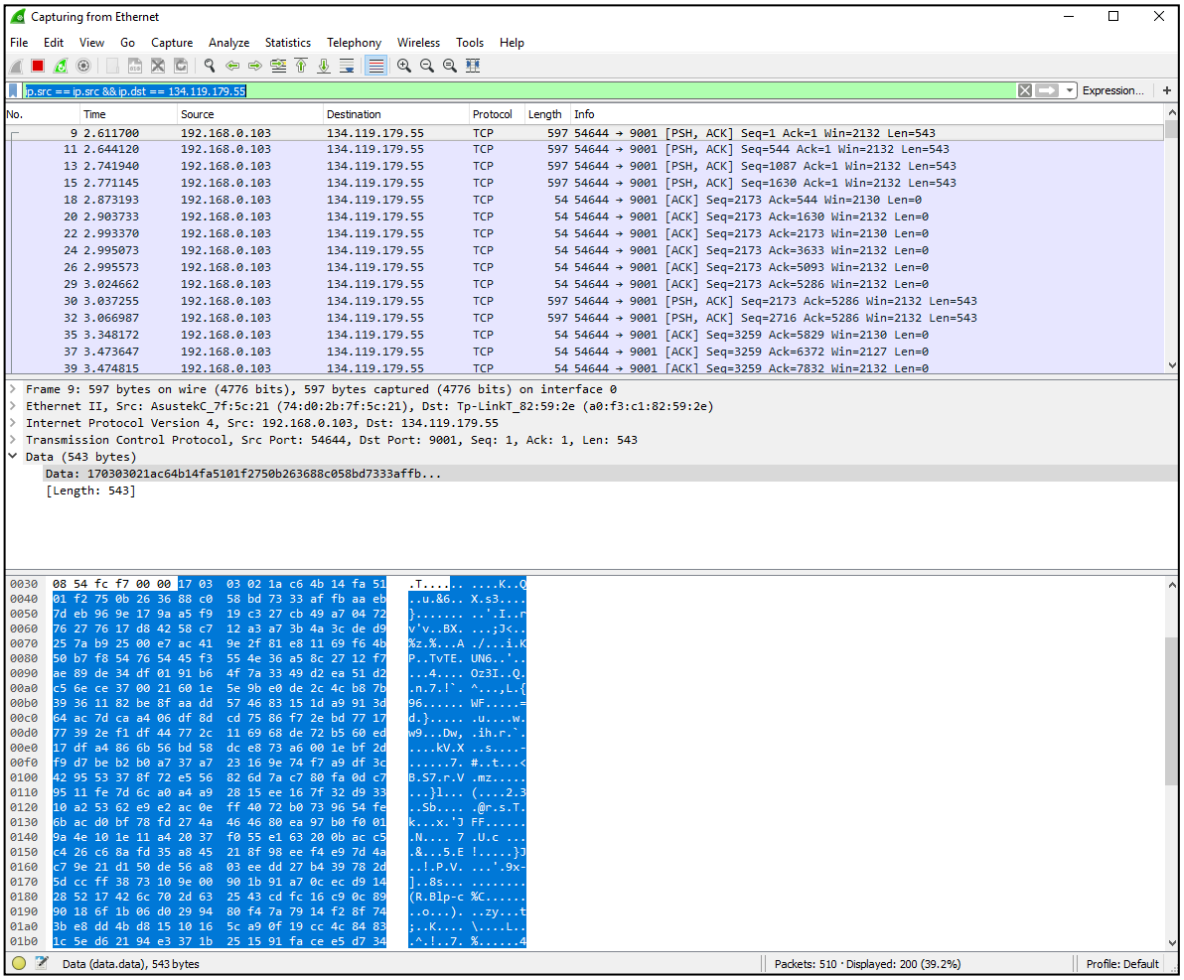
Po zapnutí prohlížeče nám Tor přidělí tři IP adresy, s čehož první je vstupní uzel, druhý je prostřední uzel a třetí je výstupní uzel. Bylo vypozorováno, že IP adresa prvního, tedy vstupního uzlu se pro daný prohlížeč mění jen zřídka. Ovšem IP adresa prostředního a výstupního uzlu se mění zhruba každé 3 minuty, což znamená, že je potřeba jednotlivé testy udělat co nejrychleji, aby se uzly nestihly změnit.

2.1 První test



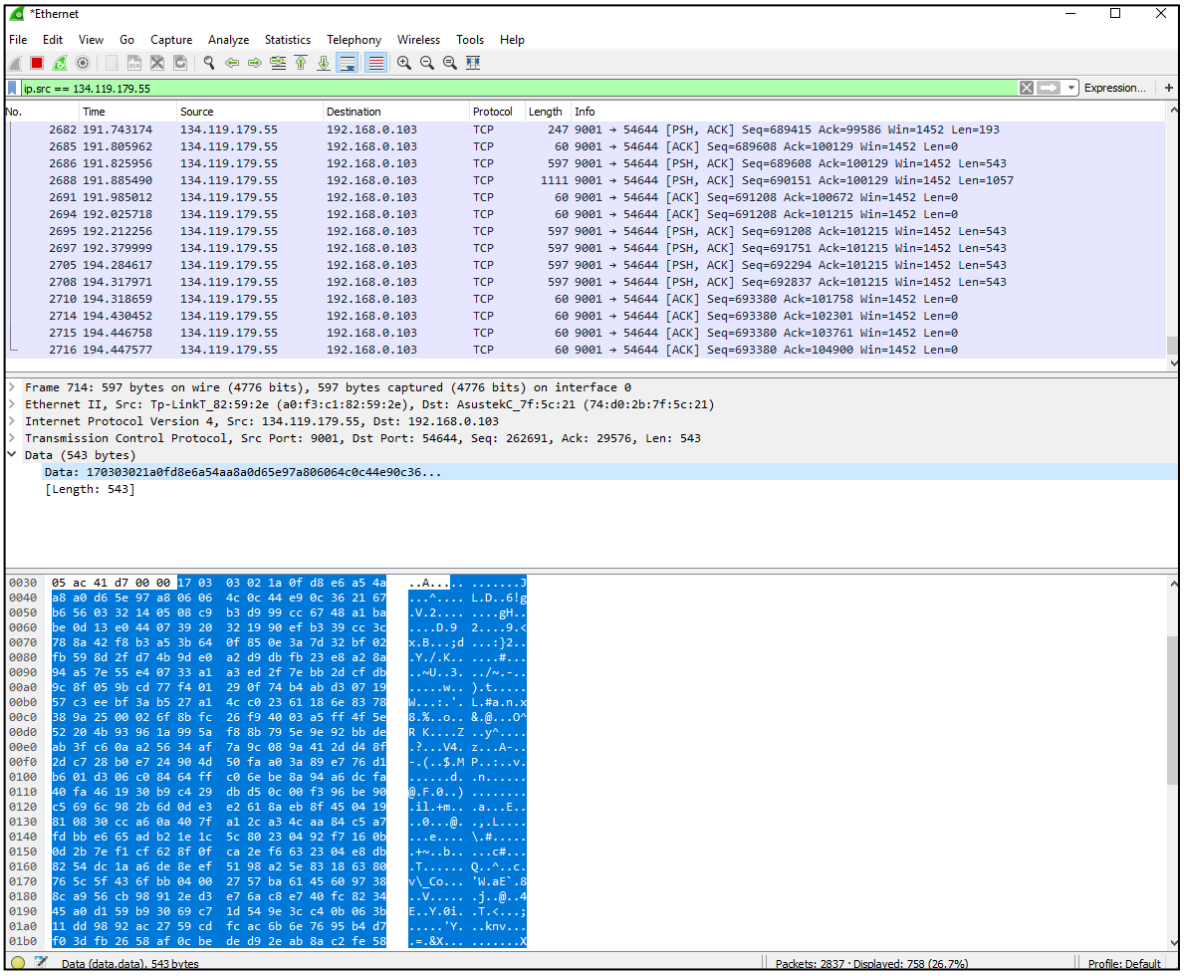
Obrázek č. 7 - Propojovací okruh v prvním testu

Pro testování síťové komunikace bude použita adresa zdroje a adresa prvního cíle, tedy **134.119.179.55**. Příkazem *ip.src==ip.src* nastavíme zdrojovou adresu na náš počítač a následně příkazem *ip.dst==134.119.179.55* nastavíme program tak, aby komunikace probíhala pouze mezi zdrojem a prvním uzlem. Jednotlivý princip komunikace se bude opakovat pro každý uzel zvlášť. V druhém bodě bude nastavena stejná adresa zdroje a změní se pouze cíl, který bude odpovídat IP adresy Francie a ve třetím kroku IP adrese Israele. V jednotlivých mezikrocích bude testován i obracený postup, tedy že jako adresa zdroje bude nastaven jednotlivý uzel, jelikož zde musí být ošetřeno i to, že i při zpáteční cestě datagramu nelze komunikaci zachytit. Komunikaci, která probíhá od veřejného internetu k jednotlivému uživateli zpět, by měla jít zachytit pouze mezi vstupním uzlem a zdrojem.



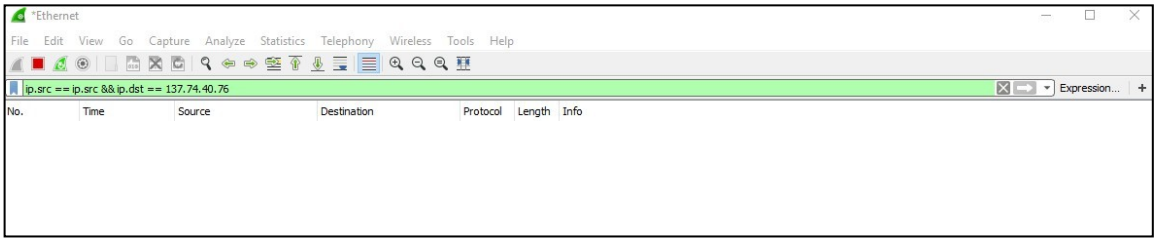
Obrázek č. 8 – Zachycená komunikace mezi zdrojem a prvním uzlem

Na obrázku č. 8 lze vidět síťovou komunikaci, kterou program WireShark zachytil. Pakety po síti doopravdy běží, což potvrzuje spojení mezi zdrojem a prvním uzlem. V další části bude testován provoz mezi zdrojem a prostředním uzlem. Mezi kterými by komunikace neměla probíhat, protože prostřední uzel vidí pouze před sebe a nemůže tedy posílat pakety zpět uzlu prvnímu.



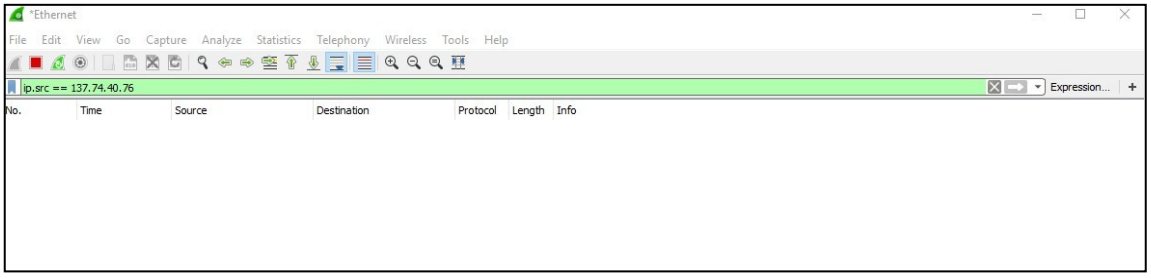
Obrázek č. 9 – Zachycená komunikace prvního uzlu

Na obrázku č. 9 lze ze zachycené komunikace vyčíst, to jak probíhá komunikace mezi prvním uzlem a cílem. Komunikaci zde lze zachytit, jelikož požadavek, který se přes síť posílá, se musí vrátit k tomu, kdo ho odeslal. V následující části bude proveden test komunikace mezi ostatními uzly, a u každého z uzlů bude proveden i opačný postup. Tak jako u prvního uzlu, tedy že jako adresa zdroje bude použit právě onen uzel, který bude testován. Lze zde předkládat, že by nemělo k žádné komunikaci docházet, jelikož jak již bylo řečeno, uzly nevidí dále než před sebe. Pokud by došlo k zachycení paketu, který by se nacházel např. mezi zdrojem a výstupním uzlem, znamenalo by to, že by zde mohlo docházet k odposlechu sítě. Tedy, že by potencionální útočník mohl zjistit zdroj i cíl komunikace.



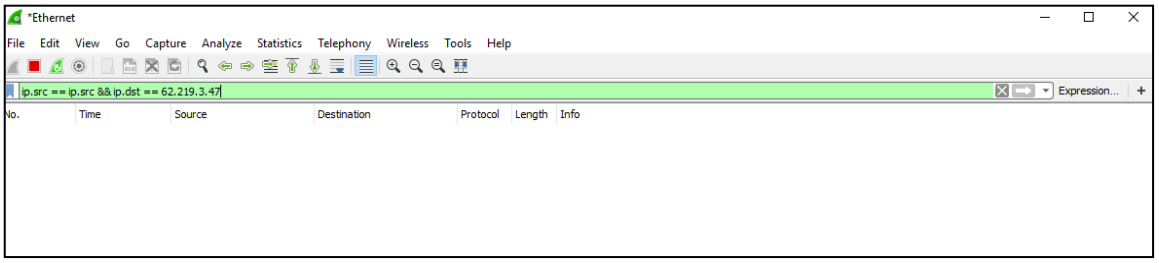
Obrázek č. 10 – Komunikace mezi zdrojem a prostředním uzlem

Síťový provoz běžel více než minutu a podle předpokladu nebyla zachycena žádná komunikace mezi zdrojem a prostředním uzlem. Z toho vyplývá, že prostřední uzel vůbec neví, odkud komunikace pochází, ale ví pouze, kam má data předat.

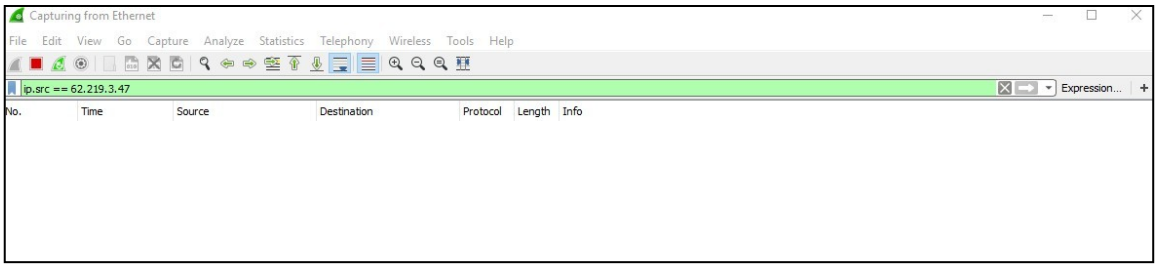


Obrázek č. 11 – Zachycená komunikaci prostředního uzlu

Na obrázku č. 11 lze vidět obrácený postup, zde se filtrují pakety, které pochází od prostředního uzlu. Síťový provoz byl spuštěný 5 minut a nebyl zachycen jediný paket, který by měl IP adresu prostředního uzlu.



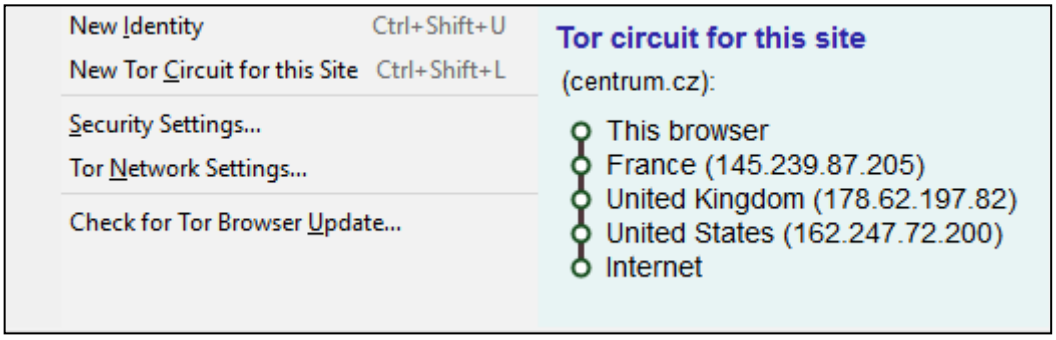
Obrázek č. 12 – Komunikace mezi zdrojem a výstupním uzlem



Obrázek č. 13 – Zachycená komunikace výstupního uzlu

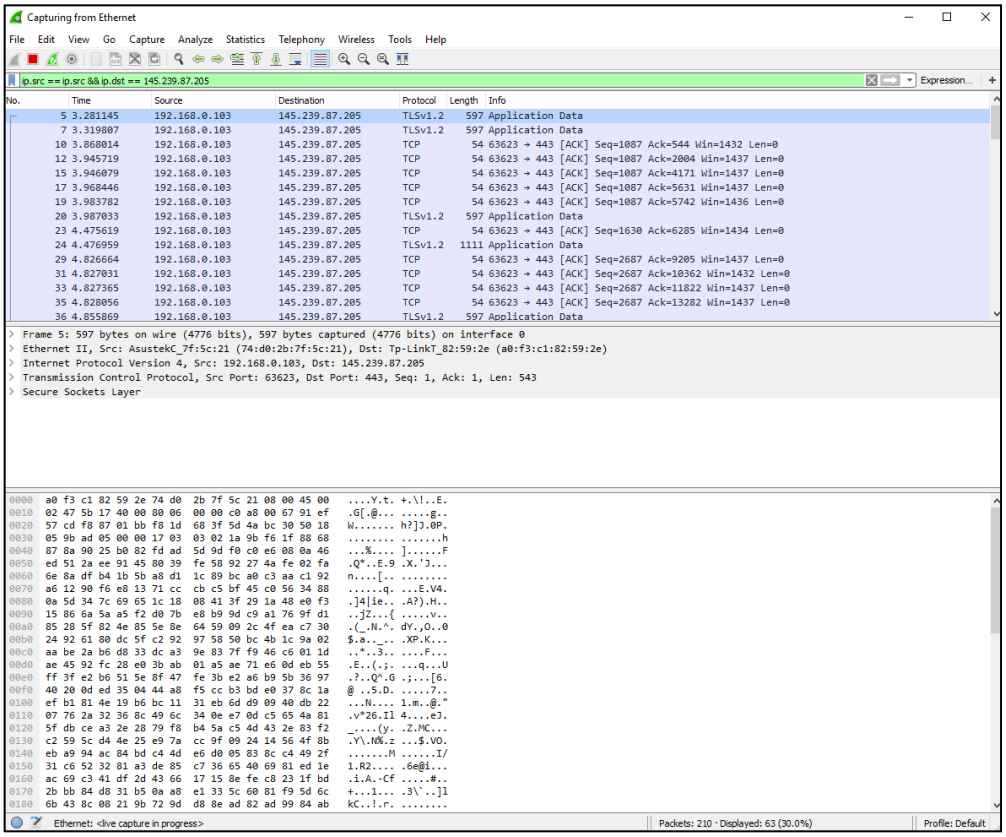
Na obrázku č. 12 lze vidět výsledky komunikace mezi zdrojem a výstupním uzlem, tedy že zde k žádné komunikaci nedochází. Obrázek č. 13 ukazuje, že nebyla zachycena komunikace ani směrem zpět. První test, který zde byl proveden, poukazuje na to, že komunikaci lze skutečně zachytit pouze mezi zdrojem a první uzlem. Popsaný princip komunikace v první části odpovídá naměřeným výsledkům. Provedeme tedy druhý test, který bude na stejném principu, jako ten první, zde bude pouze změněna adresa prvního uzlu. Lze předpokládat, že výsledky budou obdobné, jako tomu bylo u prvního testu.

2.2 Druhý test

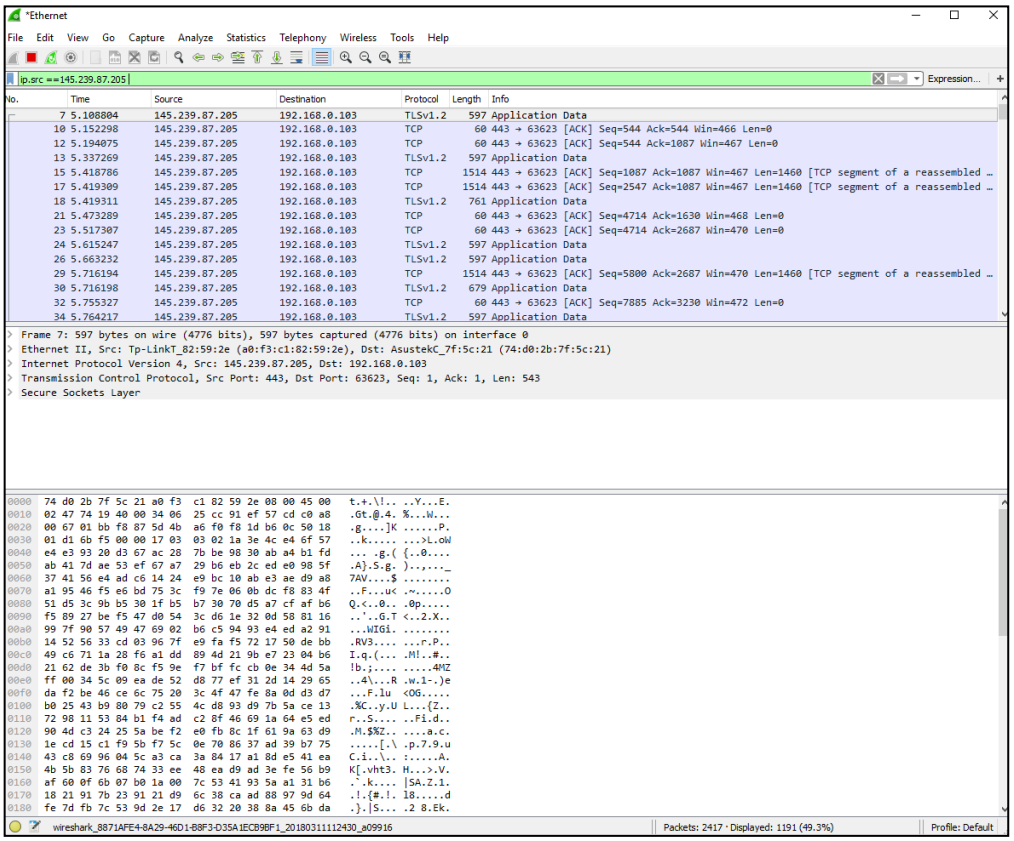


Obrázek č. 14 – Propojovací okruh ve druhém testu

Pro skutečné ověření funkce bude provedeno více testů, abychom potvrdili, že komunikaci lze doopravdy zachytit pouze mezi zdrojem a prvním uzlem. Při druhém použití prohlížeče se nastavil nový *entry guard* na území Francie, prostřední pak na Velkou Británii a výstupní na Spojené státy americké.

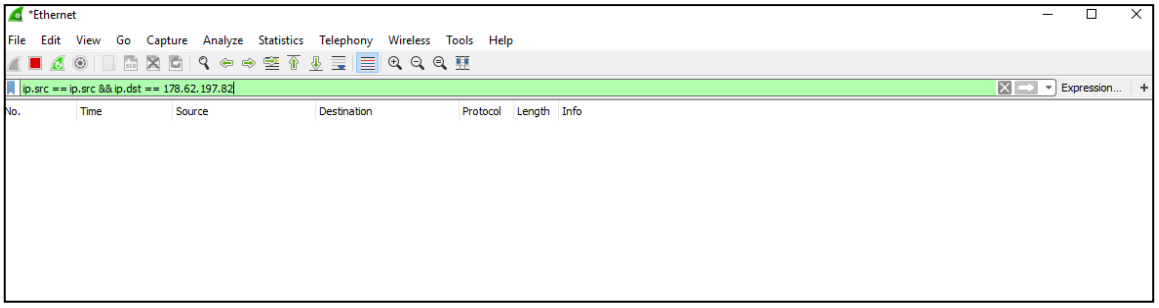


Obrázek č. 15 – Komunikace mezi zdrojem a vstupním uzlem

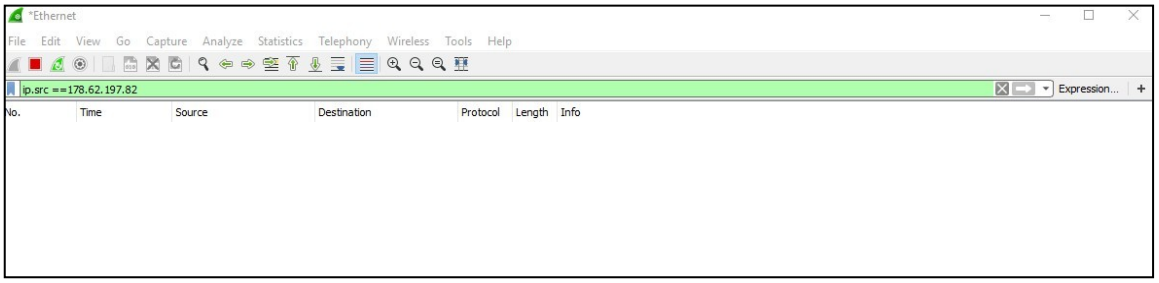


Obrázek č. 16 – Zachycená komunikace první uzlu v druhém testu

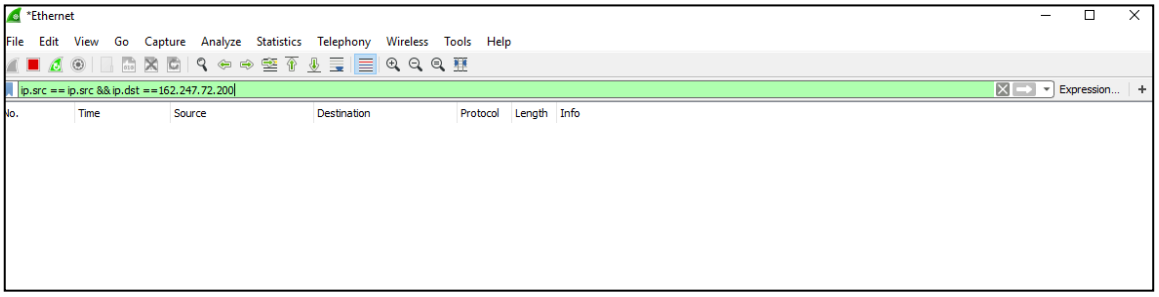
Obrázek č. 15 a 16 ukazují to, že stejně jako v prvním testu zde byla zachycena komunikace. Komunikace probíhá opět oboustranně, tedy od zdroje k prvnímu uzlu a zpět. Lze předpokládat, že výsledky testů týkajících se další uzlů dopadnou stejně jako v testu prvním.



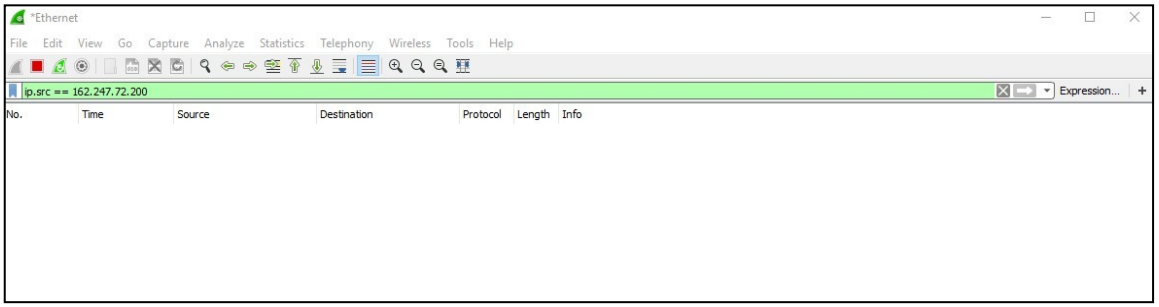
Obrázek č. 17 – Komunikace mezi zdrojem a prostředním uzlem



Obrázek č. 18 – Zachycená komunikace prostředního uzlu



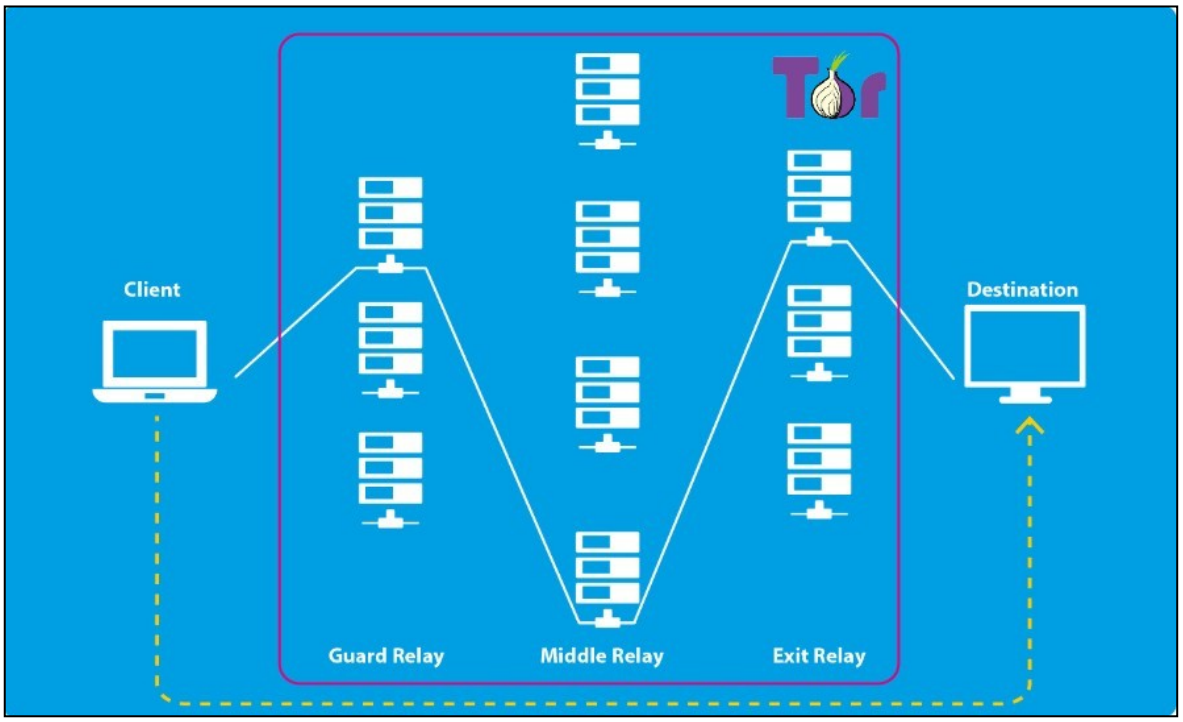
Obrázek č. 19 – Komunikace mezi zdrojem a výstupním uzlem



Obrázek č. 20 – Zachycená komunikace výstupního uzlu

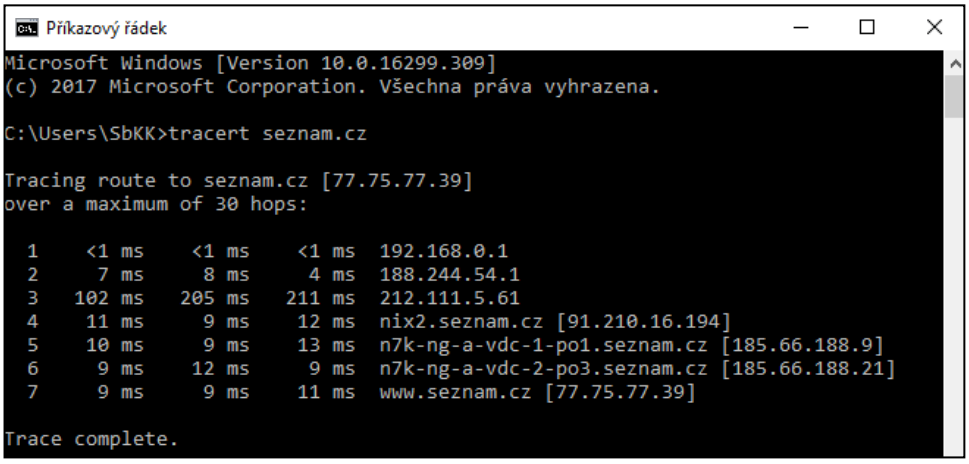
Testování komunikace v druhé části pobíhalo stejně, jako v části první, tedy že každý jednotlivý uzel byl propojen s IP adresou zdroje a čekalo se, jestli pakety přes tyto dvě IP adresy prochází. Bylo znova zjištěno, že uzly sítě nevidí dále než před sebe a tedy, že komunikaci lze detekovat pouze mezi zdrojem a prvním uzlem sítě. Na obrázku č. 17, 18, 19 a 20 jsou výsledky jednotlivých testů. Testy v druhé části dopadly stejně, jako testy v části první. Z výsledků všech testů, které zde byly uvedeny, vyplývá, že komunikaci skutečně nelze zachytit nikde jinde, než mezi zdrojem a prvním uzlem. Pro útočníka to znamená, že odposlech jednotlivých uzlů by pro něho nemělo žádný význam, jelikož jak již bylo řečeno, jednotlivé uzly nevidí dále než před sebe, a mění svoji lokalitu zhruba každé tři minuty. V následující části bude proveden test, ve kterém se bude zjišťovat, zda náhodou neexistuje nějaká postranní cesta, přes kterou by mohla komunikace probíhat. Jednoduše bude zjištěna IP adresa domény, na kterou se prohlížeč připojuje. Do příkazové řádky se napíše příkaz *tracert www.seznam.cz*, který vyhledá výslednou IP adresu.

2.3 Postranní kanál v síti



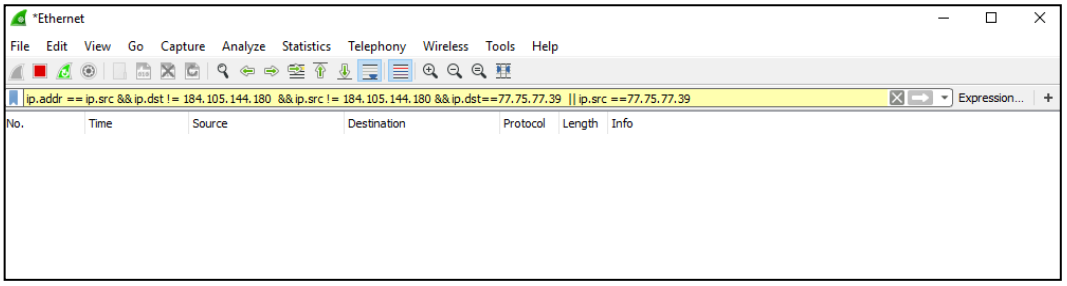
Obrázek č. 21 - Hledaný postraní kanál v komunikaci

Na obrázku č. 21 je žlutě znázorněn postranní kanál, který bude hledán. Pokud bude zamezena veškerá síťová komunikace kromě Toru, tak by mezi IP adresou zdroje a IP adresou cílové domény neměly jít zachytit žádné pakety. Případné zachycení paketů by znamenalo, že existuje i další cesta, přes kterou může komunikace probíhat.

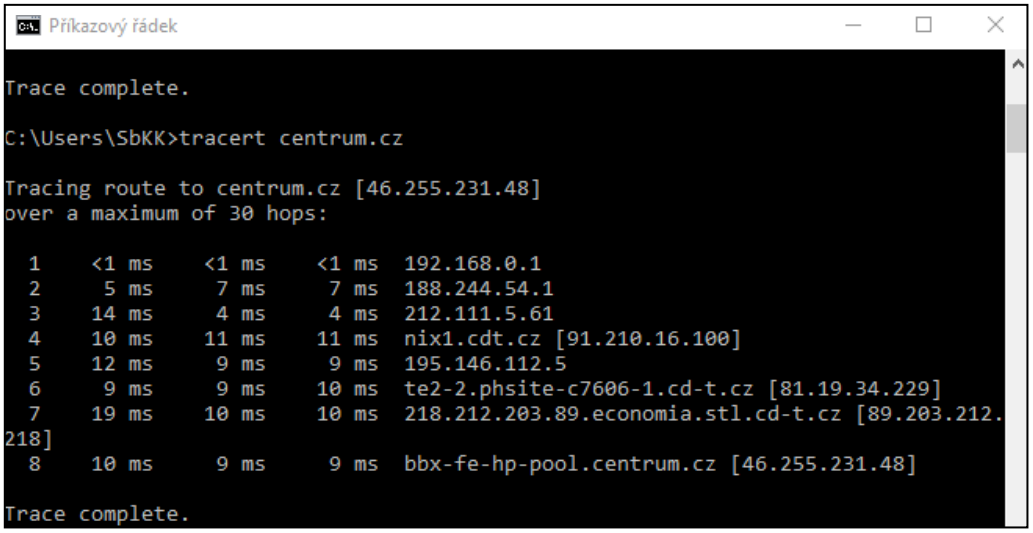


Obrázek č. 22 – Filtrování IP adresy domény www.seznam.cz

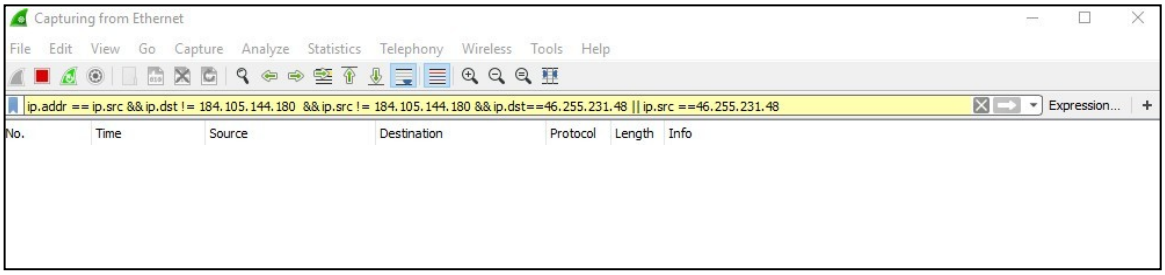
Filtr v programu WireShark se nastaví tak, že se přidá adresa zdroje. Dále se nastaví to, že adresa prvního uzlu nesmí být zdrojová ani cílová a také se nastaví pouze IP adresa, kterou vyfiltrovala příkazová řádka. IP adresa, kterou vyfiltrovala příkazová řádka, se pro jistotu nastaví jako zdrojová i cílová, aby pak šlo s jistotou říci, jestli pakety tečou od zdroje k seznamu, nebo od seznamu ke zdroji.



Obrázek č. 23 – Zachycená komunikace



Obrázek č. 24 – Filtrování IP adresy domény centrum.cz



Obrázek č. 25 – Zachycená komunikace

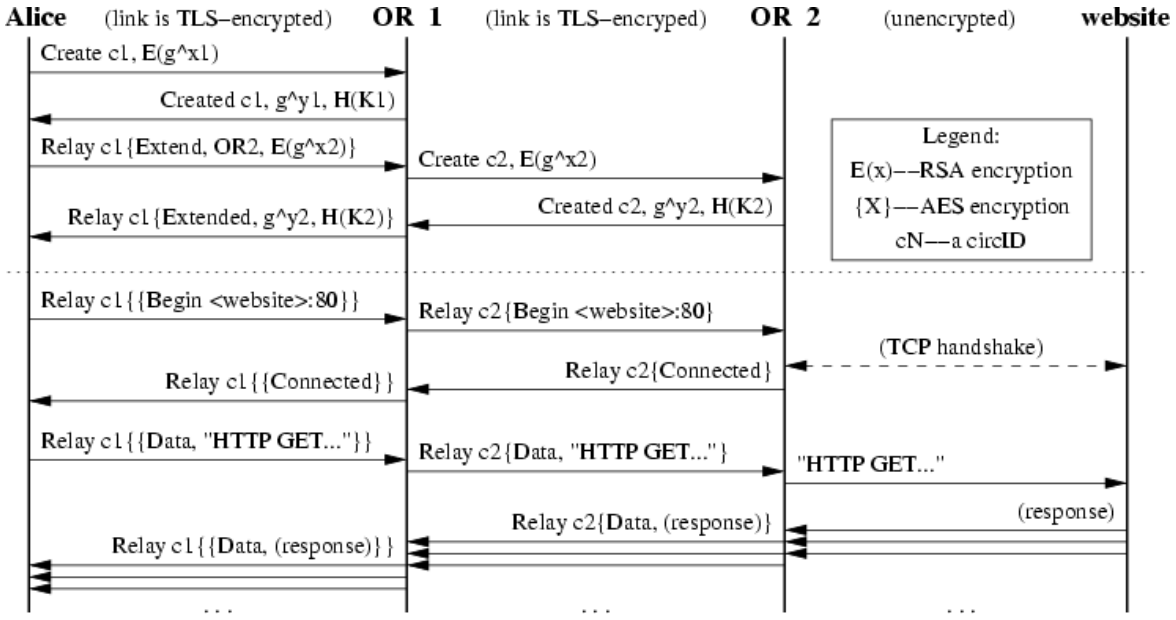
Ze zachycené komunikace na obrázcích č. 22 a 23 lze vidět, že neprobíhá žádná komunikace mezi IP adresou uvedené domény a zdrojem. Z uvedených výsledků testů lze s jistotou vyloučit jakýkoliv postraní kanál, přes který by mohla komunikace probíhat. Výsledky ze všech testů tedy potvrzují princip komunikace, který byl popsán v prvním bodě a vylučuje i odposlech sítě, který by probíhal před jednotlivé uzly. [11]

2.4 Zhodnocení výsledků měření

Předešlé testy, které byly provedeny, potvrdily princip komunikace, který byl uveden v prvním bodě. Bylo prokázáno, že jednotlivé uzly komunikace nevidí dále, než před sebe. Komunikaci tedy šlo skutečně zachytit pouze mezi zdrojem a prvním uzlem. Z případného odposlechu sítě mezi uživatelem a prvním uzlem by útočník dokázal vyvodit pouze to, že uživatel ze sítí Tor pouze komunikuje. Nedokázal by zjistit, s kým uživatel komunikuje. Jednotlivé uzly nevidí dále než před sebe, takže odposlech jednotlivých uzlů by útočníkovi nedal žádné informace o tom, s kým uživatel komunikuje. Teprve až poslední uzel předá data do internetu. Případné zachycení komunikace z výstupního uzlu by útočníkovi nezdělolo nic o tom, odkud data přišla. Bylo prokázáno, že neexistuje ani žádný postranní kanál, přes který by mohla data procházet. Z výsledků tedy vyplývá to, že sít Tor se chová skutečně tak, je popsáno v její dokumentaci.

2.4.1 Bezpečnost délky klíče

V prvním bodě se Onion proxy Alice dotáže na databázi Tor, která Onion proxy odtajní pozici jednotlivých uzlů, přes které bude komunikovat. Po obdržení lokality jednotlivých uzlů vytvoří Onion proxy spojení mezi jednotlivými uzly.



Obrázek č. 26 – Princip komunikace [12]

Data jsou zašifrována pomoci šifry RSA a dále přenášena pomoci Diffie Hellmanovy výměny klíčů, která se nazývá *Curve25519*. Délka použité šifry u RSA je 1024 bitů, která již v dnešní době není považována na bezpečnou. V roce 2007 byl za 11 měsíců pomocí hrubé síly rozšifrován 700 bitový klíč RSA. V dnešním roce 2018, kdy výkon výpočetní techniky exponenciálně roste, by rozšifrování stejné délky klíče trvalo kratší dobu. Profesor kryptografie Arjen Lenstra již v roce 2007 odpověděl na dotaz, zda je šifra 1024 bitová šifra RSA mrtvá, odpověď zněla *ano*. [12] [13] [14]

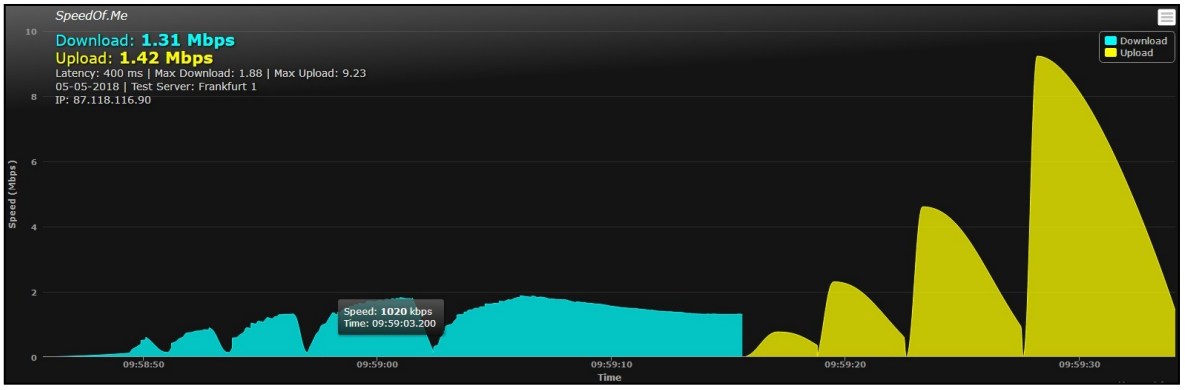
When asked whether 1024-bit RSA keys are dead, Lenstra said: The answer to that question is an unqualified yes. Hopefully, my bank is paying attention to these developments.

Síť tor by se tedy v budoucnu měla zaměřit na zvětšení klíče používaného u RSA. Dnešní minimum, které se považuje za bezpečnou velikost u RSA, je 2048 bitů, avšak podporované velikosti jsou i 4096 a 8192 bitů. [15]

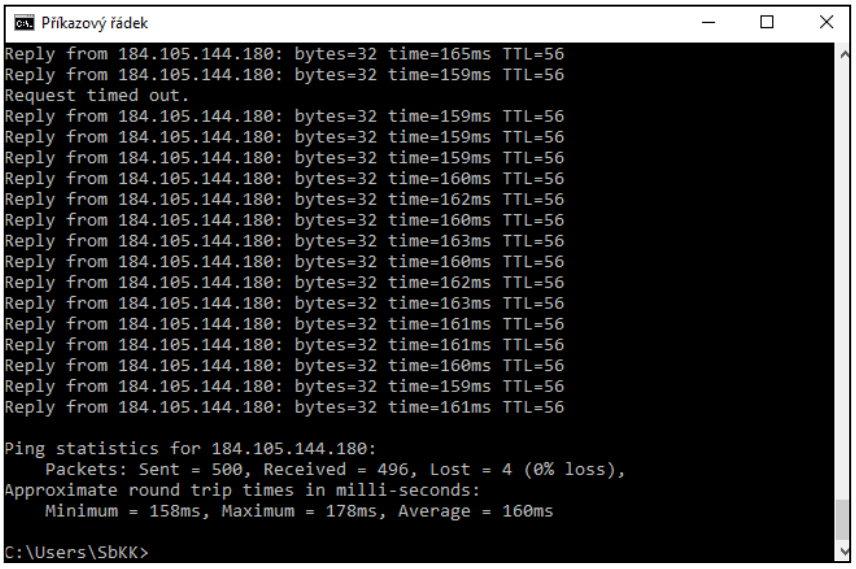
3 TESTY STABILITY SPOJENÍ

Test stability zde bude sloužit pro zjištění odezvy. V prvním kroku se zjistí odezva prohlížeče v Tor síti. Odezva, která bude naměřena, je ovšem měřena od konkrétního uživatele až po cílovou doménu. Bude tedy nutné první zjistit odezvu přes Tor prohlížeč a dále zjistit odezvu od konkrétního uživatele k prvnímu uzlu. Po zjištění celkové odezvy sítě a následně prvního uzlu, je potřeba odečíst hodnotu odezvy prvního uzlu od odezvy celé Tor sítě. Výsledná odezva, která vznikne tímto odečtením, bude již přímo souviset s vnitřkem uzlu vytvořeného Tor sítí. Pro testování stability budou provedeny čtyři testy, kde každý z nich bude vykonán v jiném časovém intervalu.

3.1 První test



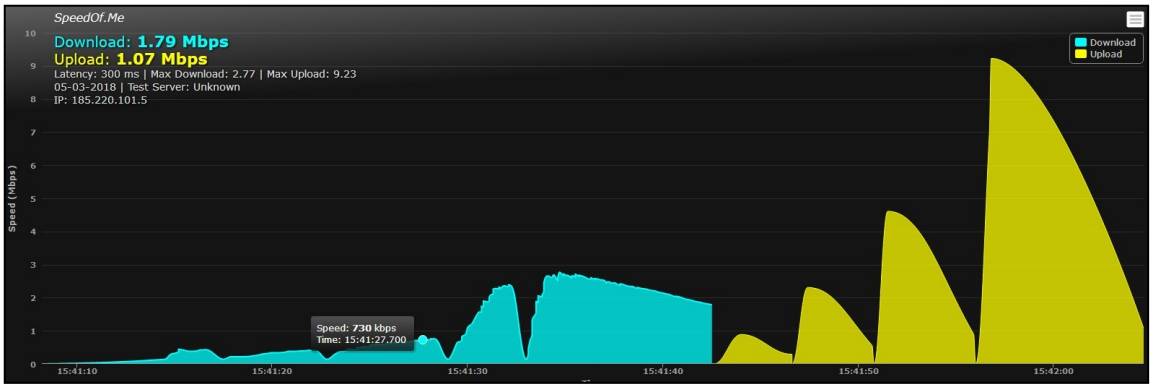
Obrázek č. 27 – Test odezvy přes Tor prohlížeč 12:10 UTC [18]



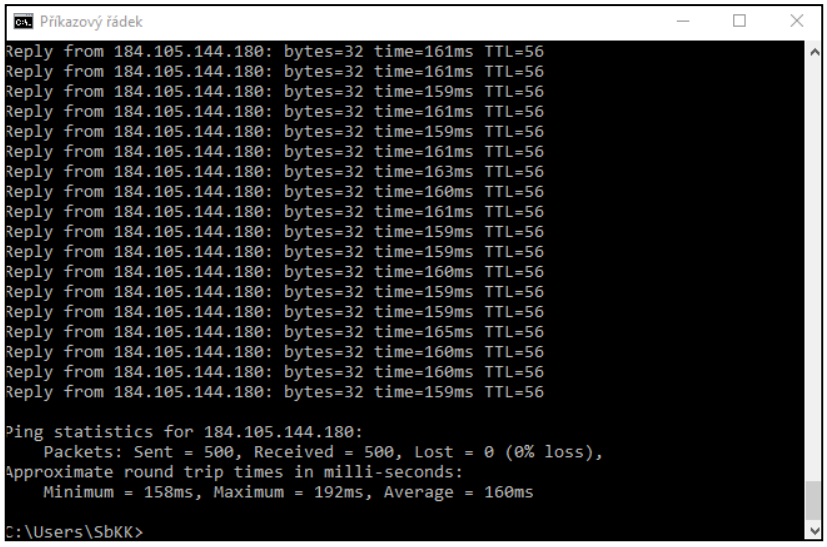
Obrázek č. 28 – Odezva prvního uzlu v síti 12:10 UTC [18]

Na obrázku č. 26 můžeme vidět test odezvy přes Tor prohlížeč. Odezva je poměrně vysoká s toho důvodu, protože požadavek na cílovou doménu musí projít přes všechny tři uzly a až poté je vpuštěn do internetu. Již první uzel na obrázku č. 27 má poměrně vysokou odezvu a to je z toho důvodu, že konkrétně tento uzel má nižší šířku pásma, než uzly ostatní. [16]

3.2 Druhý test



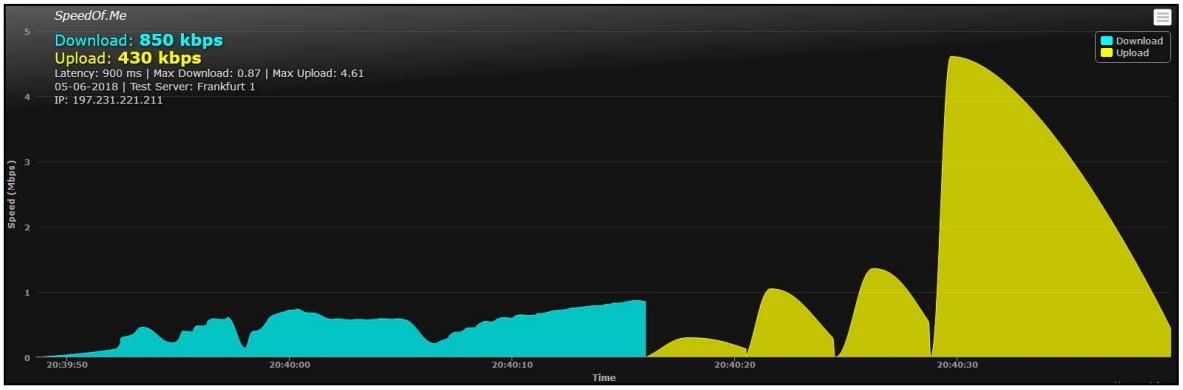
Obrázek č. 29 – Test odezvy přes Tor prohlížeč 17:40 UTC [18]



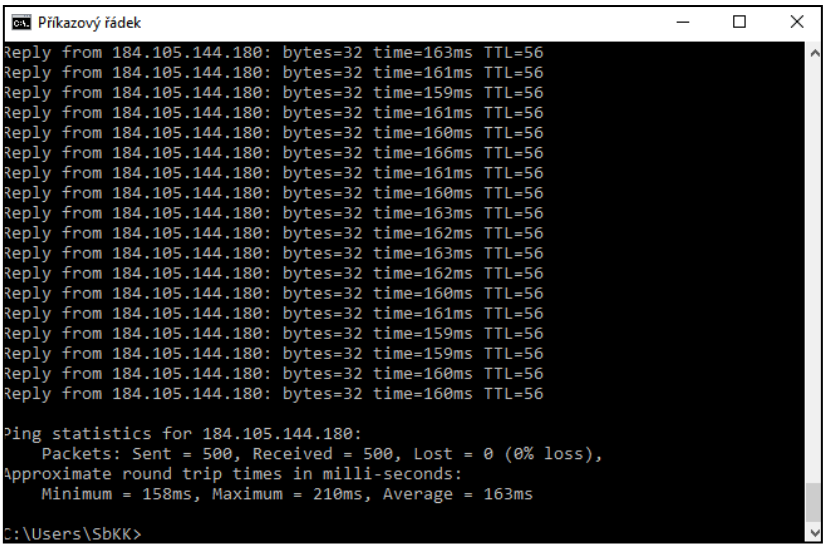
Obrázek č. 30 – Odezva prvního uzlu v síti 17:40 UTC

Na obrázku č. 29 a 30 můžeme vidět obdobné testy, jako v prvním případě. Odezva prvního uzlu se liší pouze nepatrně. Další test bude proveden v nočních hodinách. Lze předpokládat zvýšení odezvy, jelikož v nočních hodinách je více uživatelů aktivních, než přes dopolední hodiny.

3.3 Třetí test

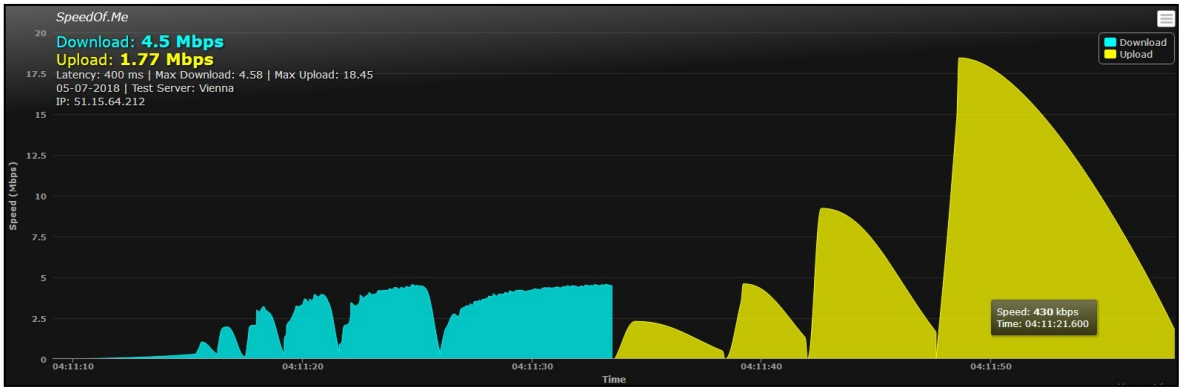


Obrázek č. 31 – Test odezvy přes Tor prohlížeč 22:40 UTC [18]

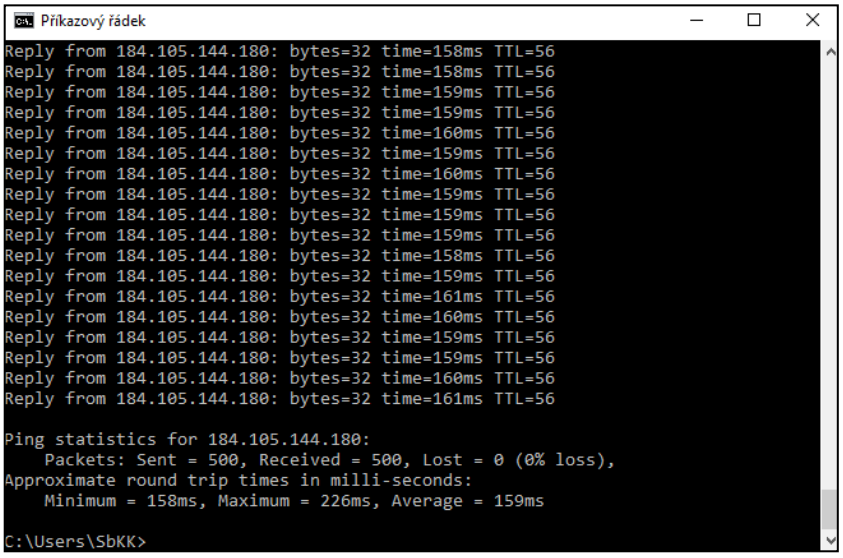


Obrázek č. 32 – Odezva prvního uzlu v síti 22:40 UTC

3.4 Čtvrtý test



Obrázek č. 33 – Test odezvy přes Tor prohlížeč 6:15 UTC [18]



Obrázek č. 34 – Odezva prvního uzlu v síti 6:15 UTC

3.5 Výsledky měření testů stability

Tabulka č. 1 – Výsledky měření testů odezvy (Vlastní zpracování)

Čas[*UTC*]	**Průměrná odezva Tor sítě[*ms*]**	**Průměrná odezva prvního uzlu[*ms*]**	**Vnitřní odezva sítě Tor[*ms*]**
12:10	400	160	240
17:40	300	160	140
22:40	900	163	737
6:15	400	159	241

V tabulce č. 1 můžeme vidět naměřené hodnoty odezvy. Největší odezva v Tor síti byla dle předpokladů v nočních hodinách, kdy je aktivních nejvíce uživatelů. Naopak nejmenší odezva byla naměřená v odpoledních hodinách. Jak již bylo řečeno, vnitřní odezva Tor sítě byla zjištěna odečtením odezvy naměřené na internetové stránce www.speedof.me, od odezvy první uzlu. Výsledná odezva, která je uvedená v pravé části tabulky již přímo souvisí s vnitřním okruhem v Tor síti, na který je konkrétní uživatel připojený. Ani v jednom z případů nebyla zaznamenána ztráta paketu, nebo jakýkoliv další výpadek sítě. Z uvedených výsledků vyplývá, že směrovače, na kterých byl test proveden, se chovají stabilně a nemají žádné výpadky, které by zpomalovaly použití sítě.

Tabulka č. 2 – Výsledky měření testů Download/Upload (Vlastní zpracování)

Čas[*UTC***]**	**Download[***Mbps***]**	**Upload[***Mbps***]**
12:10	1,31	1,42
17:40	1,79	1,07
22:40	0,85	0,43
6:15	4,5	1,77

V uvedené tabulce č. 2 můžeme vidět poměr rychlosti stahování k poměru rychlosti nahrávání. Nejlepší poměr těchto dvou hodnot byl naměřen v ranních hodinách.

4 ROZŠÍŘENÍ ANONYMIZAČNÍCH TECHNIK

Základní myšlenkou Onion routingu je anonymizace uživatelů a ochrana jejich osobních údajů. Zároveň poskytuje uživatelům možnost uniknout z normálního internetu do světa, ve kterém neplatí stejná pravidla, jako v klasickém internetu. Ovšem i samotná síť Tor trpí chybami, které by v budoucnu mohly znamenat pro uživatele rizika. V následujícím kroku budou uvedeny jednotlivé vylepšení anonymizačních technik, které by v samostatné síti pomohly zlepšit její funkčnost a zároveň bezpečnost uživatelů.

4.1 Zvětšení uživatelské komunity

První vylepšení nesouvisí ani tak s anonymitou, jakožto s fungováním celé sítě. Již od počátku vzniku sítě, byl Tor postaven na jednotlivých uživatelích, kteří samotnou síť tvořili a rozvíjeli. Největší hrozbou pro celý Tor je nezájem uživatelů o jeho používání. Přeci jen samotné cibulové uzly tvoří uživatelé, kteří dobrovolně propůjčují svoji šířku internetového připojení lidem, kteří síť používají. Bez těchto uzlů by síť jako taková fungovat nemohla. V budoucnu by se tedy uživatelé této sítě měli snažit o její propagaci mezi veřejnost, která o ní doposud neví. Čím více uživatelů bude síť používat, tím více aktivních uzlů se bude vytvářet. Zvětšení počtů aktivních uživatelů bude znamenat jednak zrychlení celé sítě a také zlepšení bezpečnosti, protože přes velkou odolnost celé sítě bude problém vystopovat informace o konkrétním uživateli. Počet aktivních uzlů se rok od roku zvětšuje, což má za následek zlepšení bezpečnostních podmínek pro uživatele. [17]

4.2 Zvětšení délky používaného klíče

Jednou z dalších možností, na které by se komunita Tor sítě měla v budoucnu zaměřit a tlačit s ní na vývojáře, je zvětšení délky používaného klíče při šifrování. Stávající použitá délka klíče RSA při šifrování je 1024 bitů což je v dnešní době naprosto nedostačující. [13] [18]

ENCRYPTION SCORECARD

ENCRYPTION STANDARD	SAFE TO USE	KNOWN WEAKNESS	DATA SECURITY HORIZON
❌ 1024-bit encryption	⛔ UNSAFE	🎛 Trapdoor Primes, Known Exploits	0 Days
❌ 2048-bit encryption	⛔ LIKELY UNSAFE	⛔ STATE LEVEL RESOURCES	2-5 Years
✅ 4096-bit encryption	✅ SAFE FOR NOW	✅ QUANTUM COMPUTING	10+ Years
❓ NSA Quantum Resistant Algorithm	❓ UNKNOWN	❓ Unknown Backdoors	50+ Years
❓ Quantum Encryption	✅ PROVABLY SAFE	❓ NOT AVAILABLE YET	INFINITE

Obrázek č. 35 – Bezpečnost použitých délek klíčů [20]

Na obrázku č. 34 můžeme vidět bezpečnost jednotlivých délek klíčů. Již použitá délka klíče 2048 bitů není v dnešní době považována za bezpečnou. Komunita sítě Tor by tedy měla tlačit na vývojáře, aby při Diffie Helmanově výměně klíčů použili u šifry RSA délku klíče 4096 bitu, která je v dnešní době považována za bezpečnou.

4.3 Zamezení síťového provozu ostatních programů

V internetovém prohlížeči Tor by se v budoucnu mohlo nacházet vylepšení, které by po aktivaci zamezilo veškerý síťový provoz ostatních aplikací. Funkcionalita by byla následující. Po spuštění internetového prohlížeče Tor by se zobrazila tabulka s funkcí skenování síťového provozu, která by našla všechny programy a aplikace, které jakýmkoliv způsobem komunikují s internetem. Po ukončení skenování by se zobrazila možnost pro blokování síťového provozu ostatních aplikací. Příslušný uživatel by poté mohl zamezit komunikaci buďto všech programů a aplikací aktivních v sítí, nebo jen těch, které si sám vybere. Toto vylepšení by samozřejmě neumožňovalo blokování síťového provozu funkcím operačního systému, které zprostředkovávají komunikaci s internetem. Blokování síťového provozu ostatních aplikací by pro uživatele znamenalo zlepšení bezpečnosti při používání prohlížeče Tor. Zamezení síťového provozu by také znamenalo celkové zrychlení prohlížeče, protože ostatní aplikace by zbytečně nebrzdily síťový provoz.

ZÁVĚR

Cílem bakalářské práce bylo objasnit fungování Tor sítě a také popsat princip anonymizace uživatelů. Celá teoretická část se tedy objas, jak síť funguje a jakým způsobem probíhá anonymizace. Dále zde byly popsány základní prvky sítě Tor a také ukázána mapa, na které byly zobrazeny jednotlivé směrovače, které fungují jako uzly sítě.

Praktická část bakalářské práce se skládala z ověření principu komunikace, který byl popsán v první části. V úvodu praktické části byl znovu nastíněn princip ve kterém by jednotlivé uzly zpuštěných neměly vidět dále než před sebe. Podle toho se odvíjel první test, který ověřil to, že uživatel ve vytvořeném okruhu, který vygeneroval Tor, může komunikovat jen a pouze s prvním uzlem. Komunikace s prostředním a výstupním uzlem tedy nemůže probíhat, což je znázorněno na jednotlivých obrázcích. V neposlední řadě bylo ověřeno to, že neexistuje ani žádný postranní kanál, přes který by mohla komunikace procházet. Bylo tedy prokázáno, že síť Tor skutečně funguje tak, jak je popsáno v její dokumentaci. Při procházení dokumentace bylo zjištěno, že Tor používá při šifrování délku klíče, která v dnešní době není považována za bezpečnou.

V předposledním bodě bakalářské práce probíhalo měření stability spojení. Testy probíhaly tak, že se v prvním bodě zjistila IP adresa prvního uzlu, na který se posílaly požadavky, a měřil se čas, za který požadavek dorazí zpět. Zjistila se odezva v Tor prohlížeči, která se následně odečetla od odezvy prvního uzlu. Odečtením těchto dvou hodnot vznikla odezva, která patřila vytvořenému okruhu sítě.

V poslední části bakalářské práce pak byly navrženy další možnosti jak rozšířit anonymizaci uživatelů. Největším problémem pro samotnou síť jsou uživatelé, kteří ji tvoří. Úbytek uživatelů by pro síť znamenal v první řadě úbytek směrovačů a také zhoršení bezpečnostních podmínek. V posledním bodě bylo upozorněno na nedostačující délku klíče RSA, která se používá při šifrování a také byl navržený jednoduchý program, který by blokoval síťovou komunikaci ostatních programů a tím zajistil lepší spojení se síti.

SEZNAM POUŽITÉ LITERATURY

[1] FEDERRATH, Hannes. *Designing privacy enhancing technologies: International Workshop on Design Issues in Anonymity and Unobservability*, *Berkeley, CA, USA, July 25-26, 2000 : proceedings.* New York: Springer, 2001. ISBN 35-404-1724-9.

[2] INTERNET PROTOCOL: PROTOCOL SPECIFICATION [online]. 1981 [cit. 2018-05-17]. Dostupné z: https://tools.ietf.org/html/rfc791

[3] COUFAL, Zdeněk a Libor POLČÁK. *Anonymizační síť Tor: Technická zpráva* [online],[cit.2018-05-17]. Dostupné z: http://www.fit.vutbr.cz/research/pubs/index.php?file=%2Fpub%2F10626%2Ftr.pdf&id=10626

[4] WRIGHT, Jordan. *How Tor Works: Part One* [online]. 2015 [cit. 2018-05-18]. Dostupné z: https://jordan-wright.com/blog/2015/02/28/how-tor-works-part-one/

[5] RESCORLA, E. a T. DIERKS. *The Transport Layer Security (TLS)*. EITF [online]. 2008, , 104 [cit. 2018-02-20].

Dostupné z: https://tools.ietf.org/html/rfc5246

[6] DINGLEDINE, Roger, Nick MATHEWSON a Steven MURDOCH. *Second-Generation Onion Router* [online]. 2014,21 [cit. 2018-02-05]. Dostupné z: http://sec.cs.ucl.ac.uk/users/smurdoch/papers/tor14design.pdf

[7] Tor: Bridges [online]. 2018 [cit. 2018-05-18]. Dostupné z: https://www.torproject.org/docs/bridges#PluggableTransports

[8] POLČÁK, Libor. *Základní informace o síti Tor* [online]. 2017, , 18 [cit. 2018-05-18].Dostupnéz:http://www.fit.vutbr.cz/research/pubs/index.php?file=%2Fpub%2F11513%2Ftr.pdf&id=11513

[9] KADIANAKIS, George. *Packet Size Pluggable Transport and Traffic Morphing* [online]. 2012, , 7 [cit. 2018-05-18].

Dostupné z: https://research.torproject.org/techreports/morpher-2012-03-13.pdf

[10] OREBAUGH, Angela. *Wireshark a Ethereal: kompletní průvodce analýzou a diagnostikou sítí.* Brno: Computer Press, 2008, 61 s. ISBN 978-802-5120-484.

[11] *How to Use TRACERT to Troubleshoot TCP/IP Problems in Windows* [online]. [cit. 2018-05-18]. Dostupné z: https://support.microsoft.com/EN-US/help/162326

[12] DINGLEDINE, Roger a Paul SYVERSON. *Tor: The Second-Generation Onion Router* [online]. 2014 [cit. 2018-05-18]. Dostupné z: https://svn.torproject.org/svn/projects/design-paper/tor-design.html#

[13] KIRK, Jeremy. Researcher: *RSA 1024-bit Encryption not Enough* [online]. 2007 [cit. 2018-05-18]. Dostupné z: https://www.pcworld.com/article/132184/article.html

[14] DINGLEDINE, Roger a Nick MATHEWSON. *Tor Protocol Specification* [online]. [cit. 2018-05-18]. Dostupné z: https://gitweb.torproject.org/torspec.git/tree/tor-spec.txt

[15] COFFEY, Neil. *RSA key lengths* [online]. 2012 [cit. 2018-05-18]. Dostupné z: https://www.javamex.com/tutorials/cryptography/rsa_key_length.shtml

[16] TorStatus - *Tor Network Status. TorStatus* - Tor Network Status [online]. Copyright © 2006 [cit. 13.05.2018]. Dostupné z: https://torstatus.blutmagie.de/

[17] Tor Metrics [online]. The Tor Project, 2018 [cit. 2018-05-18]. Dostupné z: https://metrics.torproject.org/networksize.html

[18] LUTHER, MARTIN. *Encryption is Very, Very Hard to Crack* [online]. 2015 [cit. 2018-05-18]. Dostupné z: https://www.voltage.com/encryption/encryption-is-very-very-hard-to-crack/

[19] SpeedOf. *SpeedOf* [online]. [cit. 2018-05-18]. Dostupné z: https://speedof.me/

[20] *Security Alert: Encryption is not very hard to crack* [online]. 2016 [cit. 2018-05-18]. Dostupné z: https://steemit.com/encryption/@blockcodes/encryption-is-not-very-hard-to-crack-1024-bit-2048-bit-4096-bit-encryption-and-nsa-quantum-resistant-algorithm-encryption

[21] *Word City Map of Tor Nodes* [online]. 2018 [cit. 2018-05-18]. Dostupné z: https://tormap.void.gr/

[22] *Shodan* [online]. 2018 [cit. 2018-05-20]. Dostupné z: https://www.shodan.io/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

TOR	THE ONION ROUTING
IP	INTERNET PROTOCOL
TLS	TRANSPORT LAYER SECURITY
RSA	Rivest–Shamir–Adleman
Curve25519	Označení pro Eliptickou křivku
DH	Diffieho-Hellmanova výměna klíčů

SEZNAM OBRÁZKŮ

SEZNAM TABULEK