**Česká zemědělská univerzita v Praze**

**Provozně ekonomická fakulta**

**Katedra informačních technologií**


**Bakalářská práce**

# Naše digitální stopa na počítači a na Internetu

**Štefan Tomovič**

# ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

# ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Štefan Tomovič

Informatika

Název práce
**Naše digitální stopa na počítači a na Internetu**

Název anglicky
**Digital footprint on own computer and the Internet**

---

**Cíle práce**
Hlavním cílem práce je charakterizovat jednotlivé typy digitálních stop a představit nejvýznamnější metody ochrany osobních dat. Dílčím cílem bakalářské práce je srovnání schopností a možností nástrojů k ochraně osobních dat na základě analýzy prostředí, infrastruktury, požadavků a možností navrhnout a implementovat vhodné řešení individuální ochrany dat.

**Metodika**
Metodika řešené problematiky bakalářské práce je založena na studiu a analýze odborných informačních zdrojů, ale také na praktických zkušenostech s jednotlivými produkty. Pomocí této metodiky je navrhnuto a implementováno vhodné řešení ochrany digitální stopy. Na základě syntézy teoretických poznatků a přínosů vlastního řešení budou formulovány závěry bakalářské práce.

**Doporučený rozsah práce**
30-40 stran

**Klíčová slova**
digitální stopa, ochrana dat, hesla, cookies

---

**Doporučené zdroje informací**


DOSEDĚL, T. Počítačová bezpečnost a ochrana dat. Brno: Computer Press. 2004. 190 str. ISBN 80-251-0106-1.

ECKERTOVÁ, L., DOČEKAL, D. Bezpečnost dětí na internetu: rádce zodpovědného rodiče. 1. vyd. Brno: Computer Press. 2013. 224 str. ISBN 978-80- 251-3804-5.

HOOG, A. Android Forensics. Waltham: Syngress Publishing. 2011. 432 str. ISBN 9781597496513.

LANGE, M. C. S., NIMSGER, K. M. Electronic evidence and discovery: What every lawyer should know now. Washington: American Bar Association. 2009. 429 pages. ISBN 9781604423822.

LARRY D., LARS D. Digital Forensics for Legal Professionals. 1^st edition. Waltham: Syngress Publishing. 2011. 368 pages. ISBN 9781597496438.

MATOUŠKOVÁ, M., HEJLÍK, L. Osobní údaje a jejich ochrana. 2. vydání. Praha: ASPI, Wolters Kluwer. 2008. 468 str. ISBN 978-80-7357-322-5.

PORADA, V. , RAK, R. Teorie digitálních stop a její aplikace v kriminalistice a forenzních vědách. Karlovarská právní revue 4/2006. ISSN 1801-2191.


---

**Předběžný termín obhajoby**
2015/16 LS – PEF

**Vedoucí práce**
Ing. Čestmír Halbich, CSc.

**Garantující pracoviště**
Katedra informačních technologií

Elektronicky schváleno dne 28. 10. 2015

**Ing. Jiří Vaněk, Ph.D.**

Vedoucí katedry

Elektronicky schváleno dne 10. 11. 2015

**Ing. Martin Pelikán, Ph.D.**

Děkan

V Praze dne 05. 03. 2016

# Čestné prohlášení

Prohlašuji, že svou bakalářskou práci Naše digitální stopa v počítači a na Internetu jsem vypracoval samostatně pod vedením Ing. Čestmíra Halbicha CSc. a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 10.3.2016 _____

**Poděkování**

Touto cestou bych rád poděkoval vedoucímu mé bakalářské práce Ing. Čestmíru Halbichovi CSc., za odborné konzultace a vedení této práce.

# Naše digitální stopa na počítači a na Internetu

**Souhrn**

Hlavním cílem bakalářské práce je charakterizovat jednotlivé typy digitálních stop a popsat metody ochrany dat. K této ochraně jsou použity freeware nástroje. V teoretické části jsou popsány typy digitálních stop, možnosti zneužití digitálních stop a útoky na dané počítače nebo data. V další kapitole jsou popisovány použité freeware nástroje. Jejich základní charakteristika a jejich využití. V praktické části jsou tyto nástroje rozděleny do tří skupin, podle oblasti problémů, které řeší. Podle oblasti jsou zvolena i kritéria. V poslední části jsou tyto nástroje testovány mezi sebou, použitím vícekriteriální analýzy.

**Klíčová slova:** digitální stopa, ochrana dat, hesla, cookies

# Digital footprint on own computer and the Internet

**Summary**

The main aim of this thesis is to characterize various types of digital footprint and describe the methods of data protection. This conservation uses freeware tools. The theoretical part describes the types of digital footprint, the possibility of misuse of digital footprint and attacks on the computer or data. The next chapter describes the used freeware tools. Their basic characteristics and their use. In the practical part, these instruments are divided into three groups, depending on the region the problems that it solves. According regions are also chosen criteria. In the last part, these instruments are tested each other, using multi criteria analysis.

**Keywords**: digital footprint, data protection, passwords, cookies

# Obsah

# Seznam obrázků



# Seznam tabulek

# 1. Úvod

Od roku 2013 se sice nárůst nově připojených uživatelů k síti internet snižuje, ale stále zde mluvíme o stotisících nových uživatelů každý rok. Za rok 2015 přibylo 300 tisíc lidí. Mezi roky 2000 a 2012 byl každoroční nárůst v procentech dvojciferný, za rok 2014 to bylo 8,6% a o rok později 8,1%. Na konci roku 2015 mělo přístup k internetu 3,2 miliardy lidí, což je přibližně 47% lidské populace. České republice patří 29. místo v počtu pevných připojení k vysokorychlostnímu internetu. Na 100 obyvatel to dělá 27,6 těchto připojení. I z této studie lze vyčíst, že každý rok se na internetu objeví statisíce nových uživatelů, kteří možná nemají ani nejmenší tušení o tom, co jim zde může hrozit. Ať se jedná o odcizení dat, vytvoření a zneužití profilu nebo útoků na samostatné počítače v síti. Je zřejmé že v České republice nárůst nových uživatelů nebude tak velký, ale i tak si myslím, že zpracování tématu digitální stopy bude prospěšné i pro stávající uživatele. Je i dosti pravděpodobné, že někteří budou překvapeni tím, co vše lze o nich zjistit, už jen pouhém "brouzdáním" po internetu.

I toto bylo jedním z hlavních důvodů proč jsem si zvolil toto téma. Rozšířit povědomí lidí, uživatelů o možných hrozbách, které jim na internetu hrozí. V teoretické části budou popsány různé hrozby, jako je sledování uživatelů, krádež identity, útoky na dané počítače v síti nebo modifikace dat. K tomu bude potřeba i popsat pojmy jako cookies a pixelové tagy. V praktické části je hlavním cílem představit možnosti jak se uživatel může bránit pomocí různých freeware nástrojů. Dílčím podcílem je samostatné testování a srovnávání těchto nástrojů mezi sebou, které vyústí v určitá doporučení.

# 2. Cíl práce a metodika

## 1. Cíl práce

Hlavním cílem této bakalářské práce je charakterizování typů digitálních stop a představení různých freeware nástrojů, pomocí kterých uživatel může minimalizovat svou digitální stopu jak na internetu, tak i ve svém počítači. Dílčím podcílem je rozdělení těchto nástrojů do tří skupin a jejich následné testování. Na základě výsledků testů doporučit dané nástroje či jejich kombinaci.

## 2. Metodika

Metodikou řešení daného problému digitálních stop je studie a analýza informačních zdrojů. Postupem u praktické části bylo samotné testování zvolených freeware nástrojů. Toto testování probíhalo vždy v novém virtuálním stroji s operačním systémem Windows 7. Všechny nástroje byly rozděleny do tří skupin, podle toho, který problém řeší. První skupina se zabývala anonymitou na internetu, druhá zabráněním sledování uživatele a poslední odstraňováním uložených sledovacích zařízení. Pro každou ze skupin byla určená jiná kritéria z důvodu, že každá řeší jiný problém. Porovnání softwaru proběhlo pomocí vícekriteriální analýzy.

# 3. Teoretická východiska

## 1. Digitální stopa v IT

Co to vlastně digitální stopa je? Je to souhrn informací, které po vás zůstávají v internetové síti i poté, co jste se z ní již dávno odpojili. Mohou to ale být i soubory, které vznikli připojením k internetu a jsou uloženy přímo ve vašem zařízení, ze kterého jste se připojili k internetu. Příkladem takových souborů jsou cookies. Digitální stopu lze rozdělit na dva typy.

### 1. Typy digitálních stop

Tyto stopy může uživatel zanechat vědomě i nevědomě. S tím souvisí i základní rozdělení digitálních stop. Ty se rozlišují na takzvané "aktivní digitální stopy" a "pasivní digitální stopy". Rozdíl mezi těmito typy je jednoduchý.

Aktivní digitální stopy jsou zanechávány vědomě. Jde například o příspěvek, který napíšeme, náš komentář pod diskuzí, nahrání fotografie, videa či souboru na sociální síť, či naše osobní webové stránky. Jde tedy o cílené věci, i když uživatel si sám nemusí uvědomovat, že tím za sebou nechává informace, ze kterých se může o něm vytvořit profil. Pomocí aktivní digitální stopy za sebou může zanechat i pasivní stopu.

Opakem jsou pasivní digitální stopy. Ty uživatel nezanechává vědomě a i vzhledem k tomu mohou být více nebezpečné. Mezi tyto nevědomě zanechané stopy patří například záznam aktiv o tom, jaké webové stránky jsme navštívili, co jsme na nich dělali, kolik času jsme na nich strávili, jestli jsme vyplňovali nějaký formulář, ale také sem patří například IP adresa, ze které jsme byli přihlášeni, a z toho vyplívající jméno poskytovatele připojení, lokalizace místa odkud jsme se připojili atd. Takto nasbírané informace mohou být později vůči danému uživateli zneužity.

### 2. Soubory cookies

Za otce cookies je považován Lou Montulli, který začátkem 90. let 20. století měl myšlenku, že by bylo vhodné, kdyby uživatel mohl alespoň částečně pokračovat tam, kde skončil při poslední návštěvě webu. První soubor cookies byl vytvořen v roce 1994 pro prohlížeč Navigator od firmy Netscape Communication, pro kterou v té době Lou Montulli

pracoval. Co to tedy soubor cookies je a k čemu dnes slouží. Je to malé množství dat, která www server pošle prohlížeči, který je následně uloží v počítači daného uživatele. Tato data musí mít určitou strukturu. Tím hlavním je název nebo spíše ID cookie pomocí jehož www server přesně určí o jakého uživatele se jedná. Dále obsahuje samotná data cookie, dobu platnosti, doménu, pro kterou cookie platí.

V souvislosti s cookies vydala Evropská unie směrnici, která vyústila i v novelu našeho zákona č. 468/2011 Sb., o tom, že by uživatel měl být informován, že se na dané stránce používají soubory cookies.

Samozřejmě soubory cookies lze zase rozdělit na 2 skupiny. První skupinu, nebo-li první stranu, tvoří přímo webové stránky, které je používají pro identifikaci uživatele. Druhou skupinu tvoří třetí strany, kterým jde jen o shromažďování informací. Sem řadíme jak marketingové firmy, které to využívají pro behaviorální marketing, ale také i firmy, které data pouze prodávají. Toto sledování napříč internetem se nazývá cross site tracking.

### 3. Pixelové tagy

Pixelový tag je známí také jako internetový tag nebo web beacons. Pixelovým tagem je myšlen velmi malý obrázek o velikosti 1 pixel na 1 pixel, který je umístěn ve zdrojovém kódu webové stránky či emailové zprávy. Stejně jako u cookies rozlišujeme původce tohoto tagu. Může se jednat přímo o daný web (tj. první strana) nebo cizí firma (tj. třetí strana). Tento tag funguje tak, že při otevření webové stránky nebo emailové zprávy, která jej obsahuje, odešle internetový prohlížeč na server požadavek na tento obrázek. Prostřednictvím tohoto požadavku získá server od prohlížeče různé údaje. Mezi těmito údaji se nachází IP adresa daného počítače, datum a čas, URL adresu webové stránky. V případě že daná stránka používá soubory cookies, tak se načte i hodnota z nich. Některé z pixelových tagů dokonce umožní i přesné sledování různých aktiv, včetně toho co uživatel přímo píše nebo jak se pohybuje kurzorem.

### 4. Pluginy sociálních sítí

Pixelový tag je známí také jako internetový tag nebo web beacons. Pixelovým tagem je myšlen velmi malý obrázek o velikosti 1 pixel na 1 pixel, který je umístěn ve zdrojovém kódu webové stránky či emailové zprávy. Stejně jako u cookies rozlišujeme původce tohoto tagu.

Může se jednat přímo o daný web (tj. první strana) nebo cizí firma (tj. třetí strana). Tento tag funguje tak, že při otevření webové stránky nebo emailové zprávy, která jej obsahuje, odešle internetový prohlížeč na server požadavek na tento obrázek. Prostřednictvím tohoto požadavku získá server od prohlížeče různé údaje. Mezi těmito údaji se nachází IP adresa daného počítače, datum a čas, URL adresu webové stránky. V případě že daná stránka používá soubory cookies, tak se načte i hodnota z nich. Některé z pixelových tagů dokonce umožní i přesné sledování různých aktiv, včetně toho co uživatel přímo píše nebo jak se pohybuje kurzorem.

## 2. Digitální stopa v kriminalistice a forenzních vědách

Digitální stopy se také dotýkají kriminalistiky a forenzních věd. V těchto dvou oblastech jsou vnímány především jako důkazní materiál. V kriminalistice je digitální stopa definována jako "*Každé technologické zařízení, které získává, zpracovává, předává nebo uchovává data zanechává záznamy (odrazy) o své činnosti. Tyto záznamy z kriminalistického hlediska jsou stopami."* ( Porada a Rak, 2006, str. 5) [1]Dříve se v kriminalistice používal pojem počítačová stopa. Tento pojem byl používán od druhé poloviny 80. let 20. století. Nyní tento pojem nestačí, protože stopu zanechává mnohem více druhů zařízení než jen počítače. Mezi tyto zařízení můžeme řadit mobilní telefony, notebooky či tablety. Proto se nyní používá pojem digitální stopa. Pracovní skupina Scientific Working Group on Digital Evidence, zkráceně SWGDE, v roce 1999 prezentovala svou definici, která zní: "*Digitální stopa je jakákoliv informace s vypovídající hodnotou, uložená nebo přenášená v digitální podobě.*" ( Porada a Rak, 2006, str. 5)[2] Tato definice je často používána i dnes, protože není specifická pouze pro oblast počítačů, ale dá se použít i pro oblast digitálních přenosů. V kriminalistice se tyto stopy rozdělují do tří základních skupin.

První skupinou jsou takzvané kriminalistické stopy. Tyto stopy se vztahují k vyšetřování trestných činů a přestupků, které jsou specifikované zákonem. U těchto stop dbáme na vysokou kvalitu a objektivitu při jejich získávání a zajišťování.

Druhou skupinu jsou stopy forenzní. Mezi tyto stopy řadíme všechny stopy, které jsou využitelné pro forenzní vyšetřování, ale i pro šetření orgánů činných v trestném řízení. Jde

[1] zdroj: Digitální stopy v kriminalistice a forenzních vědách. *Soudní inženýrství* . [online]. [2006] [cit. 2016-02-22]. Dostupné z: *http://www.sinz.cz/archiv/docs/si-2005-01-3-23.pdf*

[2] zdroj: Digitální stopy v kriminalistice a forenzních vědách. *Soudní inženýrství* . [online]. [2006] [cit. 2016-02-22]. Dostupné z: *http://www.sinz.cz/archiv/docs/si-2005-01-3-23.pdf*

tedy o forenzní audity v civilní nebo komerční sféře, ale i o vyšetřování trestných činů a přestupků. Kvalita i formální zpracování musí odpovídat pravidlům přípustnosti u soudních orgánů. Proto hovoříme o tom, že kriminalistické stopy jsou podmnožinou stop forenzních.

Poslední skupinu tvoří jinak využitelné stopy. Sem se řadí zbylé stopy, které neodpovídají kritériím předešlých dvou skupin. Ve většině případů to bývají interní dokumenty vnitřní kontroly instituce. Tyto stopy, na rozdíl od předešlých dvou skupin, nemusí být akceptovatelné soudními orgány kvůli své kvalitě.

# 3. Zneužití digitální stopy

Hlavní nevýhodou dnešní "internetové" doby je sám internet nebo spíše nezodpovědný a lehkovážný pohyb lidí na něm a zanechávání spousty informací o sobě. Uživatelé internetu mnohdy ani dobře netuší jaké stopy po sobě zanechávají a jak s těmito informacemi může být dále proti nim naloženo. Problémem samotného internetu je i to, že se na něm téměř nic nedá dokonale schovat. Proto by uživatelé měli dbát na to, aby za sebou nechávali minimum těchto informací a stop.

Jedním z největších rizik hrozí uživatelům, kteří využívají nezabezpečené veřejné bezdrátové wifi sítě. Při těchto spojeních je pravděpodobnost toho, že naše komunikace budu odposlouchávána velmi vysoká a tím i získání vašeho hesla k různým sociálním sítím, heslo k vašemu internetovému bankovnictví či emailové schránce a k dalším různým účtům.

Takto získané nebo spíše ukradené informace se dají zneužít různými způsoby. Mezi ty hlavní způsoby zneužití patří krádež identity a sledování návyků uživatele. Obě tyto zneužití se týkají jak aktivní tak i pasivní stopy.

## 1. Behaviorální marketing

Zanechané digitální stopy nemusí být vždy zneužity způsobem, který by nám uškodil. Příkladem tohoto dobře myšleného využití informací o nás, které jsme za sebou zanechali na internetu, může být takzvaný behaviorální marketing.

O čem vlastně tento behaviorální marketing je? Je to marketing, který o nás sbírá informace, aby nám mohl nabídnout cílenou reklamu.

Jde především o dva hlavní toky, ze kterých jsou data sbírána. Tím prvním jsou klíčová slova, která zadáváme do vyhledávačů a pomocí jichž vyhledáme webové stránky. A

tím druhým způsobem je analýza našeho putování na daných webových stránkách. Tím je myšleno, kolik času trávíme na dané stránce a odkud jsme na tuto stránku přišli a kam z ní odešli.

Takto získaná data a informace o nás se následně analyzují a je z nich sestaven profil, který vypovídá o tom, které stánky navštěvujeme, jaká je tématika těchto stránek, co nejčastěji vyhledáváme za zboží, jaké jsou naše koníčky, jak se chováme na stránkách a mnoho dalších informací. Tyto profily jsou ukládány anonymně, bez vašeho jména či příjmení, jde jen pouze o vaše chování na dané stránce a o to co jste vyhledávali. Následně nám je tedy nabízený produkt, o který, vzhledem k našemu profilu, bychom mohli mít zájem. Pro firmy a různé e-shopy je to mnohem efektivnější a méně nákladný způsob reklamy než takzvané reklamy "naslepo", které stojí více a mají menší efektivnost. Reklamou "naslepo" jsou myšleny reklamy, které jsou pevně dané a nemění se v ohledu profilu uživatele.

Většina behaviorálních reklam je dělána tak, že zadavatel platí pouze za takzvané "prokliky". Proklik je cílený a vědomí přechod na stránku, jenž nám byla nabízena reklamou. Nejde tedy o náhodná či nevědomá navštívení stránky. V tomto je hlavní síla a výhoda behaviorální reklamy. Obvykle se tedy platí částka za určitý počet prokliků.

## 2. Sledování uživatelů

Největší ohrožení soukromí uživatele hrozí v případě, že je o něm nashromážděno velké množství dat. V profilech na různých stránkách jsou většinou ukládány obecné věci o vás, jako je například pohlaví, odhadovaný věk, vaše zájmy, ale i geografická lokace místa odkud jste se připojil. Některé firmy, které prodávají tyto informace, je dále rozšiřují i o své odhady. Jsou to informace o výši vašeho platu, o vlastnictví nemovitostí atd. Čím více informací je o vás známo, tím je menší i množina lidí, kteří vyhovují těmto kritériím. Tím se zvedá i pravděpodobnost, že se najde přímo ten daný uživatel, o kterém byla ty data sesbírána.

Julie Angwin v roce 2010 vypracovala pro americký Wall Street Journal detailní studii[3], jenž monitorovala počet a původ sledovacích zařízení. Do této studie bylo zahrnuto 50 nejvíce navštěvovaných webových stránek ve Spojených státech amerických. Mezi těmito stránkami byly stránky Facebooku, Microsoftu, Wikipedie a dalších. Můžeme tedy říct, že daná studie má i význam pro naší zemi. Z této studie vyplývá, že průměrně na každém webu

[3] zdroj: The Web's New Gold Mine: Your Secrets. The Wall Street Journal. [online]. 30.7.2010 [cit. 2015-12-13]. Dostupné z: *http://www.wsj.com/articles/SB10001424052748703940904575395073512989404*

je 64 monitorovacích zařízení, která o nás sbírají informace. To při pozorování 50 stránek dělá 3180 zařízení. Pouhou necelou jednu třetinu, či-li 956 zařízení, patřilo přímo webovým stránkám, které je používali pro statistické analýzy. Zbylých 2 224 zařízení, či-li více jak dvě třetiny, patřili takzvaným třetím stranám. Třetími stranami jsou myšleny firmy, které sbírají informace a dále je prodávají. Bylo zjištěno, že těch 2 224 zařízení, patří 131 různým firmám. Nejlépe z této studie vyšel web volně uživatelsky tvořené encyklopedie Wikipedia, na kterém nebyla zjištěna žádná monitorovací zařízení. Naopak na posledním padesátém místě se umístil web Dictionary.com, na kterém bylo zjištěno 234 sledovacích zařízení, z nichž pouhých 11 bylo přímo webu. Zbylých 223 patřilo třetím stranám, které shromažďovali informace.

Mezi nejpoužívanější nástroje, pomocí nichž se snaží firmy získávat informace, jsou soubory cookies a pixelový tag, známý také jako internetový tag.

## 3. Krádež identity

S krádeží identity úzce souvisí s osobními údaji. Ty jsou definovány pomocí zákona č. 101/2000 Sb., o ochraně osobních údajů. Krátká definice z tohoto zákona, která patří pod §4 a), zní: *„jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu“*. (Zákon č. 101/2000 Sb., o ochraně osobních údajů (účinné znění), 2000) [4]Z této definice vyplývá, že se tedy nejedná pouze o odcizení těch základních informací jako je jméno, příjmení, bydliště, rodné číslo atd., ale i informací, které pomocí jichž lze určit přímo či nepřímo identitu.

Krádež identity není pouze odcizení osobních údajů, ale také i jejich shromažďování či jakékoliv využívání k vydávání se za někoho jiného. V České republice se krádež identity považuje za dvoustupňový trestný čin.

Prvním stupněm je tzv. identity theft. V tomto kroku se pachatel pokouší odcizit osobní informace. Rozlišujeme tři druhy, jak se snaží pachatel odcizit data. Prvním způsobem je neoprávněné zkopírování dat nebo-li tzn. skimming. Druhým trikem je lstivé vylákání osobních údajů též známé jako phishing. Tento trik je praktikován převážně falešnými emaily či webovými stránkami, které od lidí žádají některé z osobních údajů. Posledním způsobem je hacking, to se dá do českého jazyka přeložit jako neoprávněné vniknutí do cizího počítače.

[4] zdroj: Zákon č. 101/2000 Sb., o ochraně osobních údajů (účinné znění). *Úřad pro ochranu osobních údajů.* [online]. 4.4.2000 [cit. 2015-12-15]. Dostupné z: https://www.uoou.cz/files/101_cz.pdf

Druhým stupněm je následné využití těchto odcizených informací. Tento stupeň se označuje jako identity fraud. Ukradená data se dají využít mnoha způsoby, záleží kolik a jakých dat pachatel má. Například může jít o vytvoření falešného profilu na některé ze sociálních sítí. Takto vytvoření profil může zničit reputaci dané osoby. Hlavním důvodem k odcizení identity je vlastní obohacení. Odcizení peněz přímo z bankovního účtu, či vypůjčení si peněz od banky a nebo prodaní identity některé ze třetích stran.

### 4. Využit v personalistice

Tento bod má své klady i zápory. Zaleží to na spoustě faktorů zejména na tom, co za sebou zanecháváme na sociálních sítích. Profil, který máme na Facebooku, Twitteru, Instagramu, Googlu+ či LinkedIn, mnohdy o nás vypovídá více než vůbec tušíme a chceme. Pro personální oddělení firem je to jen další zdroj informací, které o nás lehce získají. Většina z nich, přesněji 9 z 10 personalistů, spoléhá na Linkedln, zhruba 30 procent i na Facebook. Sociální sítě nabízejí možnost oslovit zajímavé kandidáty, ale také často fungují jako síto, kterým uchazeč neprojde z důvodu obsahu na jeho sociálních sítí. Podle průzkumu [5] personální agentury Grafton Recruitment je třetina uchazečů odmítnuta, z důvodu nevhodného obsahu na profilu na sociální síti. Tohoto průzkumu se zúčastnilo 2010 kandidátů. Pozitivní vliv to může mít ve chvíli, kdy sdílíme práci, která se nám povedla a následně se stane "propagačním materiálem" díky ‚kterému nás může personalista oslovit nebo ukázat naší práci někomu dalšímu. Také se dá o nás zjistit spoustu osobních věcí například jaké činnosti preferujeme při volnočasových aktivitách, k jakým skupinám se hlásíme, co posloucháme za hudbu, z čehož se dá předpovídat část naší osobnosti a chování, co nemusí být vždy podle očekávání personalistů. Mezi další zápory můžou patřit akce, kterých jsme se zúčastnili, fotky na kterých nevypadáme dostatečně reprezentativně, ve chvíli kdy firma vyžaduje reprezentativní chování i mimo pracovní dobu.

## 4. Nebezpečí v podobě útoků

Další hroznou, která uživateli hrozí díky zanechání digitální stopy, jsou útoky na uživatelům počítač. Pokud útočník zachytí IP adresu zanechanou po uživatelově připojení do

[5] zdroj: Chraňte si své soukromí na sítích, personalisté vás vidí. *Česká televize.* [online]. 26.9.2014 [cit. 2016-02-12]. Dostupné z: *http://www.ceskatelevize.cz/ct24/ekonomika/1016148-chrante-si-sve-soukromi-na-sitich-personaliste-vas-vidi*

sítě hrozí dosti velké nebezpečí. "*Na internetu ale existují (a v praxi se používají) jednoduché programy, které procházejí zvolený prostor IP adres a "zkusmo" útočí jednoduchými útoky na počítače, které jsou zrovna v daném prostoru připojeny, tedy odpovídají například na ping.*" (Doseděl, 2004, str. 101) Tyto útoky si rozdělíme do dvou skupin. První skupina je označována jako aktivní zasahování do komunikace. Sem řadíme různé modifikace a odposlechy přenášených dat. Druhou skupinu jsou útoky na dostupnost služeb. Zde nás bude zajímat přetížení systému pomocí útoků Dos a dDos.

## 1. Modifikace a odposlechy dat

Při těchto útocích jde útočníkovi o narušení probíhající komunikace. Lze tyto útoky rozdělit do tří skupin, vzhledem k cíli, který chce útočník dosáhnout.

První skupinou zahrnuje změnu dat ve prospěch útočníka. Při těchto útocích jde tedy o pozměnění zasílaných dat. Útočník tedy může odposlechnout a následně modifikovat například číslo bankovního, na který jsou dané peníze odesílány nebo sumu, která je odesílána. Uživatel má samozřejmě možnost se proti tomuto typu modifikací bránit. Příkladem takové ochrany může být digitální podpis či technologie kontrolního součtu, která odhalí manipulaci s odeslanými daty. Pro zvýšení ochrany je ještě vhodné, aby odesílané kontrolní součty byly zašifrovány.

Druhá skupina se týká změny identity ve prospěch útočníka. Při těchto útocích nejde o změnu v datech, ale o samotné přivlastnění si něčí identity. Hovoříme zde tedy o krádeži identity. Obranou proti těmto druhům útoku je důsledná autentizace uživatelů a používání příslušných protokolů, které tento útok odrazí.

Poslední skupina se týká ničení přenášených dat. Tyto útoky jsou hlavně vedeny na dostupnost služeb. U bezdrátových sítí útok probíhá pomocí silného zdroje signálu, který vysílá na přenosových pásmech dané sítě. Tím znemožní veškerou komunikaci směrem ze sítě i do ní. Obrana proti těmto útokům je velmi složitá a téměř nemožná.

## 2. DoS a dDoS

DoS a dDoS jsou příkladem útoků na dostupnost služeb. DoS je anglická zkratka Denial of Service, do češtiny přeloženo jako odmítnutí služby. V dnešní době jsou DoS útoky velmi neefektivní, důvodem je jednoduchá obrana proti nim. Při útocích na IP adresu serveru

si servery danou zátěž, v podobě neustálých dotazů, rozdělí. Tím pádem jeden útočníkům počítač nedokáže tyto servery ochromit a přehltit dotazy. Dalším obranou je zablokování jedné konkrétní útočníkovi IP adresy a tím i zablokování dotazy z této IP adresy.

Proto se dnes používá dDoS. Název je zkratkou Destributed DoS. První fází těchto útoků je získání kontroly nad velkým množstvím počítačů. Toto převzetí může proběhnout pomocí různých virů či červů. A dále následuje klasický DoS útok. Všechny tyto kontrolované počítače ve stejné čase začnou posílat hromadu dotazů na danou IP adresu. Dnešní servery i běžné počítače se s útoky od jednoho počítače vypořádají bez problémů, ale když tyto nepřetržité dotazy proudí od tisíce počítačů, tak to již znamená problém.

# 4. Vlastní práce, testované nástroje

## 1. Anonymita v prostředí internetu

Jak lze tedy chránit vaše soukromí a minimalizovat zanechanou digitální stopu? Důležitá je prevence a tedy předejít tomu, aby vás někdo sledoval a i kdyby sledoval, tak aby to měl těžší. K tomu použijeme dva anonymní prohlížeče a těmi jsou Tor Browser Bundle a JonDoFox, které následně porovnáme. Nejprve je ale potřeba si ukázat, co o vás prozradí běžně používané webové prohlížeče.

### 1. Běžné internetové prohlížeče

Mezi běžně používané prohlížeče patří Google Chrome, Mozilla Firefox, Internet Explorer a Opera. Všechny tyto prohlížeče o vás prozradí mnoho informací. I při správném nastavení a vysokém zabezpečení o vás vždy prozradí vaší IP adresu, poskytovatele i přibližnou adresu, kde se nacházíte. Anonymní režimy těchto prohlížečů nejsou ve své podstatě anonymní, jen pouze neukládají historii webů, které jste procházeli. Nezabraňují tedy cookies třetích stran a ani pixelovým tagům, či-li o vás jsou stále shromažďovány informace.

Testování probíhalo pomocí webových stránek http://ip-check.info/?lang=en. Jsou to oficiální stránky webového anonymizéru JonDon. Tyty webové stránky umožňují otestování jakéhokoliv webového prohlížeče a ukázání jeho nedostatků v bezpečnosti nebo spíše poukázání na to, která data jsou možná zjistit z daného prohlížeče. Testovány byly prohlížeče Mozilla Firefox verze 44.0, Internet Explorer v. 11.0, Google Chrome v. 48.0 a Opera verze 35.0.

| | | |
|---|---|---|
| Your IP | 213.180.38.186 | Traceroute |
| Your location | Stredocesky kraj, Neratovice | Show on map |
| Your net provider | RIO Media a.s. | Whois IP |
| Reverse DNS | skysoftneratovice.rionet.cz | Whois Domain |

| Attribute | Value | Rating |
|---|---|---|
| Cookies | Third party sites get your cookies and may track you. | bad |
| Authentication | Your unique ID: 764746250 | bad |
| Cache (E-Tags) | Your unique ID: 804343997 | bad |
| HTTP session | unlimited | bad |
| Referer | Original: Websites may see from which other website you come from! | medium |
| Signature | 8ab3a24c55ad99f4e3a6e5c03cad9446 (Firefox) | medium |
| User-Agent | Mozilla/5.0 (Windows NT 6.1; WOW64; rv:29.0) Gecko/20100101 Firefox/29.0 | bad |
| SSL_session_id | | neutral |
| Language | cs,en-us;q=0.7,en;q=0.3 | medium |
| Content types | text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 | good |
| Encoding | gzip, deflate | good |
| Do-Not-Track | | medium |

| Attribute | Value | Rating |
|---|---|---|
| JavaScript | JavaScript is activated! (Version: 1.5) | medium |
| Plugins | Found 10 plugins. Flash is active! | bad |
| Mime types | Found 102 mime types that your browser supports. | bad |
| Tab name | "window.name" is traceable. Your unique ID: 1723204 | bad |
| Tab history | There are 10 pages in your tab history. | medium |
| Local storage | Local storage is enabled. Your unique ID: 11723204 | medium |
| Screen | 1920 x 1080 pixels 24 bit color depth | good |
| Screen (usable) | 1920 x 1040 pixels (does not match screen) | medium |
| Browser window | 1920 x 910 pixels (inner size) | medium |
| Browser bars | MenuBar PersonalBar StatusBar ToolBar ScrollBars LocationBar | good |
| WebGL | WebGL is activated, WebGL 1.0, Mozilla | medium |
| Browser type | Mozilla/5.0 (Windows) 20100101/20140506152807 Netscape (cs) | medium |
| System | Windows NT 6.1; WOW64 Win32 (Sat Feb 27 2016 16:42:46 GMT+0100) | medium |
| Fonts | 211 installed fonts have been found on your computer. | bad |

**Obrázek 1 - Informace z Mozilla Firefox**[6]

[6] zdroj: Vlastní zpracování

| | | |
|---|---|---|
| Your IP | 213.180.38.186 | Traceroute |
| Your location | Stredocesky kraj, Neratovice | Show on map |
| Your net provider | RIO Media a.s. | Whois IP |
| Reverse DNS | skysoftneratovice.rionet.cz | Whois Domain |

| Attribute | Value | Rating |
|---|---|---|
| Cookies | Third party sites get your cookies and may track you. | bad |
| Authentication | Your unique ID: 960758720 | bad |
| Cache (E-Tags) | Your unique ID: 462557780 | bad |
| HTTP session | unlimited | bad |
| Referer | Original: Websites may see from which other website you come from! | medium |
| Signature | 84f83c14f83b5f89c8c963672fe84057 (Internet Explorer) | medium |
| User-Agent | Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko | bad |
| SSL_session_id | DE4C49AE776799A84509CCD08FBFCFF4505DCE6DC5828B0443598FC2B7190F18 | neutral |
| Language | cs-CZ | medium |
| Content types | text/html, application/xhtml+xml, */* | medium |
| Encoding | gzip, deflate | good |
| Do-Not-Track | protected | good |

| Attribute | Value | Rating |
|---|---|---|
| JavaScript | JavaScript is activated! (Version: 1.3) | medium |
| Plugins | Found 2 plugins. Flash is active! | bad |
| Mime types | Found 3 mime types that your browser supports. | medium |
| Tab name | "window.name" has been anonymized. | good |
| Tab history | There are 12 pages in your tab history. | medium |
| Local storage | Local storage is enabled. Your unique ID: 11701231 | medium |
| Screen | 2133 x 1200 pixels 24 bit color depth | medium |
| Screen (usable) | 2133 x 1156 pixels (does not match screen) | medium |
| Browser window | 2133 x 1094 pixels (inner size) | medium |
| WebGL | WebGL is activated, WebGL 0.94, Internet Explorer | medium |
| Browser type | Netscape (cs-CZ) (cs-CZ) | medium |
| System | Win32 x86 (cs-CZ, windows-1250, Sat Feb 27 2016 16:41:52 GMT+0100 (Střední Evropa (běžný čas))) | medium |
| Fonts | 247 installed fonts have been found on your computer. | bad |

**Obrázek 2 - Informace z Internet Explorer**[7]

[7] zdroj: Vlastní zpracování

| | | |
|---|---|---|
| Your IP | 213.180.39.186 | Traceroute |
| Your location | Stredocesky kraj, Neratovice | Show on map |
| Your net provider | RIO Media a.s. | Whois IP |
| Reverse DNS | skysoftneratovice.rionet.cz | Whois Domain |

| Attribute | Value | Rating |
|---|---|---|
| Cookies | Third party sites get your cookies and may track you. | bad |
| Authentication | Your unique ID: 254215651 | bad |
| Cache (E-Tags) | Your unique ID: 490873865 | bad |
| HTTP session | unlimited | bad |
| Referer | Original: Websites may see from which other website you come from! | medium |
| Signature | 5f830e59fd1d47bca8821acd1910f186 | medium |
| User-Agent | Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/48.0.2564.116 Safari/537.36 | bad |
| SSL_session_id | | neutral |
| Language | cs-CZ,cs;q=0.8,en;q=0.6,sk;q=0.4 | medium |
| Content types | text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 | medium |
| Encoding | gzip, deflate, sdch | medium |
| Do-Not-Track | | medium |
| Upgrade-Insecure-Requests | 1 | medium |

| Attribute | Value | Rating |
|---|---|---|
| JavaScript | JavaScript is activated! (Version: 1.7) | medium |
| Plugins | Found 4 plugins. Flash is active! | bad |
| Mime types | Found 7 mime types that your browser supports. | medium |
| Tab name | "window.name" is traceable. Your unique ID: 2693759 | bad |
| Tab history | There are 3 pages in your tab history. | medium |
| Local storage | Local storage is enabled. Your unique ID: 12693759 | medium |
| Screen | 1920 x 1080 pixels 24 bit color depth | good |
| Screen (usable) | 1920 x 1040 pixels (does not match screen) | medium |
| Browser window | 1920 x 955 pixels (inner size) | medium |
| Browser bars | MenuBar PersonalBar StatusBar ToolBar ScrollBars LocationBar | good |
| WebGL | WebGL is activated. WebGL 1.0 (OpenGL ES 2.0 Chromium). WebKit WebGL | medium |
| Browser type | 20030107 Netscape (cs) | medium |
| System | Win32 (windows-1250, Sat Feb 27 2016 16:43:53 GMT+0100 (Střední Evropa (běžný čas))) | medium |
| Fonts | 212 installed fonts have been found on your computer. | bad |

**Obrázek 3 - Informace z Google Chrome**[8]

[8] zdroj: Vlastní zpracování

| | | |
|---|---|---|
| Your IP | 213.180.39.186 | Traceroute |
| Your location | Stredocesky kraj, Neratovice | Show on map |
| Your net provider | RIO Media a.s. | Whois IP |
| Reverse DNS | skysoftneratovice.rionet.cz | Whois Domain |

| Attribute | Value | Rating |
|---|---|---|
| Cookies | Third party sites get your cookies and may track you. | bad |
| Authentication | Your unique ID: 945325757 | bad |
| Cache (E-Tags) | Your unique ID: 1325369788 | bad |
| HTTP session | unlimited | bad |
| Referer | Original: Websites may see from which other website you come from! | medium |
| Signature | 5f830e59fd1d47bca8821acd1910f186 | medium |
| User-Agent | Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/48.0.2564.82 Safari/537.36 OPR/35.0.2066.37 | bad |
| SSL_session_id | 863314E4ED6F4C9DC88369F0956A6945ADFAC2B0C7B3B52888B2B818FC156772 | neutral |
| Language | cs-CZ,cs;q=0.8 | medium |
| Content types | text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 | medium |
| Encoding | gzip, deflate, lzma, sdch | medium |
| Do-Not-Track | | medium |
| Upgrade-Insecure-Requests | 1 | medium |

Obrázek 4 - Informace z prohlížeče Opera[9]

## 2. Tor, Tor Browser Bundle

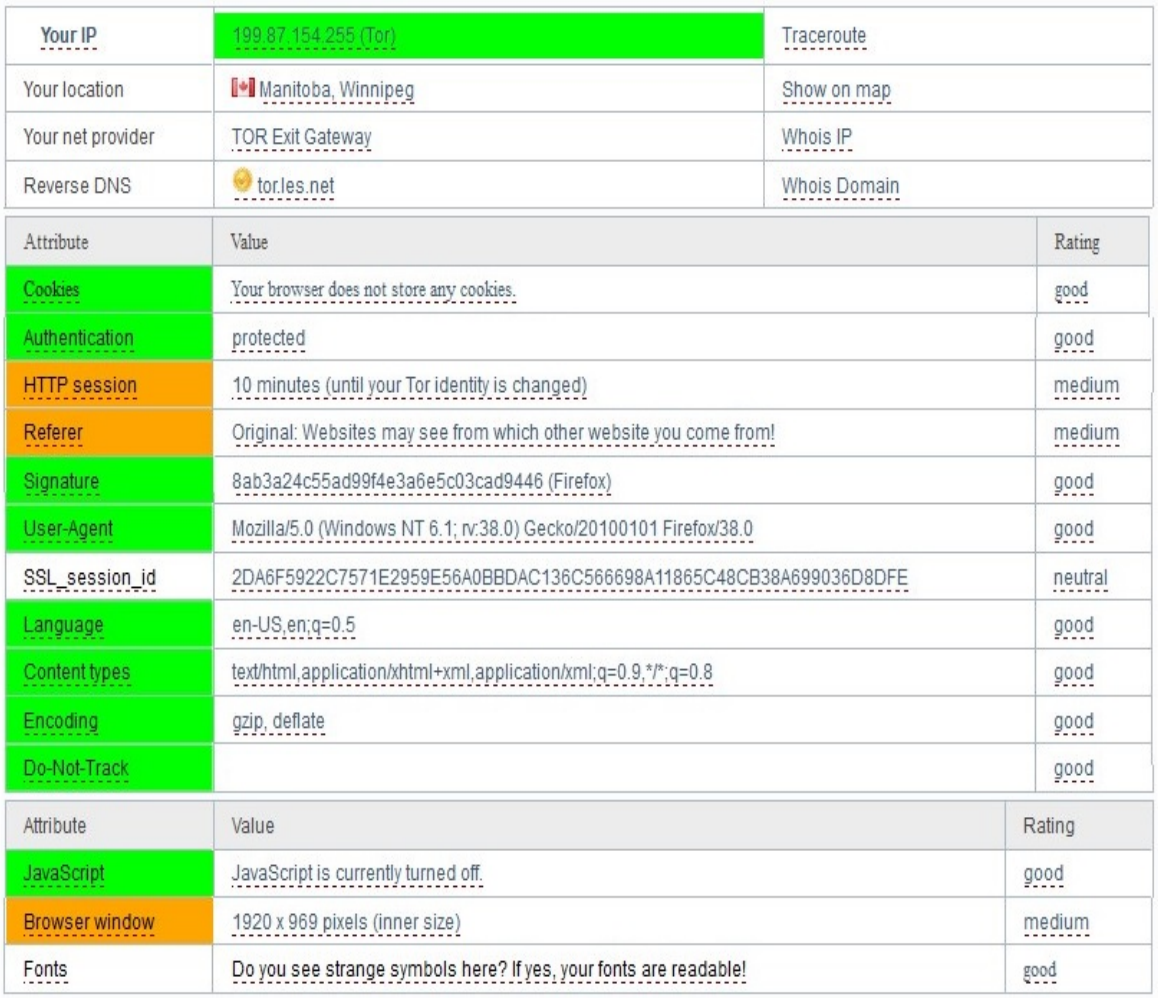
Tor Brower Bundle je webový prohlížeč od vývojářů Core Tor People. Alfa verze softwaru byla uvedena 20. září 2002. První prezentace sítě Tor proběhla 13. prosince 2004 na USENIX sympóziu věnovanému bezpečnosti na internetu. Od prosince 2006 je projekt Tor uváděn jako výzkumně-vzdělávací neziskovou organizací v USA. Nejnovější Tor verze 5.5.2, vyšla 12. února roku 2016. Název Tor vznikl z anglických slov The Onion Routing, přeloženo do češtiny jako "cibulové směrování" a tak i Tor funguje. K anonymizaci používá model klient-server. Tento model funguje následovně. Uživatel zadá požadavek, který je nejprve zaslán do sítě Tor a z ní je následně odeslán k cílovému uzlu. V síti Tor si tento požadavek mezi sebou vymění několik serverů, vše probíhá šifrovaně. Takže uživatel je přikryt vrstvou, kterou je síť Tor, stejně jako jsou vrstvy u cibule, proto ten název. Tím, že je uživatelova síť skryta pod sítí Tor, je IP adresa uživatele schována a na venek se tváří jako IP

[9] zdroj: Vlastní zpracování

adresa výstupního serveru ze sítě Tor. Tor v roce 2014 byl tvořen tisícem exit relay (výstupní brány sítě Tor) a dalšími zhruba pěti tisíci mezičlánků. V projektu jsou zapojeni i dobrovolníci a to je největší nebezpečí Toru. Mezi lety 2011 až 2013 bylo z exit relay odebráno okolo 40 počítačů, u kterých bylo zjištěno pomocí testovacího programu SoaT (Snakes on a Tor), že se snaží zachytávat či modifikovat data. SoaT je testovací program na odchytávání či modifikování dat od vývojářů Toru. V roce 2013 probíhala na švédské univerzitě v Karlstadu studie Toru, kterou vedli Philipp Winter a Stefan Lindskog. Tato studie odhalila desítky záškodníků z řad těch, kteří se starají o exit relay. Testování probíhalo pomocí softwaru Exitmap, který byl sepsán přímo na univerzitě. Nyní je tento software volně ke stažení. Záškodníci používali různé formy útoků. Příkladem je pokus o prolomení protokolů HTTPS, SSH spojení, odesílání nepravých certifikátů, vyměňování textových řetězců "https://" za "http://" nebo takzvané HTML injection. HTML injection je útok, při kterém útočník vkládá do webové stránky svůj vlastní kód ve formě javascriptu, pomocí kterého například shromažďuje informace.

Nevýhodou Toru je, že rychlost internetu záleže na rychlosti nejpomalejšího uzlu po trase, takže je určený spíše jen pro procházení webových stránek. Největším problémem mohou být záškodníci z řad dobrovolníků.

Demonstrací funkčnosti Toru je následující výsledek z testu bezpečnosti, které byly provedeny i u běžných prohlížečů. Testován byl Tor verze 5.5.2, která vyšla 12. února roku 2016.



| Your IP | 199.87.154.255 (Tor) | Traceroute |
|---|---|---|
| Your location | Manitoba, Winnipeg | Show on map |
| Your net provider | TOR Exit Gateway | Whois IP |
| Reverse DNS | tor.les.net | Whois Domain |

| Attribute | Value | Rating |
|---|---|---|
| Cookies | Your browser does not store any cookies. | good |
| Authentication | protected | good |
| HTTP session | 10 minutes (until your Tor identity is changed) | medium |
| Referer | Original: Websites may see from which other website you come from! | medium |
| Signature | 8ab3a24c55ad99f4e3a6e5c03cad9446 (Firefox) | good |
| User-Agent | Mozilla/5.0 (Windows NT 6.1; rv:38.0) Gecko/20100101 Firefox/38.0 | good |
| SSL_session_id | 2DA6F5922C7571E2959E56A0BBDAC136C566698A11865C48CB38A699036D8DFE | neutral |
| Language | en-US,en;q=0.5 | good |
| Content types | text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 | good |
| Encoding | gzip, deflate | good |
| Do-Not-Track | | good |

| Attribute | Value | Rating |
|---|---|---|
| JavaScript | JavaScript is currently turned off. | good |
| Browser window | 1920 x 969 pixels (inner size) | medium |
| Fonts | Do you see strange symbols here? If yes, your fonts are readable! | good |

**Obrázek 5 - Informace z Tor Browser Bundle**[10]

Tyto výsledky jsou mnohem lepší než u běžných prohlížečů. IP adresa uživatele je změněna, tím se i zmenšila šance a její odhalení. Provider se změnil na "výstupní bránu Toru" a geologická lokace již také nesedí. Tor zabránil i ukládání a odesílání cookies a zvýšil bezpečnost při ověřování (přihlašování).

## 3. JonDo, JonDoFox

Druhým testovaným anonymním webovým prohlížečem je JonDoFox. Tento produkt je taktéž freeware. JonDoFox spadá pod webový anonymizér JonDo, který je vyvíjen společností JonDos GmbH. JonDo funguje na bázi tzv. mixů. Mix je dvojice či trojice serverů v různých zemích. V freeware verzi může uživatel použít pouze jeden mix složený ze dvou serverů. Veškerá komunikaci mezi uživatelem a serverovými mixy je šifrována, i komunikace

[10] zdroj: Vlastní zpracování

mezi dvěma mixy. JonDoFox je tedy webovým prohlížečem, který používá jádro z Mozilly Firefox, ale ke svému správnému fungování potřebuje anonymizér JonDo. V tomto anonymizéru si zvolíte mix, přes který chcete být připojeni a ukryti. Testována byla verze JonDo 0.19 ze srpna roku 2013 a JonDoFox verze 2.14.0 z prosince roku 2015.

| | | |
|---|---|---|
| Your IP | 178.33.255.188 (JonDonym) | Traceroute |
| Your location | France | Show on map |
| Your net provider | OVH SAS | Whois IP |
| Reverse DNS | cyrax.jd.gurutek.biz | Whois Domain |

| Attribute | Value | Rating |
|---|---|---|
| Cookies | Your browser does not store any cookies. | good |
| Authentication | protected | good |
| Cache (E-Tags) | protected | good |
| HTTP session | stateless | good |
| Referer | Original: Websites may see from which other website you come from! | medium |
| Signature | 8ab3a24c55ad99f4e3a6e5c03cad9446 (Firefox) | good |
| User-Agent | Mozilla/5.0 (X11; Linux i686; rv:38.0) Gecko/20100101 Firefox/38.0 | good |
| SSL_session_id | B6DE73CD065D7B00573A8FC4D9B02904C9FF15CEE93FA104D4E41AA01D9F7AFD | neutral |
| Language | en-US,en;q=0.5 | good |
| Content types | text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 | good |
| Encoding | gzip, deflate | good |
| Do-Not-Track | protected | good |

| Attribute | Value | Rating |
|---|---|---|
| JavaScript | JavaScript is currently turned off. | good |
| Browser window | 1920 x 938 pixels (inner size) | medium |
| Fonts | Do you see strange symbols here? If yes, your fonts are readable! | good |

**Obrázek 6 - Informace z JonDoFox**[11]

Výsledky testů pro JonDoFox vyšly lépe než u běžných prohlížečů. Stejně jako u Tor, není ihned vidět reálná IP adresa uživate, poskytovatel či lokace. Test pro JonDoFox vyšel dokonce i lépe než pro Tor.

## 2. Nástroje k zabránění sledování

Dalšími preventivními nástroji k ochraně vašeho soukromí na internetu jsou rozšíření v rámci vašeho webového prohlížeče. Pro testování jsem si vybral Ghostery a TrackMeNot.

[11] zdroj: Vlastní zpracování

### 1. Ghostery

Ghostery je freeware rozšíření do vašeho webového prohlížeče. Ghostery je cross-platform nástroj, takže lze ho nainstalovat do kteréhokoliv webového prohlížeče. Ghostery Inc. je vlastníkem a vývojářem tohoto nástroje. Ghostery je již rozšířený i do mobilní sféry. Zde není veden jako doplněk pro webový prohlížeč, ale jako webový prohlížeč sám. Je dostupný jak na telefony s operačním systém Android tak i na telefony s iOS. V poslední verzi 5.4.11 pro Google Chrome, která vyšla 20. února 2016, je v databázi zaznamenáno 2080 známých trackerů, které lze blokovat. Nalezneme zde například Google Analytics, Facebook Social Plugins atd. Ghostery funguje následovně. Pokud je zakázán některý ze známých trackerů, tak se Ghostery postará o to, aby se daný skript nespustil a nebyly odeslána požadovaná data. Ghostery samozřejmě detekuje i trackery, které nejsou v seznamu zakázaných a snaží se i nové potencionální hrozby nacházet.

### 2. TrackMeNot

TrackMeNot vytrořili Daniel C. Howe a Helen Nissenbaum. Tento nástroj je použitelný pouze pro webové prohlížeče Mozilla Firefox a Google Chrome. TrackMeNot na rozdíl od Ghostery se nesnaží uživatele utajit nebo jeho komunikaci šifrovat, ale jeho cílem je posílat různé a časté dotazy do vyhledávačů jako jsou Yahoo!, Google či Bing. Těmito dotazy se zmenší pravděpodobnost, že profil, který je tvořen sbíráním dat, bude pravdivý. Tím pádem nebude tak lehké sestavit profil a sesbíraná data zneužít, protože budou smyšlená.

## 3. Nástroje k odstranění uložených sledovacích zařízení

Pokud prevence v podobě anonymního webového prohlížeče či nástroje pro zabránění sledování selže, je potřeba použít jiné nástroje, které vzniklé hrozby odstraní z vašeho počítače a sníží tím možné riziko. Mezi programy, které dokážou částečně či zcela vymazat uložené trackery ve vašem počítači, patří CCleaner, Temp File Cleaner a ATF-Cleaner.

### 1. CCleaner

CCleaner je freeware nástroj, který umožňuje odstranění sledovacích zařízení, které již jsou uloženy v paměti počítače. Tento nástroj je vyvíjen společností Piriform a původně se jmenoval Crap Cleaner a patří k jednomu z nejvíce oblíbených a stahovaných nástrojů v tomto směru. CCleaner má více využití, ať už vyhledávání a opravování chyb v registrech či odinstalování programů. Testována bude ale část, která se týká internetu a procházení na něm. Mezi tyto věci patří odstraňování cookies, historie prohlížeče či ukládání dat do cache paměti webového prohlížeče.

### 2. Temp File Cleaner

Temp File Cleaner je stejně jako CCleaner freeware nástroj. Vývojáři tohoto programu je společnost ADDPCS. Temp File Cleaner není tak multifunkční jako CCleaner, ale přesně splňuje většinu požadavků, které máme na program, jenž by se měl starat o mazání dočasných souborů, které vzniknout používáním webových prohlížečů jako jsou Google Chrome, Mozilla Firefox, Opera nebo Internet Explorer. Temp File Cleaner je kompatibilní pouze s operačním systémem Windows. Nejnovější stabilní verze je 4.4.0.

### 3. ATF-Cleaner

Posledním testovaným freeware nástrojem je ATF-Cleaner. Je to velmi malý program, jeho velikost činí 50kB. Ale i přesto je velmi efektivní. Poslední verze 3.0.0.2 vyšla v září roku 2008. Stejně jako předešlé nástroje, i ATF-Cleaner dokáže smazat historii, cookies a další záznamy. Jediná nevýhoda je, že nepodporuje, nebo spíše nedokáže smazat tato data z Google Chrome. Je to způsobeno tím, že první stabilní verze Google Chrome vyšla až měsíc po poslední verzi, tj, v říjnu 2008.

# 5. Výsledky testování

Pro to, abychom mohli zvolené nástroje testovat, je potřeba si je rozdělit do tří skupin. Všechny skupiny budou mít jako hlavní cíl chránit digitální stopu, ale každá skupina to bude dělat jinak. I podle toho, co očekáváme od dané skupiny, je nutné si stanovit rozlišná kritéria.

## 1. Anonymita v prostředí internetu

Pro testování anonymity v prostředí internetu byly použity softwary Tor a JonDo. Oba tyto freeware softwary prokázaly, že jejich používání je mnohem bezpečnější než používání běžných webových prohlížečů.[12] Pomocí více kriteriální analýzy bylo zjištěno, že o trochu lepším nástrojem pro anonymitu na internetu je JonDoFox, viz. tabulka níže.

| Kritéria | **Tor** | **JonDoFox** |
|---|---|---|
| IP adresa | Ano | Ano |
| Provider (poskytovatel) | Ano | Ano |
| Zeměpisná lokace | Ano | Ano |
| Cookies | Ano | Ano |
| E-Tag | Ne | Ano |
| Do Not Track | Ano | Ano |
| Historie prohlížeče | Ano | Ano |
| Java | Ano | Ano |
| Flash | Ano | Ano |
| Hodnocení | 88,8% | 100% |

**Tabulka 1 - Porovnání Tor a JonDoFox**[13]

Jediný rozdíl podle zvolených kritérií je v ochraně proti e-tagům. JonDoFox dokáže uživatele v tomto případě ochránit, na rozdíl od Toru. Oba prohlížeče dokážou uživatele preventivně ochránit a snížit riziko sběru informací velmi dobře. Podle stránek www.cnews.cz[14] v porovnání těchto dvou nástrojů v poměru ceny a výkonu vyhrál těsně Tor.

[12] Informace z běžných webových prohlížečů, kapitola 4.1.1.
[13] zdroj: Vlastní zpracování
[14] zdroj: Anonymně na internet: Tor a ti druzí. *Cnews*. [online]. 22.3.2011 [cit. 2016-02-20]. Dostupné z: *http://www.cnews.cz/anonymne-na-internet-tor-ti-druzi*

Řekl bych, že je to jen důkaz toho, že oba prohlížeče jsou velmi vyrovnané a nabízí téměř totéž a záleží na tom, co přesně uživatel požaduje.

## 2. Zabránění sledování

V této skupině byly testovány nástroje Ghostery a TrackMeNot, které měli za úkol zabránit sledování uživatele během jeho pobytu na internetu. Pro možnost porovnat oba nástroje bylo potřeba si zvolit kritéria, která nás budou zajímat. Následné testování vždy proběhlo na novém virtuálním otisku. Oba nástroje vždy byly nainstalovány do webového prohlížeče Google Chrome verze 48.0. Prvním nástrojem byl Ghostery verze 5.4.11 a druhým TrackMeNot verze 0.8.3. V obou případech byl scénář totožný, stejné webové stránky, stejné dotazy do vyhledávače. Výsledkem byla následující tabulka.

| Kritéria | **Ghostery** | **TrackMeNot** |
|---|---|---|
| Cookies | Ano | Ne |
| Pixelové tagy | Ano | Ne |
| Pluginy | Ano | Ne |
| Vyhledávání | Ne | Ano |
| Hodnocení | 75% | 25% |

**Tabulka 2 - Porovnání Ghostery a TrackMeNot**[15]

Z této tabulky lze vyvodit závěr, že Ghostery byl úspěšný při detekci a zabránění sběru dat ve 3 ze 4 případů. Naopak TrackMeNot byl úspěšný v jediným bodě, ve kterém Ghostery neuspěl. TrackMeNot dokázal svými častými a rozmanitými dotazy znehodnotit možný vznikající profil. Lze tedy usoudit, že k preventivní obraně proti sledování, by bylo vhodné využít kombinaci těchto dvou freeware doplňků webového prohlížeče Google Chrome.

## 3. Odstranění uložených sledovacích zařízení

V poslední testovací skupině, která byla zaměřena na odstranění uložených sledovacích zařízení, byly použity programy CCleaner, Temp File Cleaner a ATF-Cleaner. Aby bylo možné porovnat tyto tři freeware nástroje, bylo potřeba si stanovit kritéria, která

[15] zdroj: Vlastní zpracování

vyjádří požadované věci. U těchto programů je tedy důležité, aby uměly odstranit co nejvíce druhů uložených sledovacích zařízení a také, aby to uměly co nejlépe. Jak již bylo několikrát zmíněno, tak digitální stopu lze sestavit jak z historie prohlížení či za pomocí ukrytých sledovacích zařízení v cookies či v jiných dočasně uložených datech. Proto je potřeba tyto data zpětně odstranit a snížit tím i riziko. Všechny běžné prohlížeče již nabízejí možnost neukládat či mazat cookies po vypnutí daného webového prohlížeče. To se ale netýká cookies vytvořenými Flash či Silverlight, které jsou ukládány multimediálními objekty. Výsledky testů jsou znázorněny v následující tabulce.

| Kritéria | **CCleaner** | **Temp File Cleaner** | **ATF-Cleaner** |
|---|---|---|---|
| Cookies | Ano | Ano | Ano |
| Historie prohlížení | Ano | Ano | Ano |
| Cache | Ano | Ano | Ano |
| Java cache | Ano | Ano | Ano |
| Flash cookies | Ano | Ano | Ne |
| Silverlight cookies | Ano | Ne | Ne |
| Hodnocení | 100% | 83,3% | 66,6% |

**Tabulka 3 - Porovnání CCleaner, Temp File Cleaner a ATF-Cleaner**[16]

Ve všech zvolených kritériích jako jediný dokázal uspět CCleaner. Je nutno podotknout, že si špatně nevedl ani jeden ze zvolených freeware nástrojů. Dokonce ani ATF-Cleaner, jehož poslední verze vyšla v roce 2008. Je zde ale nutno podotknout, že tento program nepodporuje jeden z nejvíce používaných webových prohlížečů dnešní doby a to Google Chrome. Jediné s čím si Temp File Cleaner neporadil jsou Silverlight cookies.

[16] zdroj: Vlastní zpracování

# 6. Závěr

Hlavním cílem práce bylo zjisti, jak a do jaké míry se uživatel může chránit proti vzniku digitálních stop a případnému zneužití proti němu. Základní preventivní ochranou je správné nastavení firewallu, šifrování dat a používání zabezpečených protokolů jako HTTPS, pokud to jde. Zaměření této práce bylo na jiné nástroje, které se snaží ochránit uživatele.

Z testování lze usoudit, že v oblasti anonymity na internetu jsou dostupné dva freeware nástroje, které mají téměř totožné výsledky. Těmi nástroji jsou JonDo a Tor. Lépe v testu vyšel o kousek lépe JonDo.

U testů nástrojů, které zabraňují sledování uživatelů, je nejlepší možnosti obrany kombinace nástrojů Ghostery a TrackMeNot. Ghostery v testu neuspěl pouze v jediném kritériu, ve kterém naopak TrackMeNot ano.

V poslední testované oblasti, která se týkala dodatečného odstranění sledovacích zařízení přímo z počítače, nejlépe obstál CCleaner. Ten si dokázal poradit se všemi zvolenými kritérii. Zbylé dva nástoje, Temp File Cleaner a ATF-Clenaer, si také nevedly špatně, ale CCleaner zvládl vše.

Závěrečným doporučením tedy je, mít vhodně nastavený firewall, používat zabezpečený protokoly a šifrovat data. Pro zvýšení ochrany a zmenšení digitální stopy lze použít kombinaci vhodných nástrojů z každé testované oblasti.

# 7. Seznam použitých zdrojů


1. Česko patří do první třicítky zemí podle přístupu k internetu. Technet.cz. [online]. 23.9.2015 [cit. 2016-02-02]. Dostupné z: http://technet.idnes.cz/internet-ma-3-2-miliardy-lidi-df7-/sw_internet.aspx?c=A150922_140133_sw_internet_vse

2. Digitální stopa. Co je to. [online]. ©2010-2013 [cit. 2015-12-27]. Dostupné z: http://cojeto.superia.cz/ruzne/digitalni_stopa.php

3. Digitální stopy. E-Bezpečí. [online]. 19.9.2011 [cit. 2016-01-03]. Dostupné z: http://www.e-bezpeci.cz/index.php/temata/sociotechnika/312-digitalni-stopy

4. Lou Montulli. Lou Montulli. [online]. [2008] [cit. 2015-12-27]. Dostupné z: http://www.montulli.org/lou

5. Co potřebujete vědět o Cookies a Web Beacons. Monster. [online]. ©2015 [cit. 2015-12-27]. Dostupné z: http://rady-a-tipy.monster.cz/hledani-prace/jak-zacit-s-hledanim-prace/co-potrebujete-vedet-o-cokkies-web-beacons/article.aspx

6. Digitální stopy v kriminalistice a forenzních vědách. Soudní inženýrství . [online]. [2006] [cit. 2016-02-22]. Dostupné z: http://www.sinz.cz/archiv/docs/si-2005-01-3-23.pdf

7. The Web's New Gold Mine: Your Secrets. The Wall Street Journal. [online]. 30.7.2010 [cit. 2015-12-13]. Dostupné z: http://www.wsj.com/articles/SB10001424052748703940904575395073512989404

8. Behaviorální marketing. Media Guru. [online]. ©2016 [cit. 2016-01-02]. Dostupné z: http://www.mediaguru.cz/medialni-slovnik/behavioralni-marketing/

9. Krádež identity a jak se jí bránit. Bezpečný Internet. [online]. [] [cit. 2016-02-15]. Dostupné z: http://www.bezpecnyinternet.cz/pokrocily/ochrana-prav/kradez-identity.aspx

10.Zákon č. 101/2000 Sb., o ochraně osobních údajů (účinné znění). Úřad pro ochranu osobních údajů. [online]. 4.4.2000 [cit. 2015-12-15]. Dostupné z: https://www.uoou.cz/files/101_cz.pdf

11. Digitální stopa: Jak si nezavřít cestu k práci snů? Využívejte sociální sítě s rozumem, radí experti. Investiční web. [online]. 31.3.2015 [cit. 2016-02-10]. Dostupné z: http://www.investicniweb.cz/2015/3/31/digitalni-stopa-jak-si-nezavrit-cestu-k-praci-snu-vyuzivejte-socialni-site-s-rozumem-radi-experti/

12. Chraňte si své soukromí na sítích, personalisté vás vidí. Česká televize. [online]. 26.9.2014 [cit. 2016-02-12]. Dostupné z: http://www.ceskatelevize.cz/ct24/ekonomika/1016148-chrante-si-sve-soukromi-na-sitich-personaliste-vas-vidi

13. DOSEDĚL, T. Počítačová bezpečnost a ochrana dat. Brno: Computer Press. 2004. 190 str. ISBN 80-251-0106-1.

14. Proceedings of the 13th USENIX Security Symposium. Usenix. [online]. 9.8.2004 [cit. 2016-02-06]. Dostupné z: http://static.usenix.org/event/sec04/tech/full_papers/dingledine/dingledine.pdf

15. About Tor. Tor. [online]. [] [cit. 2016-02-06]. Dostupné z: https://www.torproject.org/about/overview.html.en

16. Anonymně na internet: Tor a ti druzí. Cnews. [online]. 22.3.2011 [cit. 2016-02-20]. Dostupné z: http://www.cnews.cz/anonymne-na-internet-tor-ti-druzi

17. Why using JonDonym. JonDonym. [online]. [] [cit. 2016-02-08]. Dostupné z: https://anonymous-proxy-servers.net/en/why.html

18. JonDonym: Die Tor-Alternative, Interview mit den Betreibern. Gulli. [online]. 26.11.2007 [cit. 2016-02-08]. Dostupné z: http://www.gulli.com/news/7229-jondonym-die-tor-alternative-interview-mit-den-betreibern-2007-11-26

19. About Ghostery. Ghostery. [online]. ©2016 [cit. 2016-02-15]. Dostupné z: https://www.ghostery.com/about-us/about-ghostery/

20. TrackMeNot. TrackMeNot. [online]. ©2003 [cit. 2016-02-28]. Dostupné z: https://cs.nyu.edu/trackmenot/

21. CCleaner. Piriform. [online]. ©2015-2016 [cit. 2016-02-14]. Dostupné z: https://www.piriform.com/ccleaner

22. Temp File Cleaner. ADDPCS. [online]. ©2014 [cit. 2016-02-20]. Dostupné z: https://addpcs.com/software/tfc/#/about

23. ATF-Cleaner 3.0.0.2. Slunečnice. [online]. ©1998-2016 [cit. 2016-02-01]. Dostupné z: http://www.slunecnice.cz/sw/atf-cleaner/

24. ATF-CLEANER.EXE. Atribune. [online]. 27.2.2008 [cit. 2016-02-01]. Dostupné z: http://www.atribune.org/index.php?option=com_content&task=view&id=25&Itemid=25