Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Naše Digitální stopa na počítači a na internetu

Tomáš Cizler

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Tomáš Cizler

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

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. 1ˆst 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

2017/18 LS – PEF

Vedoucí práce

Ing. Mgr. Vladimír Očenášek, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 31. 10. 2017

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 1. 11. 2017

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 09. 03. 2018

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Naše Digitální stopa na počítači a na internetu" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce 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 13.3.2018 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Mgr. Vladimíru Očenáškovi, Ph.D. a Ing. Čestmírovi Halbichovi, CSc. za vedení mé práce.

Naše Digitální stopa na počítači a na internetu

Abstrakt

Tato bakalářská práce je zaměřena na problematiku digitálních stop a jejich ochrany. Jejím cílem je představit významné druhy digitálních stop a doporučit vhodné řešení ochrany digitálních stop.

V teoretické části práce jsou představeny různé typy digitálních stop a možnosti jejich využití a zneužití. Mezi představenými způsoby využití digitální stopy jsou zahrnuty například personalistika a marketing. Dále jsou představeny způsoby sledování vlastních digitálních stop. Nakonec teoretická část obsahuje způsoby skrývaní a odstranění vlastní digitální stopy.

V praktické části je testována schopnost webových prohlížečů chránit soukromí uživatele. Jsou v ní testovány jak prohlížeče vhodnější pro běžné využití, tak prohlížeče s více specializovaným zaměřením. Dále je testovaný vliv VPN na schopnosti běžných prohlížečů zakrývat data o uživateli.

Klíčová slova: cookies, digitální stopa, hesla, ochrana dat, sledování, tor, VPN, webový prohlížeč

Digital footprint on own computer and the Internet

Abstract

This thesis is focused on the issue of digital footprints and the ways to protect them. The goal of the work is to characterize significant types of digital footprints and to recommend appropriate solution for the protection of a digital footprint.

Different kinds of digital footprints and their use are introduced in the theoretical part of the thesis. Among introduced uses of digital footprints are for example human resources management and marketing. Additionally, ways of tracking persons own footprint, is also introduced. Lastly the theoretical part also contains ways to hide and even delete footprints.

Ability of web browsers to protect the privacy of user is tested in the practical part of the thesis. Among the tested web browsers are both more user-friendly browsers and the more specialized browsers. Influence of VPN on the browsers ability to protect privacy is also tested.

Keywords: cookies, data security, digital footprint, passwords, tor, tracking, VPN, web browser

Obsah

Seznam Obrázků

1 Úvod

Internet v dnešní době pravidelně využívá většina lidí. V roce 2016 byl počet uživatelů internetu v České Republice 76,5%. Z této části populace však ne každý má s internetem rozsáhlé zkušenosti. Mnoho uživatelů internetu disponuje pouze velice základními znalostmi. Samotné užívání internetu přináší uživateli mnoho pozitivních věcí, ovšem mnohdy s sebou přináší také rizika. O těchto rizicích mnoho běžných uživatelů nemá žádný přehled. Pro mnoho z nich je internet pouze nástrojem k vyhledávání informací, rychlé komunikace či způsob trávení volného času.

Běžný uživatel si často neuvědomuje, že informace, které o sobě na internetu sdílí, pro něj mohou mít následky. Pouhý profil na sociálních sítích může být použit například ke sledování uživatelova pohybu. Pokud člověk pravidelně sdílí fotky, u kterých je vidět lokace, může tím předat i informaci o tom, že je mimo bydliště. Což může snadno vést například k vykradení domu.

Získání hesla na uživatelovo internetové bankovnictví může mít pro uživatele katastrofické následky. Mnohdy si uživatel neuvědomuje, kolik různých hesel lze získat přístupem na email, který se v dnešní době velice často používá k registraci na různé weby. Z emailu lze tedy získat nebo změnit hesla na mnohé další weby.

Toto téma jsem si zvolil kvůli jeho aktuálnosti a ve snaze rozšířit uživatelskou informovanost. V teoretické části budou popsány digitální stopy a možnosti jejich zneužití. V praktické části bude provedeno porovnání webových prohlížečů a doporučení vhodného prohlížeče.

2 Cíl práce a metodika

2.1 Cíl 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.

2.2 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.

3 Teoretická východiska

3.1 Digitální stopa

Digitální stopu uživatel vytváří veškerým svým pohybem a aktivitou na internetu a využíváním digitálních zařízení. Jedná se tedy o souhrn informací vytvářených používáním digitálních zařízeních.

„Digitální stopa je jakákoliv informace s vypovídající hodnotou, uložená nebo přenášená v digitální podobě.“ (1, s. 5)

Digitální stopy dělíme na aktivní a pasivní podle původu jejich vzniku.

3.1.1 Aktivní Digitální stopy

Aktivní stopy vznikají vlastním přičiněním uživatele, ovšem ne vždy s jeho plným vědomím. Nejčastěji v dnešní době vznikají aktivní digitální stopy právě používáním sociálních sítí, kde většina uživatelů sdílí osobní informace, hlasitě vyjadřuje svoje názory bez ohledu na to, jak snadno jsou dohledatelné a jak jim mohou uškodit. Aktivní digitální stopy jsou také například příspěvky na diskuzních fórech, záznamy z chatů, fotografie, videa a mnoho dalších věcí, které uživatel sám dobrovolně sdílí na internetu. Takové stopy mohou občas sdělovat mnohem více informací, než si sám uživatel uvědomuje. Například při žádosti o pomoc na technických fórech je mnohdy možné vidět úplné popisy problémů s technickými specifikacemi daného zařízení, nebo i celé domácí sítě. Aktivní digitální stopy je snazší ovlivnit a zakrýt změnou vlastního chování na internetu.

3.1.2 Pasivní Digitální stopy

Pasivní stopy vznikají bez vědomého přispění uživatele. Jedná se o vedlejší produkt uživatelovi aktivity na internetu. Jedná se nejčastěji o záznamy uživatelova chování na internetu, které si ukládají servery. Jde například o délku návštěvy daného webu, IP adresu atd. Takovéto záznamy si vede mnoho společností nabízející služby na internetu. Nemusí však jít pouze o samotnou uživatelovu aktivitu. V době chytrých lednicí a televizí je možné digitálně zjistit spoustu informací i mimo procházení internetu. Pasivní digitální stopy lze ovlivnit hůře než stopy aktivní.

3.2 Digitální stopy uložené lokálně

3.2.1 Cookies

Cookies jsou v HTTP protokolu malá množství dat, která si na klientské straně ukládá server. Používají se již od roku 1994. Cookies patří mezi pasivní digitální stopy. Při návratu na web, který vytvořil cookie, klient posílá cookie zpět serveru, který tím získá informace, které si na klientském zařízení uložil.

Každá cookie typicky obsahuje:

- Server, ze kterého byla poslána
- Životnost
- Hodnotu, většinou náhodně vygenerované unikátní číslo.

3.2.1.1 Využití

Cookies umožňují odlišit jednotlivé uživatele a uložit si tak o nich údaje pro daného klienta specifické (2). Cookies takto usnadňují personalizaci webů a udržování informací při pohybu v rámci webu nebo i při návratu. Typickým příkladem využití cookies je například nákupní košík na e-shopech. Na principu cookies pracují i statistiky webu a různé další nástroje webové analytiky, které si do cookies uloží identifikátor klienta, čas jeho návštěvy a další informace.

Právě tímto způsobem umožňují cookies sledovat pohyb uživatele po webu. Čehož je dosaženo, pokud například nějaká společnost má svůj widget na webové stránce. Při prvním navštívení takového webu se uloží cookies s unikátním identifikátorem klienta. Následně se pokaždé, když klient vstoupí na jiný web používající ten stejný widget, je zaznamenáno, na které weby tento identifikátor dříve přistupoval.

Z tohoto vyplývá, že pokud je cookies s unikátním identifikátorem pravidelně mazána, nelze pak tímto způsobem pohyb uživatele na internetu sledovat. Pravidelné mazání cookies tedy může toto sledování omezit.

3.2.1.2 Typy cookies

Cookies lze dělit podle životnosti.

Session cookies – Jsou to dočasné cookies, které jsou smazány po uzavření prohlížeče. Jako session cookie se ukládá například obsah košíku, který takto není ztracen při pohybu v rámci webové stránky (2).

Persistent cookies – Jsou cookies, které zůstávají uložené na disku, dokud je uživatel nesmaže manuálně nebo nevyprší jejich udaná platnost. Příkladem těchto cookies jsou například výše zmiňované cookies používané ke sledování pohybu na internetu.
Dále se dají dělit také podle původu.

Cookies první strany – Cookie uložená pomocí skriptu běžícího na dané doméně (2). Je obecně považována za bezpečnější, tím pádem lépe prochází skrze přísněji nastavené bezpečnostní zásady. Používá je například systém Google Analytics.

Cookies třetí strany – Cookie, která byla uložena skriptem z jiné domény než té, na které se uživatel právě nachází. Načítá se napříč doménami, čímž umožňuje sledování napříč internetem. Používá se pro cílení reklam.

3.2.1.3 Flash cookies

Flash cookies, také známé pod názvem Local Shared Objects, jsou textové soubory posílané klientovi, pokud si vyžádá obsah vyžadující Adobe flash. Na rozdíl od běžných cookies, které používají webové prohlížeče, se neukládají do složky prohlížeče, ale do vlastní složky Adobe flash. Flash cookies jsou méně známé a mohou obsahovat informace jako například to, kde uživatel přestal sledovat video nebo kde skončila animace reklamního banneru. A stejně tak jako klasické cookies je lze použít ke sledování pohybu uživatele na internetu. (3)

3.2.2 Další lokální data prohlížeče

Náš internetový prohlížeč ukládá velké množství dat na vlastní disk počítače. Nejnápadnějším příkladem je právě historie prohlížení, která obsahuje v podstatě kompletní záznam uživatelova chování na internetu. Většina prohlížečů nabízí nějakou formu anonymního prohlížení, při které se lokální data neukládají.

Prohlížeče kromě historie prohlížení také lokálně ukládají mnoho dalších údajů. Například historii stahování nebo historii formulářů, která se zobrazuje k napovídání při používání různých vyhledávačů a ukazuje tak co uživatel vyhledával v předchozích vyhledáváních.

Mnoho uživatelů může překvapit, jak snadné je dostat se k uloženým heslům na počítači. Google Chrome i Mozilla Firefox vám umožní zobrazit uložená hesla přímo v nastavení prohlížeče. Na což běžný uživatel nepomyslí, pokud předává své zařízení k opravě, nebo jej popřípadě někomu zapůjčuje. Lokální obsah by tedy před tím měl uživatel vymazat. Dále to samozřejmě znamená že při nakažení počítače virem nebo při jiném druhu

kybernetického útoku může útočník soubor s hesly poměrně snadno získat. Je tedy vhodné zvážit, zda předvyplněné přihlašovací formuláře za takové riziko opravdu stojí.

3.2.3 Web beacons

Web beacons jsou malé objekty vložené do webových stránek nebo emailů. Nejčastěji se jedná o transparentní gif s rozměrem 1x1 pixel. Rozměr 1x1 se pro web beacons používá, aby vyžadovaly minimální množství přenesených dat a tím neměly vliv na chod webu. Formát gif se využívá proto, že je podporován téměř všemi internetovými prohlížeči.

Pokud internetový prohlížeč narazí na web beacon, pošle žádost o stažení obrázku obsahující ip adresu, datum a čas i další údaje. Toto může vlastník serveru využít pro zjištění kolikrát a kdy byla stránka navštívena.

Web beacons jsou často používány pro sledování emailů (4). Pomocí web beacons je možné sledovat, zda byl email otevřen a kdy. Když se uživatel pokusí o načtení obrázku v emailu, server je upozorněn na přístup unikátního uživatele a tím dokáže identifikovat, že email byl otevřen. Podle času a ip adresy je pak možné zjistit, zda uživatel například klikl na odkaz uvnitř emailu a tím sledovat účinnost reklamy.

Při zakázání cookies v prohlížečích se zpravidla automaticky zakazují také web beacons (4).

3.3 Využití a zneužití digitálních stop

Digitální stopu lze využít mnoha způsoby, ať už jde o využití nebo zneužití. Proto je velmi důležité, aby si uživatel svých digitálních stop a jejich využití byl vědom. Může si tímto ušetřit mnoho ošklivých překvapení.

3.3.1 Personalistika

Personalisté v dnešní době používají digitální stopy pro rozhodování o přijetí zaměstnance velice často. Vzhledem k tomu, jak je snadné nalézt o téměř každém profil na Facebooku jednoduchým použitím internetového vyhledávače, tak by si každý měl ostražitě hlídat to, co o sobě na sociálních sítích zveřejňuje a jak má nastavený přístup ke svým

profilům (5). Pokud jste na sociálních sítích sdíleli například negativní kritiku na své bývalé zaměstnavatele, tak se vaše šance na přijetí do zaměstnání výrazně snižuje.

Podle Olivera Perkinse v roce 2015 používalo 52% zaměstnavatelů informace ze sociálních sítí. A 35% dokonce uvedlo, že je pravděpodobnější, že upřednostní člověka s volně dostupným profilem na sociálních sítích před někým, kdo takový profil vůbec nemá (6). Takže ani nevyužívání sociálních sítí není vždy dobrým řešením. Lidé by tedy při hledání práce měli na internetu prezentovat spíše čistý a profesionální dojem a hlídat si to co o nich lze dohledat, nikoliv to, aby o nich nebylo možné dohledat nic.

Zájemce o práci by si tedy nejdříve měl zjistit, co se zobrazí při vyhledávání jeho jména a popřípadě se to snažit upravit, pokud je to možné. Personalista může hledat informace, které podpoří to, že je pro práci kvalifikovaný, co o něm píší ostatní uživatelé a občas i přímo hledají důvod, proč zájemce nepřijmout (6).

3.3.2 Marketing

V marketingu se sleduje pohyb uživatele po internetu ve snaze najít vzorec, který by naznačoval o jaké produkty by mohl mít uživatel zájem a tím na něj byla cílena reklama, která na něj bude působit nejefektivněji. Například Google využívá informace o tom, jaké stránky uživatel navštěvuje, v jakých hodinách, co Googlem vyhledává, kde se fyzicky nachází a jaké reklamy viděl, popřípadě na ně klikl (7). Podle průzkumu provedeného Network Advertising Initiative je cílená reklama více než 2x efektivnější než reklama necílená (8).

3.3.3 Digitální forenzika

Digitální forenzika je aplikace forenzní vědy na elektronické důkazy v právních záležitostech. Zahrnuje obory, jako je například počítačová forenzika, forenzika mobilních zařízení, síťová forenzika (9). Mezi všemi těmito podtypy existují 4 základní principy (10):

- Pořízení
- Uchování
- Analýza
- Prezentace

3.3.3.1 Pořízení

Pořízení je samotný proces získání elektronických dat, může se jednat například o zabavení počítače z místa činu. Částí pořízení je také tvorba kopie samotných dat (9). V digitální forenzice pro proces kopírování dat používáme termín „Získání“.

Pořízení je prvním krokem zpracování důkazů a je kritické pro integritu důkazů. Právě při pořízení je nejvyšší šance poškození důkazů. Samotné zapnutí počítače nebo zařízení může vést k modifikaci mnoha důkazných souborů (9).

3.3.3.2 Uchování

Uchování je proces, který začíná již před pořízením důkazu a končí, pokud je důkaz zničen nebo předán vlastníkovi (9). Je nutné zachovat přesný přehled o tom, kdo měl k důkazu přístup a kdy, aby nedošlo ať k úmyslnému nebo neúmyslnému poškození.

3.3.3.3 Analýza

Analýza je proces, který ze získaných důkazů vyčlení ty části, které jsou relevantní pro daný případ. Každý případ je v tomto unikátní a správné provedení analýzy velice záleží na znalostech člověka který ji provádí (9).

3.3.3.4 Prezentace

Prezentace je posledním krokem ve forenzické analýze elektronických důkazů. Zahrnuje sepsání forenzní zprávy (9).

3.3.4 Kyberstalking

Kyberstalking je forma stalkingu, tedy opakovaného obtěžování a pronásledování oběti pachatelem, při které pachatel využívá informačních technologií například email nebo sociální sítě.

Kyberstalking dělíme na přímý a nepřímý. Při přímém kyberstalkingu pachatel obtěžuje oběť nevyžádanými zprávami nebo fotkami s nevhodným nebo nenávistným obsahem. Při nepřímém kyberstalkingu pachatel o oběti šíří nenávistné nebo nevhodné informace prostřednictvím internetových stránek nebo sociálních sítí nepřímo (11).

Oběti kyberstalkingu by hlavně neměli nevyžádané zprávy mazat. Takovéto zprávy je vhodné zachovat a nahromadit. Je také vhodné vést si seznam veškerého kontaktu s pachatelem. Potom co se důkazy nahromadí a lze na nich prokázat, že se nebezpečnost pachatele stupňuje, měla by oběť důkazy předat policii, která podle nich může provést opatření (12).

3.3.5 Kyberšikana

„Jde o šikanu, která probíhá v prostředí virtuálním, prostřednictvím moderních komunikačních technologií (13,s 63).“

Zpravidla se tedy jedná o to, že nějaké dítě nebo skupina dětí psychicky týrá jiné dítě. U kyberšikany je problémem to, že je často těžší ji odhalit. Nezanechává totiž viditelné stopy a je čistě psychická. U kyberšikany je také typické, že samotní pachatelé ji vidí jako pouhý vtip a nemají tedy ani v úmyslu nějak vážněji oběť poškodit. Podle výzkumu z roku 2012 v Kanadě 95% pachatelů vidělo kyberšikanu pouze jako vtip (14). Nicméně kyberšikana, stejně jako každý jiný typ šikany, může mít vážné následky. Šikanované dítě může dohnat dokonce až k sebevraždě. Kyberšikana se ovšem netýká jen dětí. Její obětí se může stejně tak stát dospělá osoba. Nejčastěji je zaměřená právě na učitele.

3.3.6 Krádež Identity

Krádež identity je snaha vydávat se za někoho jiného. V současné době se krádež identity nejčastěji odehrává právě v prostředí internetu. Založit falešný profil není nijak náročné i s poměrně malým množstvím informací. A čím víc informací o oběti pachatel získá, tím těžším se stává odhalení falešné identity a tím horší mohou být následky. Je tedy rozumné pro každého uživatele si svou digitální stopu pečlivě hlídat.

Z právního hlediska je krádež identity dvoustupňový trestný čin. V první fázi pachatel získá informace k odcizení identity například odcizením dat pomocí nějakého digitálního útoku nebo sociálním inženýrstvím. Ve druhé fázi získané údaje nějakým způsobem zneužije. Pokud jde o zneužití za cílem finančního zisku, kategorizuje se jako podvod. Pokud jde o poškození druhé osoby, považuje se za poškozování cizích práv (15).

Motivem ke krádeži identity může být snaha o pošpinění dobrého jména nebo snaha získat nějaký finanční zisk. Snahu o pošpinění dobrého jména vidíme na internetu velmi často u velkých firem nebo například u známých osobností. Ovšem i pro obyčejného člověka může v extrémních případech vést například i k problémům v zaměstnání a dalším důsledkům.
K získání údajů pro krádež identity na internetu je často využíván phishing nebo pharming.

3.3.6.1 Phishing

Za phishing považujeme podvodné emailové útoky, které se snaží vylákat z uživatele citlivé informace (16). Nejčastěji je jejich cílem získat údaje o platebních kartách, přihlašovací údaje na různé weby, nejčastěji internetové bankovnictví.

Phishingový email se snaží vypadat co nejvíce jako email od organizace, jejíž informace se z klienta snaží vylákat. Často se jedná o různé výzvy ke změně hesla nebo falešné informace o nepodařené platbě, které obsahují odkaz na web připomínající web originální ve snaze přimět uživatele zadat své heslo (17). Uživatelé by tedy nikdy neměli zadávat své osobní údaje do odkazů, které jim přichází v emailu a nejlépe na takové odkazy ani neklikat.

Nejlepší obranou před phishingem je obezřetnost. Pokud uživatel nekliká na odkazy v nevyžádaných emailech ani neotvírá jejich přílohy, je poměrně v bezpečí. Dále by uživatel samozřejmě měl kontrolovat webovou adresu stránek, na kterých se nachází. Podvodné stránky mohou často vypadat stejně, ale v jejich adrese obsahují překlep nebo jsou na jiné top level doméně (16). Používání aktuálních antivirových programů je také důležité, některé antivirové programy mají i antiphishingovou funkci.

3.3.6.2 Pharming

Jedná se o variantu útoku, při které útočník napadne DNS server, a tím změní překlad adresy například internetového bankovnictví na stránku podvodnou, která je od ní téměř nerozeznatelná, a i v adresním řádku se zobrazuje správná adresa (18). Nejjednodušším způsobem, jak toto provést je podstrčení falešného souboru hosts, ve kterém útočník lokálně změní nastavení překladu adresy pro daný web (17). Tím dosáhne přesměrování na jinou adresu, které není uživatelem snadno zjistitelné. Podstrčení falešného souboru se realizuje nejčastěji při nakažení počítače virem.

3.4 Sledování vlastní stopy

Jak již bylo zmíněno, tak by si uživatel měl svou vlastní digitální stopu kontrolovat, aby věděl, co je o něm na internetu k nalezení. Sledování aktivních stop není příliš složité, sledování pasivních stop může být o něco problematičtější.

3.4.1 Egosurfing

Je nejčastější a nejjednodušší způsob sledování vlastní digitální stopy. Jde o vyhledávání svého jména, přezdívky a dalších informací pomocí internetového vyhledávače. Tímto způsobem můžete snadno a rychle ověřit, co je o vás na internetu zjistitelné.

Jako efektivnější varianta k egosurfingu je vyhledávat své osobní informace na specializovaných vyhledávačích, které slouží k vyhledávání lidí. Tyto vyhledávače se

nazývají People search engines a jejich výsledky pro vyhledávání lidí bývají přesnější a přehlednější.

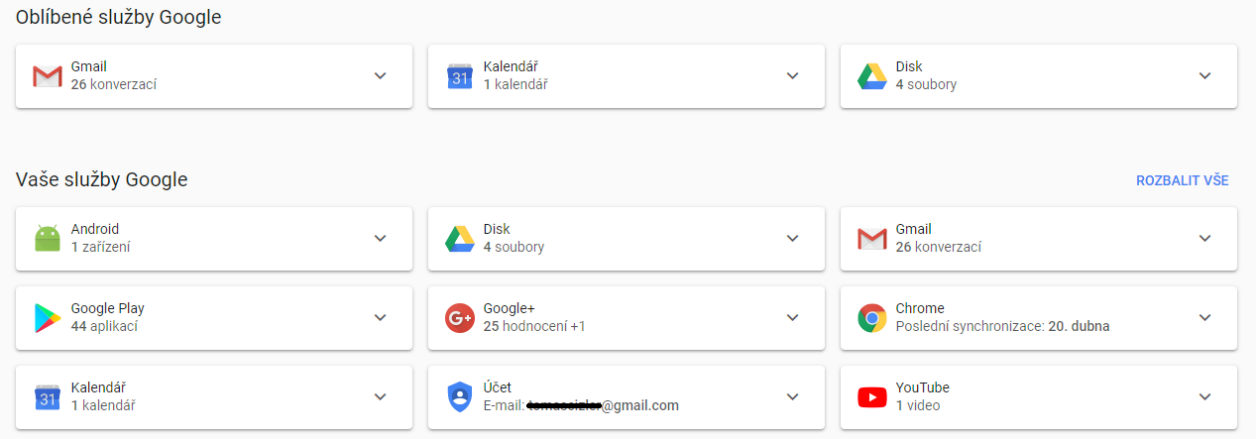
3.4.2 Facebook

Facebook nabízí službu, díky které je možné si stáhnout všechna data, která o uživateli Facebook má. V těchto datech je možné nalézt poměrně zajímavé informace. Obsahuje to například záznamy o všech konverzacích, seznam přátel, seznam smazaných přátel, veškeré stránky a média označená jako pro vás zajímavé. Dále zde lze nalézt například historii připojení k Facebooku nebo reklamní okruhy, které pro uživatele Facebook zvolil a historii reklam na které klikl.

Na Facebooku lze také nastavit a upravovat preference cílené reklamy. V nastavení Facebooku lze tyto preference upravit v záložce reklamy. Zde je možné nastavit také to, zda se na vás má cílená reklama používat na celém Facebooku, nebo popřípadě lze cílenou reklamu na základě facebookových údajů vypnout jen pro ostatní partnerské weby.

3.4.3 Google dashboard

Google nabízí možnost prohlédnout si a spravovat údaje, které o vás má ve svých službách uložené. V dashboardu je možné si je po přihlášení prohlédnout. Je tímto možné snadno najít například zapomenutá videa na Youtube, která uživatel nahrál pod svým jménem, informace ze starého účtu na Google+, nebo i propojené aplikace, které využívají jeho Google účet. Tato data jsou přístupná veřejně pouze pro účet, ze kterého je uživatel přihlášen. V Google dashboard lze také stáhnout archiv obsahující všechna data o vašem účtu.



Obrázek 1 Google dashboard (Zdroj: Vlastní tvorba)

3.4.4 Google alerts

Google alerts je Google služba, která nabízí upozorňování na nové výsledky pro zadanou frázi. Pokud pro danou frázi vznikne nový výsledek, pošle vám emailem upozornění. Je zde možné nastavit, z jakých zdrojů se mají upozornění brát, jak často se vám mají aktualizace posílat, nebo v jakém jazyce či regionu je výsledek uveden. Často se tato služba používá pro sledování věcí, které uživatele zajímají. Ke sledování digitální stopy je tedy snadno možné alerts použít, aby za uživatele automaticky prováděli egosurfing. Stačí do alerts zadat jako parametr například své jméno nebo přezdívku a budou nás upozorňovat, pokud se o vás na webu objeví zmínka.

3.4.5 Pasivní digitální stopy

Kontrolovat své pasivní digitální stopy není tak snadné. Běžný uživatel o jejich existenci většinou neví a nevšímá si, jaký na něj mají vliv. Trackerů, které o vás zjišťují informace je na internetu mnoho. Většinu z nich nemá uživatel po jejich vzniku možnost ovlivnit. Některé společnosti vám umožňují si data, která o vás nasbírali pasivně zobrazit, upravit je nebo dokonce i smazat. Ovšem nikdy se uživateli nepodaří smazat údaje ze všech trackerů, nanejvýš je tedy možné smazat údaje právě z trackerů nejvíc rozšířených.

3.4.5.1 Google

Google používá získaná data k cílení reklamy. Dokonce uživatelům poskytuje možnost si vlastní cílenou reklamu řídit nebo popřípadě vypnout. Své nastavení cílené reklamy si může uživatel zjistit na webu https://adssettings.google.com/authenticated. Google s použitím digitální stopy sestaví jakýsi profil, do kterého uživatel zapadá. Takto si může uživatel zjistit, co o něm vypovídá jeho digitální stopa. Na tomto webu může uživatel spravovat, jaká témata ho zajímají, nebo dokonce zcela vypnout cílenou reklamu ve službách Google. Někteří uživatelé mohou také mít zájem si tento profil upravit, aby doopravdy seděl realitě. Jde sice o narušení vlastního soukromí, ale pokud má uživatel zájem o opravdu kvalitní cílenou reklamu, tato možnost se nabízí.

3.4.5.2 Bluekai

Data o uživatelích sbírá i společnost Oracle. Její výsledky jsou ke zobrazení na webu http://bluekai.com/registry/. Zde se můžete dozvědět, jaká témata k vám na základě vaší digitální stopy přiřadil Oracle. Je zde také možné získat takzvanou Opt-out cookies, která zabrání službám Oracle sbírat vaše data (19).

3.5 Omezování Digitální stopy

3.5.1 Chování na internetu

Ač není snadné zcela zabránit tvorbě digitálních stop, je poměrně snadno možné je alespoň redukovat. Uživatel by se měl snažit chránit si především své jméno a jeho asociaci s různými online přezdívkami, své telefonní číslo, svůj osobní email a fotografie. Jak šíření těchto věcí zabránit? Pro email je nejsnadnějším řešením pravděpodobně využití více emailových adres. Zejména pro své volnočasové aktivity by měl uživatel využívat oddělený email a pro aktivity profesionálnějšího charakteru využívat email striktně profesionální. Na volnočasových webech a webech, kde není zcela nutné sdílet své pravé jméno, stojí za to využívat nějaký pseudonym, popřípadě zkomoleninu vlastního jména a nezadávat své telefonní číslo. Dále je možné využívat více platebních karet, údaje o platebních kartách jsou v dnešní době považovány za velice zajímavé.

Uživatel by měl využívat více hesel a snažit se nepoužívat pro důležité účty hesla stejná jako pro účty méně důležité. Ideálně by bylo vhodné používat pro každou službu jiné heslo, obzvlášť poté využívání stejného hesla na email jako na službu, která je na email zaregistrována je velice nebezpečné. Samozřejmostí také je dodržovat zásady o složitosti hesel. Heslo, které neobsahuje žádná čísla ani speciální znaky není příliš bezpečné. Dále také není vhodné používat jako hesla informace, které lze získat sociálním inženýrstvím, věci jako datum narození, jména rodinných příslušníků nebo domácích mazlíčků jsou velmi snadno odhadnutelná. Dále by se uživatel měl vyhýbat heslům, která jsou často používaná a jednoduchá. Právě tato hesla útočník zkusí při slovníkovém útoku jako první. Hesla typu „heslo123“ nebo „letmein“, ať už jakkoliv snadno zapamatovatelná, nejsou nikdy dobrým nápadem (6).

Dále stojí za to podívat se na nastavení sdílení informací na svých účtech na sociálních sítích. Při správném nastavení soukromí je možné zajistit, aby informace o uživateli nebyly snadno dohledatelné, nebo dokonce zvolit, které příspěvky budou veřejné a které naopak ne. Jak již bylo zmíněno v kapitole o personalistice, personalisté nemusí mít zájem o lidi, o kterých nelze najít nic. Oproti tomu, pokud si veřejné příspěvky uživatel vhodně spravuje, je možné tím prezentovat mnohem profesionálnější obraz. Na Facebooku je dokonce možné nastavit si mezi příteli okruhy tak, aby určité příspěvky viděla pouze určitá skupina vašich přátel. Tímto lze poměrně snadno oddělit profesionální a pro veřejnost vhodný obsah od obsahu soukromého v rámci jednoho profilu.

3.5.2 Nastavení prohlížeče

Špatně nastavený prohlížeč zanechává velice silnou digitální stopu. Lokální obsah ve formě cookies a jiných místních dat se v prohlížeči hromadí, je tedy vhodné nastavit prohlížeč tak, aby tyto údaje pravidelně mazal.

Toto lze také vyřešit použitím Anonymního prohlížení, které dnes podporuje téměř každý prohlížeč. Při anonymním prohlížení prohlížeč nevyužívá žádný předchozí uložený lokální obsah a veškerá data vytvořená prohlížením jsou po ukončení relace smazána. Ovšem použitím anonymního prohlížení uživatel samozřejmě ztrácí výhody, které uchovávání lokálních dat přináší například trvalá přihlášení a personalizace webů.

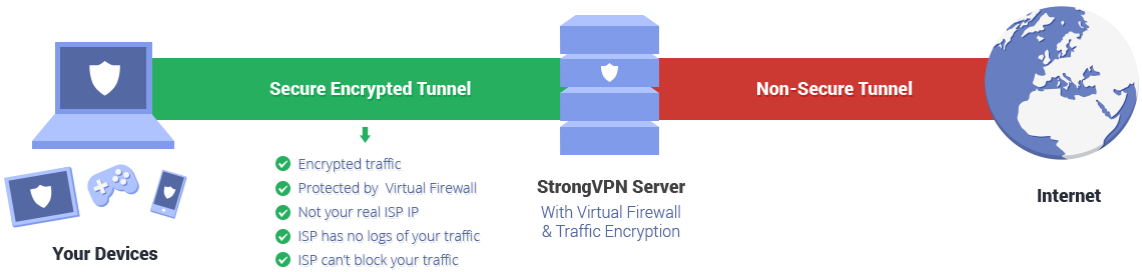
Lze také využít funkci „Do not track me“. Kdy se do hlaviček HTTP requestů přidá do not track me, čímž uživatel požaduje, aby o něm nebyla uchovávána data. Dodržování DNT není nijak závazné, je tedy na poskytovateli služby, do jaké míry a zda vůbec vám vyhoví, ovšem také DNT nepřináší v podstatě žádné nevýhody. Stojí proto za to si ji zapnout. DNT je možné zapnout v nastavení soukromí téměř všech prohlížečů.

3.5.3 VPN

VPN propojuje počítače do zabezpečené soukromé sítě, i pokud jsou na různých místech v internetu. Nejčastěji se s nimi setkáme například při připojování se do firemních sítí z míst mimo firmu (20). V dnešní době se stále více rozvíjí soukromé využití VPN, především protože VPN zakrývá adresu a další informace o klientském počítači a zaměňuje je za údaje o serveru poskytujícím VPN (21).

Data se prostřednictvím VPN klienta zašifrují na uživatelově počítači a potom jsou tunelem odeslána na VPN server, kde se rozšifrují a VPN server je odešle na cílovou stránku. Samozřejmě z tohoto principu vyplývá nutnost toho, aby klient věřil právě svému poskytovateli VPN, na jehož serveru jsou data rozšifrována (20).

Většina dostupných kvalitních VPN služeb je placená (21). A je samozřejmě třeba počítat i s tím, že VPN zpomalí rychlost internetového připojení a zvýší dobu odezvy. Obzvláště pak VPN, které jsou dostupné zadarmo, bývají velice pomalé.



Obrázek 2 Princip fungování VPN (Zdroj: https://strongvpn.com/security.html)

3.5.4 Web proxy

Web proxy je rychlý způsob, kterým lze zamaskovat ip adresu při surfování na internetu. Web proxy nevyžaduje instalaci žádného softwaru a lze je použít přímo z prohlížeče (22). Proxy server se chová jako prostředník pro komunikaci s koncovým serverem a posílá mu komunikaci se svou ip adresou. Proxy server tedy vaší ip adresu zná a prochází jím veškerá komunikace, většinou nezašifrovaná. Proto by se z web proxy serveru nemělo přistupovat na stránky, které vyžadují přihlášení. Web proxy serverů je na internetu dostupných celá řada. Servery dostupné zdarma jsou zpravidla pomalé. Toto lze vyřešit opět zaplacením prémiových serverů.

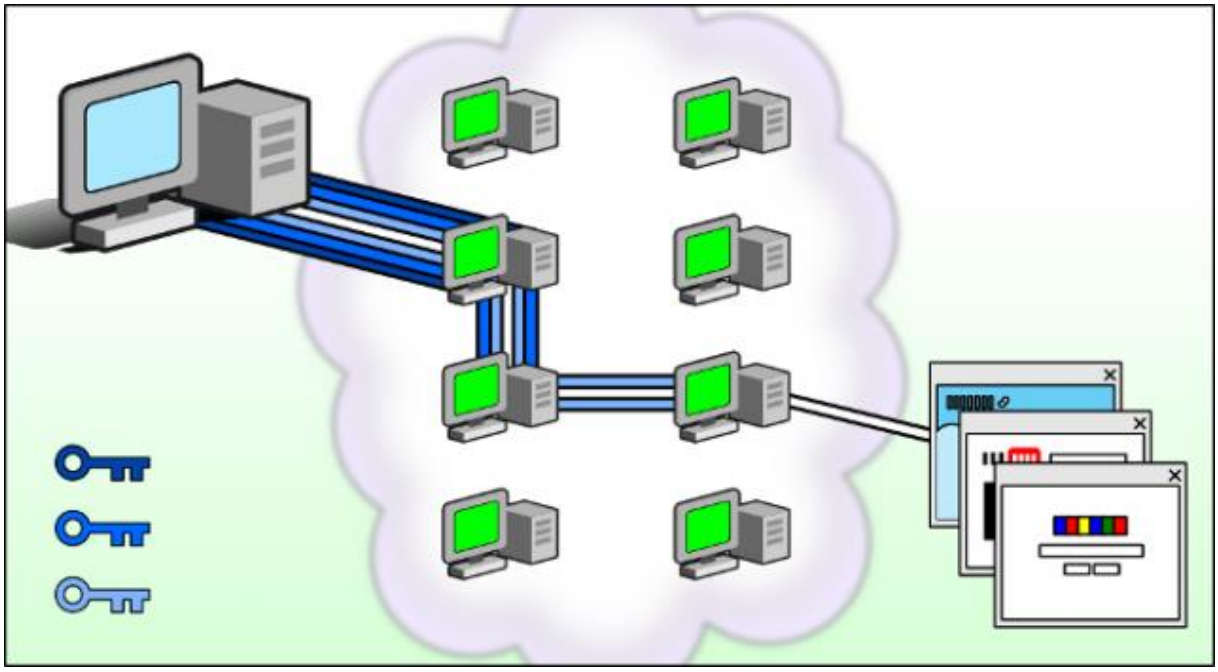
3.5.5 Tor

Metoda Tor funguje na principu postupně zesilujícího zašifrování komunikace. Při použití této metody komunikace prochází přes větší množství počítačů, takzvaných uzlů, kdy každý z nich má informace pouze o uzlu předešlém (23). Každý uzel zašifrovaná data opět zašifruje a zašifrování se tímto vrství, od čehož pochází název The Onion Routing. Slabinou je koncový uzel, na němž se data rozšifrují.

Z důvodů počtu uzlů, přes které se data přenáší a mnohdy jejich geografické vzdálenosti je přenosová rychlost při použití Toru často velmi nízká. Proto Tor není příliš vhodný k běžnému používání. Používá se často pro obcházení vládní cenzury nebo jej používají různé nevládní organizace, které chtějí skrývat svou činnost (23). Tor je také často spojován s nelegální činností.

Nejjednodušším způsobem, jak používat tor je nainstalováním Tor browseru, což je internetový prohlížeč, který umožňuje připojení přes síť tor. Dále lze tor nakonfigurovat i pro

použití mimo webový prohlížeč. To je ale složitější proces.



Obrázek 3 šifrování TOR (zdroj: https://www.extremetech.com/extreme/211169-mit-researchers-figure-out-how-to-break-tor-anonymity-without-cracking-encryption)

3.6 Odstranění digitální stopy

Výše byly uvedeny způsoby, jak svou digitální stopu najít. Pokud svou digitální stopu dokážeme najít, dokážeme se jí také zbavit? Úplné odstranění digitální stopy je velice těžko realizovatelné. Většinou se uživateli podaří odstranit jen její větší část. Aktivní stopy lze odstranit poměrně snadno, pokud jde o místa, která má uživatel pod vlastní správou. Problém nastává, pokud je obsah sdílený na servery nebo profily na sociálních sítích pod správou jiného člověka. Jejich odstranění je potom téměř nemožné. Uživatelova jediná možnost je potom kontaktovat vlastníky jednotlivých serverů nebo profilů a žádat o smazání obsahu. Ne všechny internetové služby poskytují uživateli možnost úplně odstranit svůj profil. Občas nejlepší, co může uživatel udělat je upravit informace na profilu a odstranit příspěvky, ale přesto jeho profil zůstává na síti. Informace o náročnosti smazání profilů na jednotlivých službách je možné najít na adrese http://www.justdelete.me/ (6). Na tento web stojí za to se podívat před vytvořením profilu na některé z daných webových stránek a zvážit, zdali tam uživatel opravdu chce zadávat informace. Občas uživatel nemá na výběr a profil si opravdu založit potřebuje, nicméně zde se nabízí možnost používat falešné informace, pokud to je možné.

4 Vlastní práce

4.1 Běžné webové prohlížeče

Nejběžněji používané webové prohlížeče jako například Google Chrome, Mozzila Firefox a další často sdílí mnoho informací o uživateli. Takovéto prohlížeče preferují uživatelské pohodlí a jednoduchost používání před bezpečností. Lze jim nastavit i zvýšenou úroveň zabezpečení a uchovávání soukromí, ovšem tímto uživatel ztrácí některé funkce, na které je při surfování na internetu zvyklý. Například zakázání používání cookies výrazně sníží sledovatelnost uživatele na internetu, ovšem za cenu snížené použitelnosti nebo i dokonce nevyužitelnosti některých webů. Weby vyžadující přihlášení jsou bez cookies nedostupné. Důsledkem toho, že cookies využívají pro udržení informací o přihlášeném uživateli. Pro omezení sledování je možné zakázat cookies třetích stran, které jsou nejčastěji používány ke sledování pohybu mezi různými weby.

Tyto prohlížeče většinou nabízí nějakou formu anonymního prohlížení, která však pouze zajistí smazání historie a dalších lokálních dat po ukončení anonymního prohlížení, což je sice užitečná funkce, ovšem nepřinese nijak převratný rozdíl v anonymizaci.

Pro testy byl využit test anonymity na webu ip-check.org, který provozuje německá společnost JonDos GmbH, která také poskytuje vlastní anonymizační prohlížeč JonDoBrowser. V následujícím testu je testován jako zástupce běžných prohlížečů Google Chrome verze 63.0.3239.132.

Your IP	217.168.215.130	Traceroute
Your location	Stredocesky kraj, Horni Pocaply	Show on map
Your net provider	T¢□	Whois IP
Reverse DNS	IP-15-130.trionet.cz	Whois Domain

WARNING: You are supposed to surf with your own or an inadequately protected IP address. You are observable.

WARNING: Your browser sends data that may allow web sites to track your computer easily!
Move your mouse over the underlined fields in order to get detailed information.
Learn more about the individual tests performed by the IP Check... Click here!↗

Attribute	Value	Rating
Cookies	Third party sites get your cookies and may track you.	bad
HTTP session	unlimited	bad
Signature	1142a9b979396a415ad2a8176e56b2f9	good
User-Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36	bad
SSL_session_id		neutral
Language	cs-CZ,cs;q=0.9	medium
Content types	text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8	medium
Encoding	gzip, deflate	good
Do-Not-Track		good
Upgrade-Insecure-Requests	1	good

Flash Cookies	ON (Click here to fix this problem)
Fonts	244
Flash Player	Google Pepper [WIN 28,0,0,137]
Operating system	Windows 10 [cs, Fri Feb 2 2018 04:12:24 PM]
Screen	1920*1080, 72 DPI

Attribute	Value	Rating
JavaScript	JavaScript is activated! (Version: 1.7)	medium
Plugins	Found 5 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: 9795608	medium
Tab history	There are 5 pages in your tab history.	medium
Local storage	Local storage is enabled. Your unique ID: 19795608	medium
Screen	1920 x 1080 pixels 24 bit color depth	medium
Screen (usable)	1920 x 1040 pixels (does not match screen)	medium
Browser window	1920 x 949 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 (Fri Feb 02 2018 16:15:14 GMT+0100 (Střední Evropa (běžný čas)))	medium
Fonts	141 installed fonts have been found on your computer.	medium

Obrázek 4 Ip-check anonymity test Google Chrome

Z výsledku testu je vidět že Google Chrome žádným způsobem nezakrývá uživatelovu ip adresu. Ostatní údaje ukazují, co všechno je možné o prohlížeči zjistit. Zelená pole

představují ideální výsledky. Oranžová pole poukazují na nastavení, která nejsou ideální, ovšem nejsou považována za kritická. Červená pole poukazují na zásadní nebezpečí pro zachování anonymity.

Výsledky jsou zcela identické, pokud je test proveden v anonymním okně. Z čehož je možné soudit, že anonymní režim sám o sobě nepřináší žádnou významnou změnu anonymity prohlížeče.

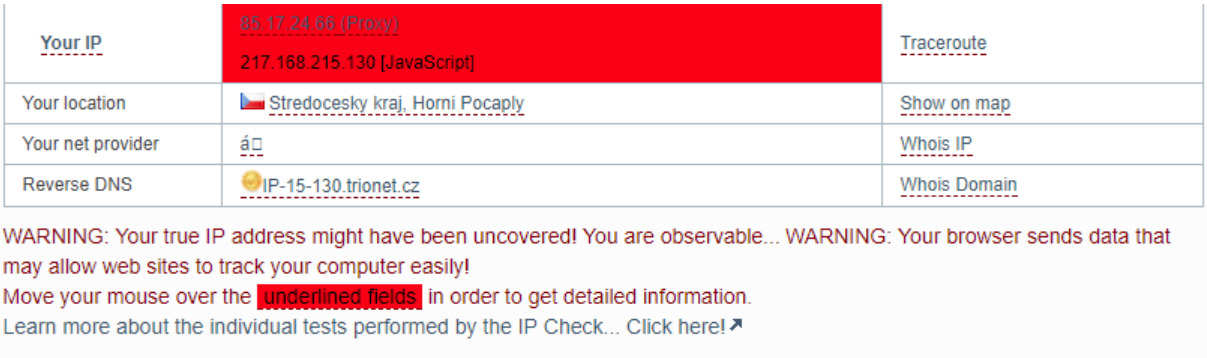
Změnou nastavení prohlížeče lze některé výsledky zlepšit. Například vypnutí ukládání cookies třetích stran je snadno nastavitelné v samotném Chrome bez většího omezení uživatelského pohodlí. Vidíme také, že je aktivovaná hlavička Do-Not-Track, která je v základním nastavení prohlížeče vypnutá. Za velké nebezpečí jsou považované také doplňky, které si mohou o uživatelově aktivitě samy ukládat informace, čímž představují velké riziko pro anonymitu. Zajímavou informací jsou také například dostupné fonty písma, jejichž kombinace může přispět k identifikaci. U fontů také vidíme že Google Chrome nepoužívá všechny dostupné fonty, ovšem z pluginu flash byli zjistěny i nainstalované fonty, které Chrome nevyužívá.

Z testu také vyplývá, že flash cookies jsou pro anonymitu nebezpečné. Google Chrome vyžaduje při základním nastavení ruční aktivaci pro každé využití doplňku flash, lze jej také aktivovat pro všechny instance flashe na určité doméně.

4.2 Google chrome + Webové proxy

Webová proxy jsou rychlým způsobem, jak zamaskovat ip adresu. Jsou poměrně snadno dostupná a sehnat je zdarma není zpravidla problém. Nevyžadují instalaci žádného softwaru, uživateli stačí přijít na web, který tuto službu nabízí a zadat cílový web ke kterému se chce připojit.

Pro testování byl použit web hideproxy.me, který své webové proxy nabízí zdarma.



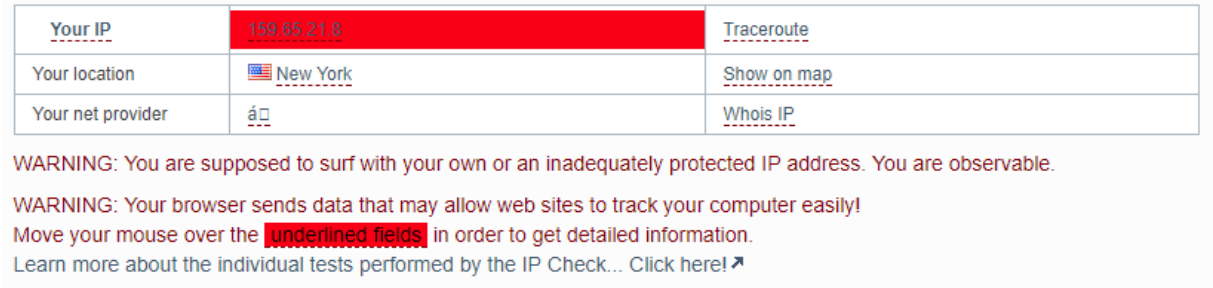
Obrázek 5 Ip-check anonymity test web proxy

Z výsledků je vidět že i přes použití web proxy ip-check originální adresu odhalil. K odhalení byl použit Javascript. Tento způsob odhalení vyžaduje specifický skript, který se nenachází na všech webech. Web proxy by tedy bylo úspěšné, pokud by se cílový server specificky nesnažil o odhalení pravé ip adresy. Je tedy možné říct, že pro některé účely a určité weby má použití web proxy smysl. Zbytek výsledků byl totožný s předchozím testem, protože web proxy se snaží pouze o skrytí ip adresy.

Při používání web proxy, obzvláště volně dostupných, je velice znatelné zpomalení rychlosti připojení. Využití volně dostupného web proxy je tedy pro běžné využívání nepříliš praktické. Vhodné je spíše pro jednorázová připojení bez nutnosti instalace zvláštního software.

4.3 VPN

VPN, jak již bylo popsáno výše, používá zašifrování k vytvoření virtuální soukromé sítě. Výhodou VPN je, že umožňuje šifrování veškeré internetové komunikace a nevztahuje se pouze na prohlížeč. Volně dostupná VPN jsou zpravidla silně omezená. Jako poskytovatel pro tento test VPN byl použit TunnelBear. TunnelBear nabízí své VPN uživatelům zdarma s limitem 500MB dat měsíčně. Což je limit pro běžné užívání nedostatečný, ale na rozdíl od například web proxy je rychlost spojení poměrně vysoká.



Obrázek 6 Ip-check anonymity test Chrome + Tunnelbear

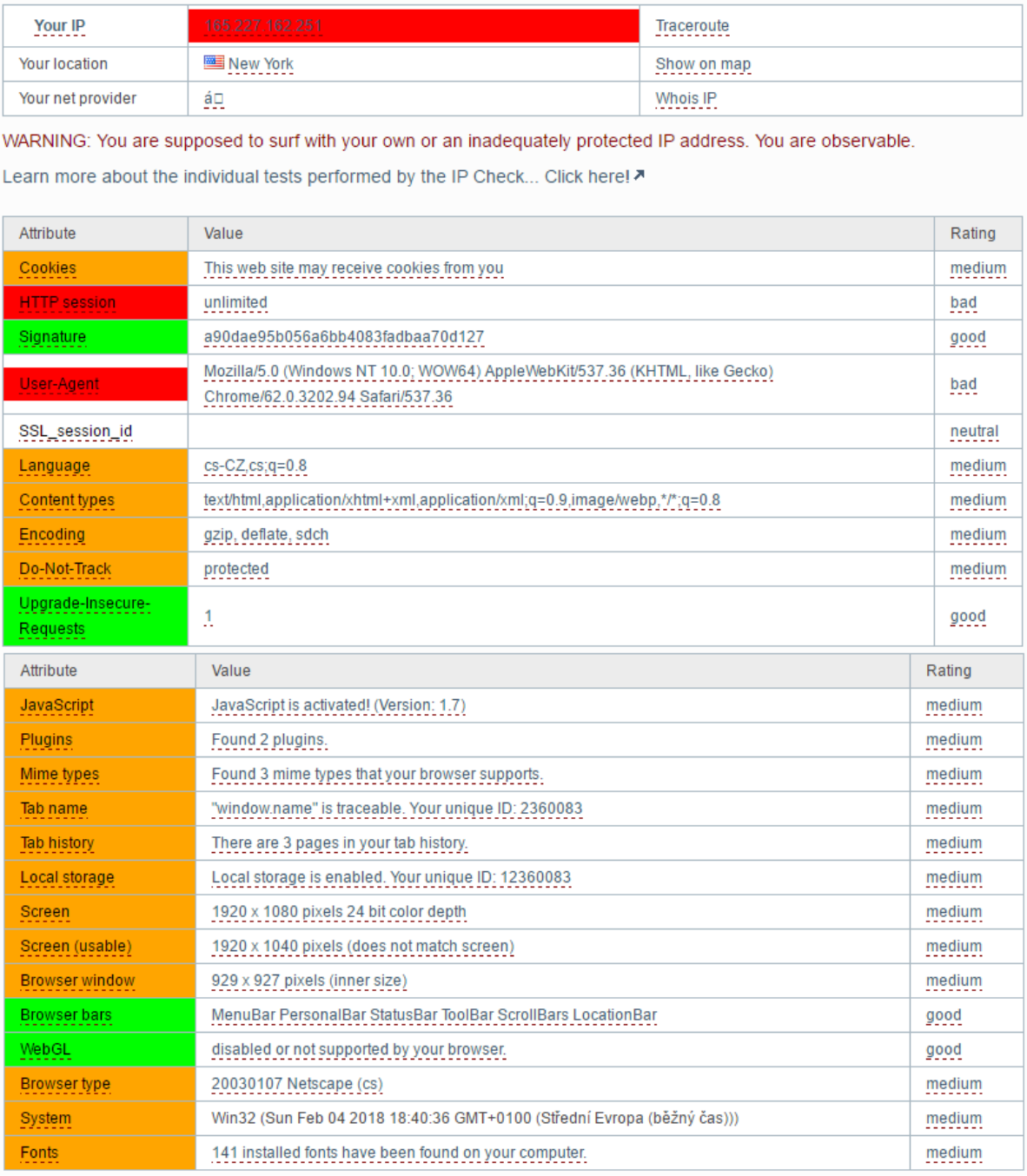
Z výsledků vidíme, že pro VPN úspěšně ukryl ip adresu i před javaskriptem a ipcheck tedy nezaregistroval použití proxy.

Zbytek výsledků byl opět totožný vzhledem k využití prohlížeče Google Chrome.

4.4 Epic privacy browser

Epic privacy broser je prohlížeč postavený na základě open source prohlížeče Chromium. Je zaměřený na ochranu soukromí uživatele s co nejmenším narušením pohodlí prohlížení. Snaží se uchovávat co nejméně informací a zabraňuje trackerům a dalším způsobům sledování na internetu. Má zabudovaný i vlastní adblocker. Nabízí také

zabudované šifrované proxy, které zpravidla nabízí překvapivě vysokou přenosovou rychlost pro volně dostupné proxy. Umožňuje také snadné individuální nastavení pro specifické webové stránky.



Your IP	165.227.162.251	Traceroute
Your location	New York	Show on map
Your net provider	á□	Whois IP

WARNING: You are supposed to surf with your own or an inadequately protected IP address. You are observable.

Learn more about the individual tests performed by the IP Check... Click here!

Attribute	Value	Rating
Cookies	This web site may receive cookies from you	medium
HTTP session	unlimited	bad
Signature	a90dae95b056a6bb4083fadbaa70d127	good
User-Agent	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36	bad
SSL_session_id		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, sdch	medium
Do-Not-Track	protected	medium
Upgrade-Insecure-Requests	1	good

Attribute	Value	Rating
JavaScript	JavaScript is activated! (Version: 1.7)	medium
Plugins	Found 2 plugins.	medium
Mime types	Found 3 mime types that your browser supports.	medium
Tab name	"window.name" is traceable. Your unique ID: 2360083	medium
Tab history	There are 3 pages in your tab history.	medium
Local storage	Local storage is enabled. Your unique ID: 12360083	medium
Screen	1920 x 1080 pixels 24 bit color depth	medium
Screen (usable)	1920 x 1040 pixels (does not match screen)	medium
Browser window	929 x 927 pixels (inner size)	medium
Browser bars	MenuBar PersonalBar StatusBar ToolBar ScrollBars LocationBar	good
WebGL	disabled or not supported by your browser.	good
Browser type	20030107 Netscape (cs)	medium
System	Win32 (Sun Feb 04 2018 18:40:36 GMT+0100 (Střední Evropa (běžný čas)))	medium
Fonts	141 installed fonts have been found on your computer.	medium

Obrázek 7 Ip-check anonymity test Epic privacy browser

Zabudované proxy úspěšně skrylo ip adresu i před Javaskriptem. Celkově je zbytek výsledků porovnatelný s ideálně nastaveným Google Chrome. Ovšem Epic Privacy Browser je takto nastaven už po instalaci. S ohledem na další nabízené funkce má nad Chrome značné

výhody obzvláště pro uživatele, kteří nejsou technicky zdatní nebo nemají zájem o vlastní nastavování prohlížeče.

Zvláštní se může zdát neaktivovaná hlavička Do-Not-Track, která je ovšem v prohlížeči aktivovaná, ale ipcheck ji nehlásí.

4.5 Tor browser

Tor browser je oficiální prohlížeč od Tor Core People, který používá vrstvené šifrování, jak již bylo popsáno výše. Je založený Mozzila firefox. Testována byla verze 7.5.

Your IP	171.25.193.77 (Tor)	Traceroute
Your location	Sweden	Show on map
Your net provider	á	Whois IP
Reverse DNS	tor-exit1-readme.dfri.se	Whois Domain

Learn more about the individual tests performed by the IP Check... Click here!

Attribute	Value	Rating
Cookies	This web site may receive cookies from you	medium
HTTP session	10 minutes (until your Tor identity is changed)	medium
Signature	8ab3a24c55ad99f4e3a6e5c03cad9446 (Firefox)	good
User-Agent	Mozilla/5.0 (Windows NT 6.1; rv:52.0) Gecko/20100101 Firefox/52.0	good
SSL_session_id	8EE3A5AFA453998A857D24D398070BA78BA69702D153A1D8A3FCF4F203764785	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
Upgrade-Insecure-Requests	1	good

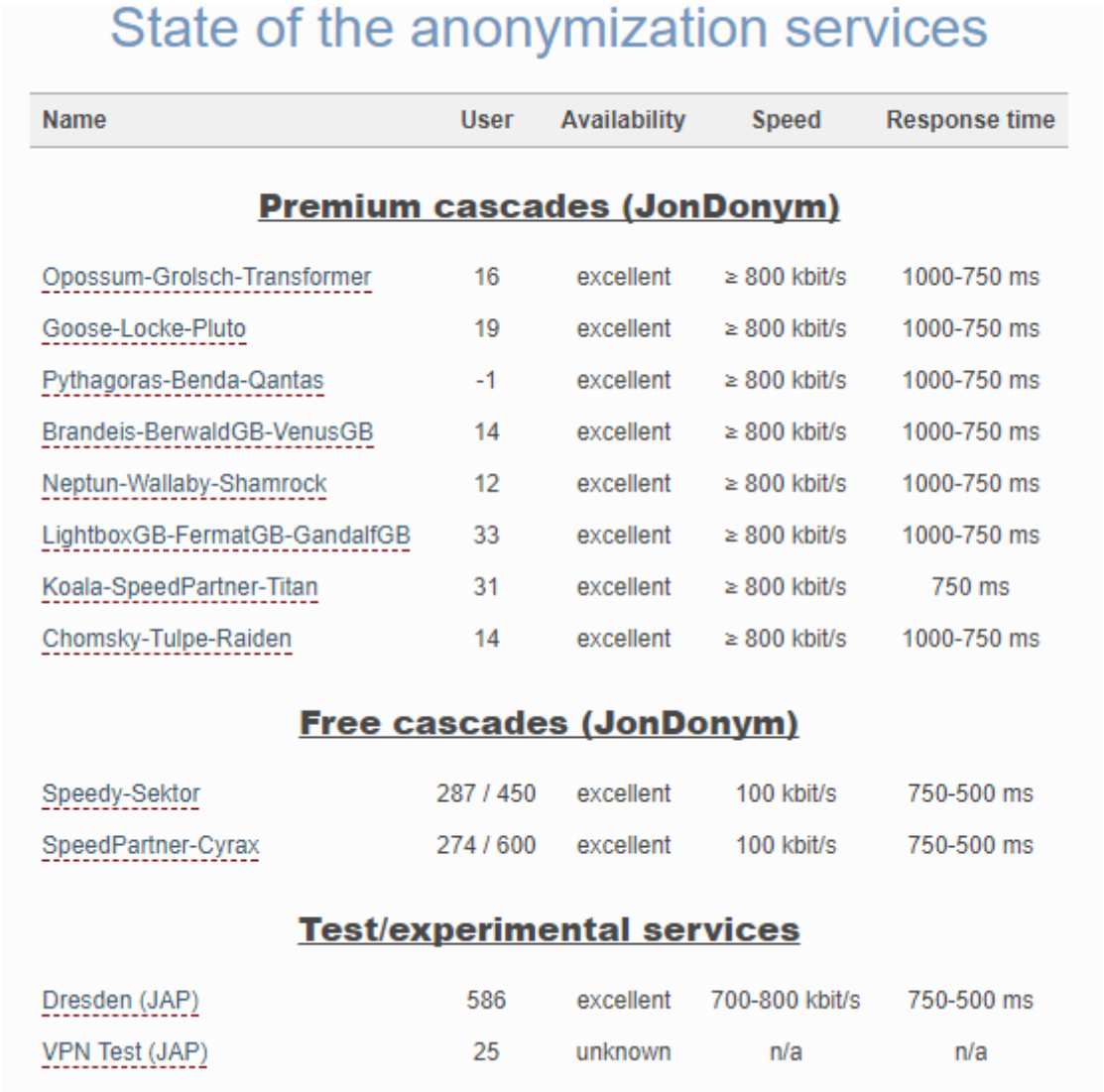
Attribute	Value	Rating
JavaScript	JavaScript is activated! (Version: 1.5)	medium
Tab name	"window.name" is traceable. Your unique ID: 2834232	medium
Tab history	There are 6 pages in your tab history.	medium
Local storage	Local storage is enabled. Your unique ID: 12834232	medium
Screen	1920 x 971 pixels 24 bit color depth	medium
Screen (usable)	matches screen resolution	good
Browser window	matches screen resolution	good
Browser bars	MenuBar PersonalBar StatusBar ToolBar ScrollBars LocationBar	good
WebGL	disabled or not supported by your browser.	good
Browser type	Mozilla/5.0 (Windows) 20100101 Netscape (en-US)	good
System	Windows NT 6.1 Win32 (Sun Feb 04 2018 15:54:34 GMT+0000 (UTC))	medium
Fonts	37 installed fonts have been found on your computer.	medium

Obrázek 8 Ip-check anonymity test TorBrowser

Z výsledků můžeme na první pohled vidět, že výsledek je podstatně lepší než u předchozích prohlížečů. Ip adresa byla úspěšně skryta. Ipcheck dokázal identifikovat fakt, že na web přistupujeme s použitím tor browseru. Na rozdíl od předchozích prohlížečů je například nastaven limit pro trvání http relace. Prohlížeč hlásí svůj preferovaný jazyk jako angličtinu, což ho řadí do největšího množství ostatních prohlížečů. Překvapit může například aktivovaný Javaskript, který je v základním nastavení aktivovaný i přes bezpečnostní riziko proto, aby příliš neomezoval funkčnost vzhledem k tomu, že mnoho webových stránek vyžaduje pro své fungování javaskript. Nezapnutí javaskriptu by mohlo být problémem pro technicky nezdatné uživatele, kteří by chtěli tor využít například k obcházení cenzury nebo z podobných důvodů (24). Je zde také vidět že prohlížeč byl zapnutý v režimu na celou obrazovku, což se nedoporučuje, protože je podle toho možné určit rozlišení uživatele a to opět umožňuje kategorizaci.

4.6 JonDoBrowser

JonDoBrowser je webový prohlížeč od společnosti JonDos GmbH. Na rozdíl od Toru nevyužívá modelu peer-to-peer a jeho koncové body jsou certifikované. Pracuje na principu kaskádových mixů. Daná skupina uživatelů ve stejné kaskádě posílá svá data přes stejné servery a jejich datová spojení se mixují (25). JonDoBrowser poskytuje několik volně dostupných kaskád a větší množství prémiových kaskád, které jsou dostupné pouze platícím uživatelům.



State of the anonymization services

Name	User	Availability	Speed	Response time
Premium cascades (JonDonym)				
Opossum-Grolsch-Transformer	16	excellent	≥ 800 kbit/s	1000-750 ms
Goose-Locke-Pluto	19	excellent	≥ 800 kbit/s	1000-750 ms
Pythagoras-Benda-Qantas	-1	excellent	≥ 800 kbit/s	1000-750 ms
Brandeis-BerwaldGB-VenusGB	14	excellent	≥ 800 kbit/s	1000-750 ms
Neptun-Wallaby-Shamrock	12	excellent	≥ 800 kbit/s	1000-750 ms
LightboxGB-FermatGB-GandalfGB	33	excellent	≥ 800 kbit/s	1000-750 ms
Koala-SpeedPartner-Titan	31	excellent	≥ 800 kbit/s	750 ms
Chomsky-Tulpe-Raiden	14	excellent	≥ 800 kbit/s	1000-750 ms
Free cascades (JonDonym)				
Speedy-Sektor	287 / 450	excellent	100 kbit/s	750-500 ms
SpeedPartner-Cyrax	274 / 600	excellent	100 kbit/s	750-500 ms
Test/experimental services				
Dresden (JAP)	586	excellent	700-800 kbit/s	750-500 ms
VPN Test (JAP)	25	unknown	n/a	n/a

Obrázek 9 Dostupné kaskády JonDo

Pro testování byla použita volně dostupná verze JonDoBrowseru.

Your IP	164.132.26.13 (JonDonym)	Traceroute
Your location	France	Show on map
Your net provider	á	Whois IP
Reverse DNS	sektor.jd.gurutek.biz	Whois Domain

Learn more about the individual tests performed by the IP Check... Click here!

Attribute	Value	Rating
Cookies	This web site may receive cookies from you	medium
HTTP session	unlimited	medium
Signature	8ab3a24c55ad99f4e3a6e5c03cad9446 (Firefox)	good
User-Agent	Mozilla/5.0 (Windows NT 6.1; rv:52.0) Gecko/20100101 Firefox/52.0	good
SSL_session_id	E24308E6304505DC3F5DF5DBB0FA31185F976F344BB60723E0769ED619099CE2	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
Upgrade-Insecure-Requests	1	good

Attribute	Value	Rating
JavaScript	JavaScript is activated! (Version: 1.5)	medium
Tab name	"window.name" is traceable. Your unique ID: 1899174	medium
Tab history	There are 7 pages in your tab history.	medium
Local storage	Local storage is enabled. Your unique ID: 11899174	medium
Screen	1920 x 907 pixels 24 bit color depth	medium
Screen (usable)	matches screen resolution	good
Browser window	matches screen resolution	good
Browser bars	MenuBar PersonalBar StatusBar ToolBar ScrollBars LocationBar	good
WebGL	disabled or not supported by your browser.	good
Browser type	Mozilla/5.0 (Windows) 20100101 Netscape (en-US)	good
System	Windows NT 6.1 Win32 (Sun Feb 04 2018 16:03:09 GMT+0000 (UTC))	medium
Fonts	37 installed fonts have been found on your computer.	medium

Obrázek 10 Ip-check anonymity test JonDoBrowser

Výsledek JonDoBrowseru je téměř totožný s výsledkem Tor browseru s jediným rozdílem v délce http relace, která se ovšem při opakovaných testech liší. V některých případech se hlásí jako neomezená a v jiných jako stateless. Ačkoliv se JonDo významně neliší ve výsledcích od Tor browseru, tak jeho přenosová rychlost byla nižší a měl problémy s navázáním spojení, které trvalo delší dobu.

4.7 Vyhodnocení

Každý způsob uchovávání anonymity s sebou přináší určité nevýhody. Každý určitým způsobem omezuje uživatelovo pohodlí a funkčnost při surfování na internetu. A tedy velmi záleží na úmyslu uživatele.

Pro běžného uživatele za nejvhodnější řešení pro zachování anonymity při běžném používání považuji Epic Privacy Browser. Nabízí dobrý poměr bezpečnosti vůči omezení uživatelnosti. Obsahuje také různé bezpečnostní prvky, které by v běžném prohlížeči bylo nutné doinstalovat zvlášť s využitím doplňků třetích stran. Jeho funkce proxy se ukázala být schopná zabránit odhalení Javascriptem a zároveň měla přijatelnou přenosovou rychlost. Ovládání prohlížeče je poměrně intuitivní a běžný uživatel v něm na první pohled neuvidí přílišný rozdíl od běžného webového prohlížeče, se kterým již má zkušenosti. Za jeho slabinu lze pro některé uživatele považovat právě neukládání některých lokálních dat jako je například historie prohlížení. Ovšem toto nepovažuji za příliš zásadní problém.

Pro případy, při nichž zabezpečení Epic Web Browseru není dostačující, navrhuji použití Tor Browseru, který ač se svou úrovní anonymizace téměř shoduje s JonDoBrowserem, osvědčil se jako uživatelsky přijatelnější a jeho funkčnost byla při testování lepší. JonDo se na volně dostupných kaskádách prokázal jako pomalejší.

Pro potřebu jednorázového skrytí identity, jako například pro přístup na web, který je regionálně omezený, postačí i web proxy. Ovšem jeho jedinou předností se ukázala jednoduchost jeho zprovoznění. Ve většině případů doporučuji se web proxy vyhýbat a raději využít některý z komplexnějších nástrojů pro anonymizaci.

5 Závěr

Hlavním cílem práce bylo charakterizovat typy digitálních stop a představit metody ochrany osobních dat. Dílčím cílem bylo srovnat možnosti nástrojů k ochraně osobních dat. V práci byly charakterizovány jak lokálně uložené stopy, tak stopy ukládané na internetu. Mezi lokálními stopami byly představené cookies a další lokální stopy. Byly také představeny způsoby využití a zneužití digitálních stop. Dále byly charakterizovány způsoby a nástroje ochrany osobních dat uživatele, od způsobů nastavení prohlížeče po specializovanější nástroje ke skrývání digitální stopy.

Byla srovnána schopnost webových prohlížečů skrývat digitální stopu. Toto porovnání bylo provedeno pomocí webu ip-check.info provozovaného německou společností JonDos GmbH. Z testů nejhůře vyšly běžné webové prohlížeče, jejichž zástupcem byl zvolen Google Chrome. Dále byl testován Google Chrome s použitím webového proxy, který se také ukázal jako nedostatečný pro skrytí uživatelovy ip adresy. Při použití VPN s Google Chrome se podařilo ip adresu skrýt, ovšem stále nezakrýval všechny možnosti identifikace. Jako další byl testován Epic privacy browser, který se svou aktivovanou funkcí proxy dokázal skrýt ip adresu a jeho ostatní nastavení, ač neideální, bylo lepší než v předchozích testech. Díky jeho uživatelské přívětivosti a poměrně vysoké přenosové rychlosti při použití zabudovaného proxy, byl doporučen jako vhodné řešení pro běžné užívání.

V dalším testu byl testován Tor browser. Ten se svým zabezpečením ukázal jako nejsilnější, ovšem za cenu silného zpomalení přenosové rychlosti. Jako poslední byl testován JonDoBrowser, který byl svým zabezpečením porovnatelný s Tor browserem. Měl však ve své volně dostupné verzi špatnou funkčnost a přenosovou rychlost. Z tohoto důvodu byl pro situace, ve kterých je potřeba silnější zabezpečení, zvolen Tor browser.

6 Seznam použitých zdrojů

1. PORADA, V. , RAK, R. Teorie digitálních stop a její aplikace v kriminalistice a forenzních vědách. Karlovarská právní revue 4/2006. ISSN 1801-2191.
2. cookies. Adaptic [online]. Praha: adaptic, c2005-2017 [cit. 2017-06-25]. Dostupné z: http://www.adaptic.cz/znalosti/slovnicek/cookies/
3. Flash prý skrývá nebezpečí, říká se mu Flash Cookies. Živě.cz [online]. Jakub Čížek, 2010 [cit. 2017-11-02]. Dostupné z: https://www.zive.cz/clanky/flash-pry-skryva-nebezpeci-rika-se-mu-flash-cookies/sc-3-a-153412/default.aspx
4. How Advertisers Use Web Beacons to Track You on the Web and in Emails. Www.makeuseof.com [online]. 2016 [cit. 2017-10-10]. Dostupné z: http://www.makeuseof.com/tag/how-web-beacons-track-web/
5. More than half of employers now use social media to screen job candidates, poll says; even send friend requests. Cleaveland.com [online]. 2015 [cit. 2017-11-02]. Dostupné z: http://www.cleveland.com/business/index.ssf/2015/05/more_than_half_of_employers_no_1.html
6. BRECHLEROVÁ, Dagmar. Digitální stopy a jejich odstraňování. Computer World 06/2016. 2016.
7. Reklamy Google|Jak Google využívá vaše data k výběru reklam. Google.com [online]. [cit. 2017-11-02]. Dostupné z: https://privacy.google.com/intl/cs/how-ads-work.html?utm_source=google&utm_medium=ad-settings&utm_campaign=inbound-site-link
8. Behavioral Ads Offer A Windfall For Marketers, Publishers. Forbes [online]. [cit. 2017-11-02]. Dostupné z: https://www.forbes.com/2010/03/24/behavioral-targeted-ads-advertising-ftc-privacy-cmo-network-ads.html
9. Digitální forenzika jako součást vaší kybernetické obrany. Control Engineering [online]. 2014 [cit. 2017-06-25]. Dostupné z: http://www.controlengcesko.com/hlavni-menu/artykuly/artykul/article/digitalni-forenzika-jako-soucast-vasi-kyberneticke-obrany/
10. Digital Forensics for Legal Professionals Understanding Digital Evidence From The Warrant To The Courtroom. Burlington: Elsevier Science, 2011. ISBN 9781597496445.
11. Cyberstalking. EPRAVO.cz [online]. Mgr. Ivana Jarošová, 2013 [cit. 2017-11-02]. Dostupné z: https://www.epravo.cz/top/clanky/cyberstalking-91552.html

12. Mladá právnička radí, jak čelit kyberstalkingu. Online.muni.cz [online]. Jana Řeháková, 2015 [cit. 2017-11-02]. Dostupné z: https://www.online.muni.cz/udalosti/6028-mlada-pravnicka-radi-jak-celit-kyberstalkingu
13. 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.
14. Cyberbullying and bullying are not the same. Science Daily [online]. University of British Columbia, 2015 [cit. 2017-11-02]. Dostupné z: https://www.sciencedaily.com/releases/2012/04/120413122202.htm
15. Krádež identity a jak se jí bránit. Bezpecnyinternet.cz [online]. [cit. 2017-11-02]. Dostupné z: http://www.bezpecnyinternet.cz/pokrocily/ochrana-prav/kradez-identity.aspx
16. Co je to phishing. Hoax.cz [online]. [cit. 2017-11-02]. Dostupné z: http://www.hoax.cz/phishing/co-je-to-phishing
17. Phishing. Bezpečný internet [online]. [cit. 2017-11-02]. Dostupné z: http://www.bezpecnyinternet.cz/zacatecnik/e-mail/phishing.aspx
18. Rhybaření střídá pharming. Lupa [online]. Ondřej Bitto, 2005 [cit. 2017-11-02]. Dostupné z: https://www.lupa.cz/clanky/rhybareni-strida-pharming/
19. Opt Out. Oracle [online]. [cit. 2017-11-02]. Dostupné z: http://bluekai.com/consumers.php#optout
20. What is a VPN? Whatismyip.com [online]. [cit. 2017-11-02]. Dostupné z: https://www.whatismyip.com/what-is-a-vpn/
21. VPN pro začátečníky: princip fungování, výhody a nevýhody. Root.cz [online]. Roman Bořánek, 2017 [cit. 2017-11-02]. Dostupné z: https://www.root.cz/clanky/vpn-pro-zacatecniky-princip-fungovani-vyhody-a-nevyhody/
22. What is a web proxy. Whatismyip.com [online]. Brian Gilbert [cit. 2017-11-02]. Dostupné z: https://www.whatismyip.com/what-is-a-web-proxy/
23. Tor project: Overview. Tor [online]. [cit. 2017-11-02]. Dostupné z: https://www.torproject.org/about/overview.html.en
24. Tor Project: FAQ. Torproject [online]. [cit. 2018-01-31]. Dostupné z: https://www.torproject.org/docs/faq.html.en#TBBJavaScriptEnabled
25. SCHREIBER, Manuel. Anonymně na webu. Chip.cz[online]. 2009 [cit. 2018-02-03]. Dostupné z: https://www.chip.cz/casopis-chip/earchiv/rubriky/testy-a-technika/anonym-na-webu/