# Ochrana dat na mobilních a dalších zařízeních

## proti krádeži a zneužití

Šárka Vavrečková

Ústav informatiky, FPF SU Opava

sarka.vavreckova@fpf.slu.cz

Poslední aktualizace: 30. října 2014

# Ukradli mi notebook/tablet/mobil.

## Co z toho plyne?

- Nemám notebook/tablet/mobil. Potřebuji nové zařízení ⇒ finanční náklady.
- Mám tam vlastní cenné údaje (certifikáty, přístupová hesla, fotografie, videa, domácí úkoly dítěte, atd.). Přijdu o ně, navíc mohou být zneužity.
- Mám tam firemní data (přístupové údaje, adresy, údaje o vyráběných produktech, návrhy, patenty, údaje z firemního účetnictví, firemní tajemství, atd.) – zneužitelné, podobné údaje mají na černém trhu velkou cenu.
- Zloděj se dotýká něčeho mého!

# Ukradli mi notebook/tablet/mobil.

## Co s tím?

1. Nepodléhat panice. Nahlásit na policii. Nahlaste takovou hodnotu ukradené věci, která je odpovídající, tj. nejen hodnotu hardwaru, ale i hodnotu ukradených dat s ohledem na cenu při jejich zneužití.
   Zároveň:
2. Využít možnosti vyhledání mobilního zařízení.
3. Když už vím, že to nepůjde, zajistit smazání všeho, co by mohlo být zneužito.

# Preventivní opatření

- Instalace softwaru, který pomůže s dohledáním zcizeného zařízení.
- Instalace softwaru, který dokáže na dálku smazat data, příp. systém.
- Pravidelně zálohovat.
- Dávat pozor na své věci, nenechávat nic viditelně v autě, netahat „drahá“ firemní data domů.

# Notebooky – základní ochrana

- zámek Kensington: možnost přichytit notebook ke stolu (funguje jen v součinnosti se stolem či jiným podobným kusem nábytku)
- zaheslovaný bios: dá se obejít
- uživatelské heslo do systému: dá se obejít, zvláště ve Windows
- čtečka otisků prstů: postupně se zanáší, nutno čistit, pokud to umíme, navíc může stávkovat
- další biometrické metody (snímání oka, hlasu apod.): drahé, taky může stávkovat

# Řešení pro vzdálenou lokalizaci a ovládání

- nutno mít předem nainstalováno a aktivováno
- schopnosti různé podle toho, jak „hluboko“ je řešení integrováno
- buď se zařízení pravidelně hlásí (když se nehlásí, je zřejmě ukradeno), nebo aktivace mechanismu na dálku, přenos videa
- zjištění polohy a její zaslání (pokud je to možné), možnost zkartování dat

# Řešení pro vzdálenou lokalizaci a ovládání

## Možnosti lokalizace

- GPS čip (pokud v zařízení je)
- mobilní sítě
- Wi-fi Access Pointy

Přenos lokalizačních informací přes síť vhodným protokolem, posláním SMS, e-mailu apod.

# Intel Anti-Theft

- hardwarové zabezpečení v kombinaci s příslušným softwarem
- mobilní procesory Intel Core od roku 2010 (od druhé generace), včetně slabších Core i3 (ale ne Pentium, Atom ani Celeron), i některé desktopové
- pokud zjistíme, že se notebook ztratil či byl odcizen, můžeme na dálku zablokovat zařízení, po navrácení je možné odblokovat
- možnosti zajištění zablokování: přes internet, telefonem, pomocí speciálních hardwarových časovačů
- taky je možné data smazat, ale už nejdou obnovit

# Intel Anti-Theft

- určení polohy: přes webový portál, lokalizace pomocí GPS, nejbližších AP nebo něčeho jiného (co je k dispozici)
- funguje i v případě: odpojení od sítě, bootování z jiného média (obecně multi-boot), přeinstalování, výměny disku

# Intel Anti-Theft

## Jak to funguje

- Intel poskytuje pouze hardwarovou podporu v procesorech
- technologii (vč. softwaru) zprovozní až některý z poskytovatelů (jeden z nich je např. McAfee)
- operační systém – pouze Windows 7 nebo 8
- předplacená služba, existují zkušební verze
- jak na to:
  - registrace u poskytovatele služby
  - instalace aktivujícího softwaru, postupujeme dle průvodce
  - konfigurace ve webovém rozhraní

Cena cca 500–1000 Kč za rok, podle poskytovatele služby

# Intel Anti-Theft

## Zdroje

- http://www.svetsiti.cz/clanek.asp?cid=Technologie-Intel-Anti-Theft-30-proti-ztrate-cennych-dat-pri-odcizeni-firemniho-notebooku-932011
- http://notebook.cz/clanky/prislusenstvi/2013/intel-anti-theft
- http://www.cnews.cz/clanky/intel-anti-theft-technology-30-neprustrelna-ochrana-vasich-dat
- http://www.youtube.com/watch?v=rH6YJzt82wI
- http://www.intel.com/content/www/us/en/architecture-and-technology/anti-theft/anti-theft-general-technology.html

# CompuTrace

- není na úrovni HW, ale na úrovni BIOSu, provozuje firma Absolute, poskytují výrobci zařízení
- běží jako skrytá (nezobrazovaná) služba Computrace Agent v systémovém procesu, není běžným způsobem odhalitelná
- musíme mít podporovaný notebook (většina výrobců takové stroje nabízí)
- Computrace Agent v pravidelných intervalech posílá přes síť IP adresu a další informace (podle nastavení), příp. přijímá instrukce ke smazání dat či systému
- Windows včetně starších verzí
- funguje i v případě: odpojení od sítě, bootování z jiného média (obecně multi-boot), přeinstalování, výměny disku

# CompuTrace

## Zdroje

- http://notebook.cz/clanky/technologie/2008/Computrace
- http://www.absolute.com/en/products/absolute-computrace
- http://www.dell.com/learn/us/en/555/vsl-absolute

# Prey

- řešení pro notebooky, tablety, smartphony
- open-source software, volně dostupný (většina kódu pro klienta)
- na serveru máme zřízen účet (ve verzi zdarma až pro 3 zařízení)
- na zařízení instalujeme agenta, který očekává instrukce (síť nebo SMS)
- po obdržení instrukcí agent shromáždí veškeré dostupné informace (vč. snímků), které mohou pomoci najít zařízení, odešle na účet na server

# Prey

- lokalizace: GPS nebo Wi-fi AP
- umí
  - skrýt data a aplikace,
  - případně odstranit hesla,
  - uzamknout zařízení,
  - detekce změny SIM karty,
  - hlasitý alarm, ochrana před odinstalací,
  - vydávat se za neškodnou hru

# Prey

## Zdroje

- http://preyproject.com/
- http://www.svetandroida.cz/prey-najdete-svuj-ztraceny-ci-odcizeny-telefon-201306
- http://mac.appstorm.net/reviews/security/prey-a-powerful-recovery-tool-for-your-missing-laptop/

# Další řešení pro mobilní zařízení

- pro Android: IOBit, Cerberus a další
- produkty antivirových firem, často součásti bezpečnostních balíků (Norton, Eset, avast!, Lookout, AVG, Zoner, atd.)
- výsledky bezpečnostních funkcí můžeme srovnat na http://www.av-test.org/en/

# Další

## Zdroje

- https://play.google.com/store/apps/details?id=com.lsdroid.cerberus&hl=cs
- Jak přidat ochranu proti odcizení telefonu do ROM? [online] *Android Fórum*, 2011. Dostupné na: http://androidforum.cz/jak-p-idat-ochranu-proti-odcizeni-telefonu-do-rom-t21135.html

# Jak postupovat

- hlavně rychle – čím dřív reagujeme, tím líp
- získat co nejvíc informací a předat Policii ČR
- v žádném případě nezveřejňovat snímky či videa zloděje, důsledkem by mohla být žaloba na ochranu osobnosti (zákon bohužel nechrání jen nevinné, ale všechny :-))

# Ukládání informací o uživateli

## Cookies

- server webové stránky ukládá na našem počítači informace, které
  - nás mohou identifikovat
  - obsahují položky nákupního košíku
  - přihlašovací údaje a další informace
- vedlejší účel: lze zjistit, na jakých stránkách se pohybujeme, kolik času tam trávíme, co nás zajímá
- teoreticky by web měl mít přístup jen k „vlastním“ cookies
- doba platnosti: může být i desítky let

# Typy cookies

## Klasické HTML cookies

- malé textové soubory nebo malá SQLite databáze, nejméně nebezpečné
- max. 4 KB, se stanoveným časovým omezením, závislé na webovém prohlížeči
- obvykle v profilu uživatele ve složce `AppData`
- účely: identifikuje uživatele při přístupu na web, přihlašovací údaje (session cookie), nákupní košíky, další data pro webové stránky
- pokud celá webová aplikace nekomunikuje přes SSL, odesílají se nezašifrovaná data
- posílá se při každém HTTP požadavku na server

# Typy cookies

## HTML5 cookies

- určeno pro interaktivní aplikace vyžadující ukládání většího množství dat lokálně, aby nebylo nutné často přenášet velké objemy dat
- taky se nazývá Local Storage nebo DOM Storage
- SQLite databáze, přístupné přes JavaScript
- 5 MB nebo 10 MB

# Typy cookies

## Flash cookies

- binární soubory
- max. 100 KB (ale může požádat uživatele o rozšíření prostoru), bez limitu platnosti, bez závislosti na webovém prohlížeči, je mnohem těžší je smazat
- soubory s příponou .SOL v lokální složce Flash Playeru
- původně pro informace k videím a hrám, dnes i pro sledování uživatele, dokážou sledovat a případně obnovit HTTP cookies

# Typy cookies

## Supercookies

- kombinace HTML, HTML5 a Flash cookies
- pokud některé smažeme, bude obnoveno pomocí ostatních částí

## Evercookie

- demonstrační „multicookie“, vytvořeno, aby ukazovalo, kam všude je možné data zastrčit (samy.pl/evercookie)
- uloženo na 13 různých místech v systému

# Získávání dat pro reklamní společnosti

## Adelphic

- analýza vzoru chování uživatelů mobilních telefonů
- zjišťuje, jak uživatel reagoval na předchozí reklamní nabídky

## Drawbridge

- statistická analýza anonymních údajů, také z cookies
- dává dohromady různá zařízení, která pravděpodobně patří témuž uživateli
- užitečné pro cílení reklam

a další firmy

# Získávání dat pro reklamní společnosti

## Kombinace on-line a off-line dat

- on-line data: viz dříve (cookies apod.)
- off-line data: databáze nejrůznějších firem včetně zásilkových, webových obchodů, mobilních operátorů, atd.

# Webkamery

## K čemu jsou „netradičně“ využívány:

- legální zabezpečení místnosti
- Prey – šedá zóna, stopování vlastního zařízení
- v USA půjčovna notebooků tajně sledovala své klienty
- USA: počítač na splátky – software DesignerWare (lokalizace a blokování počítačů, které nebyly spláceny), zneužíváno zaměstnanci
- ransomware – když je na vyděračském oznámení snímek uživatele, působí to důvěryhodněji
- další možnosti

webkamerou může být vybavena i „chytrá“ televize

# Zneužití webkamery

## Obrana

- ve skutečnosti může natáčet, i když nesvítí kontrolka
- pokud je to možné: zakrýt, otočit, vysunout USB konektor
- vypnutí pomocí klávesové zkratky nemusí vést k cíli
- SpyBot Search & Destroy: dokáže odhalit malware přistupující k webkameře

Podobně může být zneužit i mikrofon a různé senzory zařízení.

# Zneužití webkamery

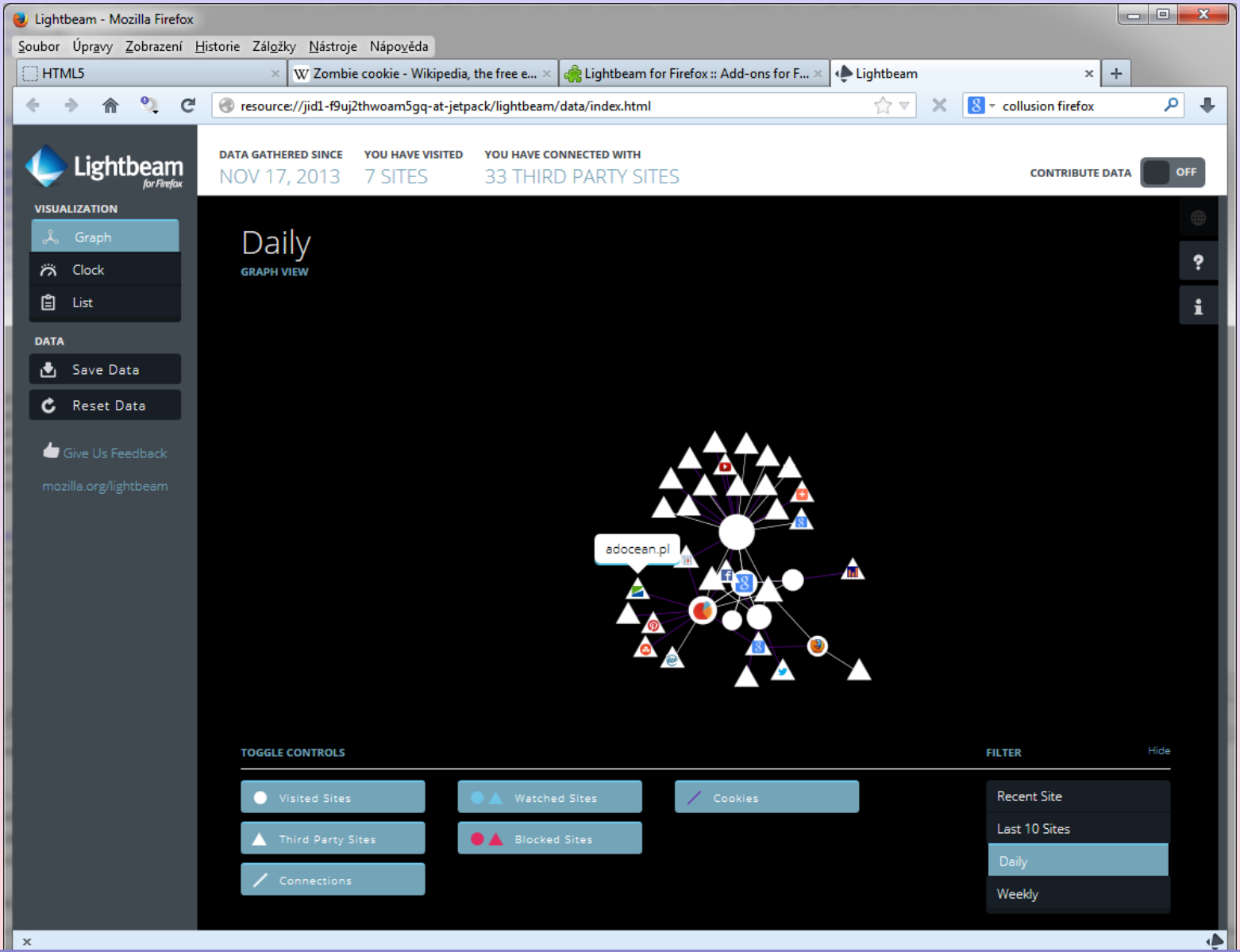
## Place Raider

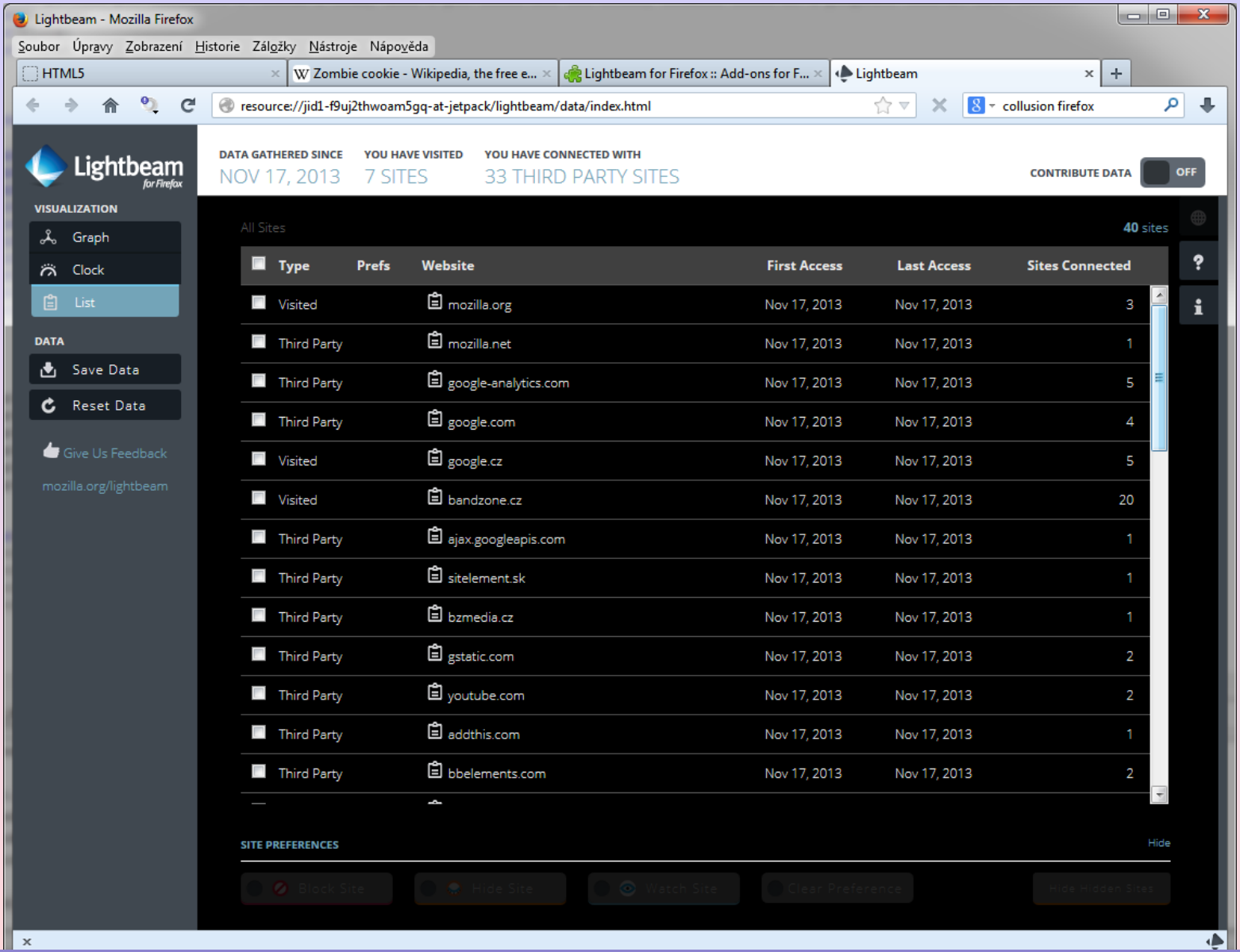
- trojský kůň pro smartphony, který pravidelně vytváří fotografie a ukládá na serveru
- z balíku fotografií lze poskládat 3D panoramatický zoomovatelný model bytu
- zatím ve fázi proof-of-concept
- ochrana: vhodné nastavení ovládání webkamery/fotoaparátu, zvukový signál při aktivaci záznamu

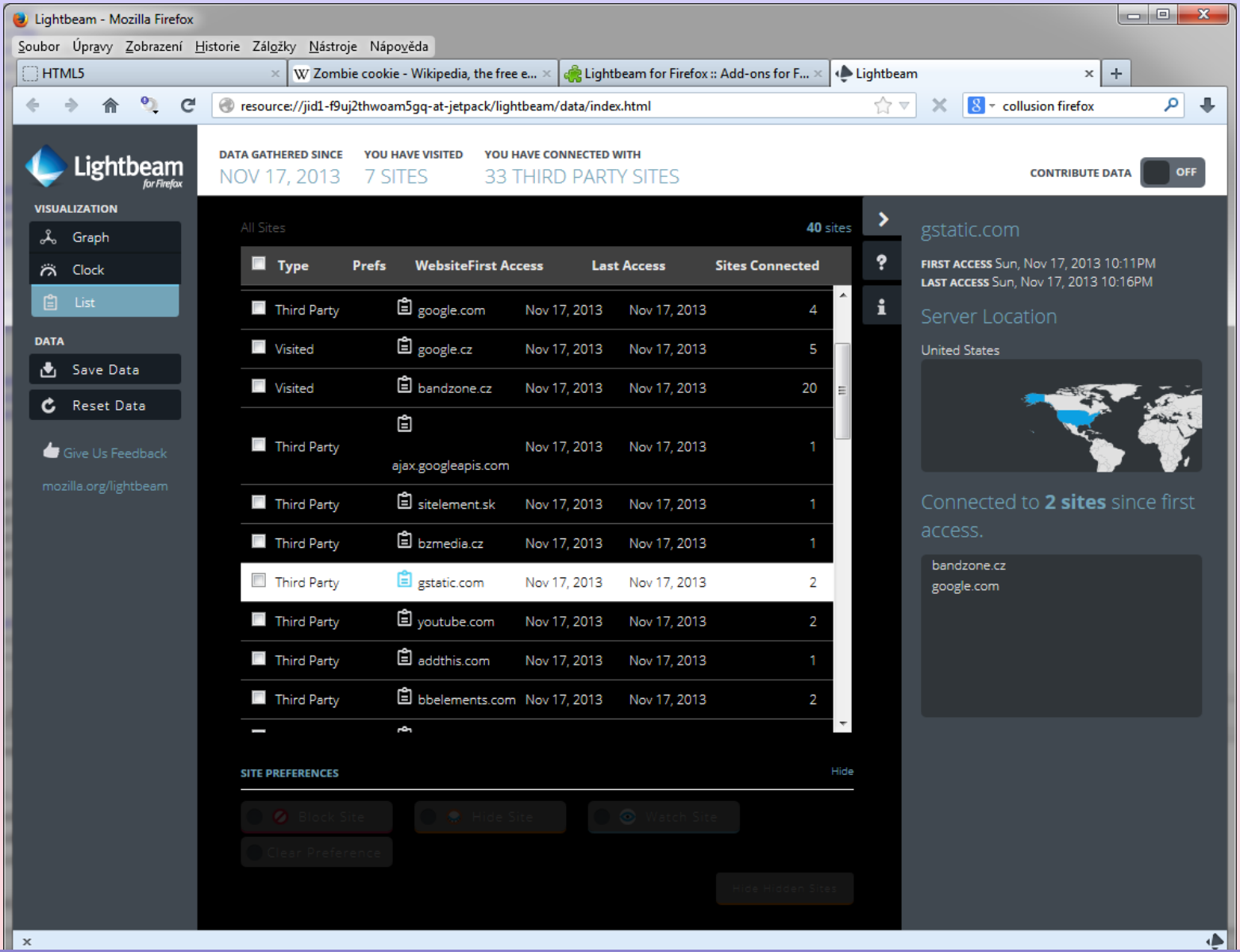
# Jak vizualizovat cookies

## Lightbeam

- dříve Collusion
- doplněk do webového prohlížeče, dostupný přes ikonu v pravém dolním rohu
- po klepnutí na ikonu se zobrazí seznam cookies (ale až od aktivace doplňku) – volíme způsob zobrazení


Lightbeam - Mozilla Firefox
Soubor Úpravy Zobrazení Historie Záložky Nástroje Nápověda
HTML5
Zombie cookie - Wikipedia, the free e...
Lightbeam for Firefox :: Add-ons for F...
Lightbeam
resource://jid1-f9uj2thwoam5gq-at-jetpack/lightbeam/data/index.html
collusion firefox
Lightbeam for Firefox
DATA GATHERED SINCE
NOV 17, 2013
YOU HAVE VISITED
7 SITES
YOU HAVE CONNECTED WITH
33 THIRD PARTY SITES
CONTRIBUTE DATA
OFF
VISUALIZATION
Graph
Clock
List
DATA
Save Data
Reset Data
Give Us Feedback
mozilla.org/lightbeam
Daily
GRAPH VIEW
adocean.pl
TOGGLE CONTROLS
Visited Sites
Watched Sites
Cookies
Third Party Sites
Blocked Sites
Connections
FILTER
Hide
Recent Site
Last 10 Sites
Daily
Weekly


Lightbeam - Mozilla Firefox
Soubor Úpravy Zobrazení Historie Záložky Nástroje Nápověda
HTML5
Zombie cookie - Wikipedia, the free e...
Lightbeam for Firefox :: Add-ons for F...
Lightbeam
resource://jid1-f9uj2thwoam5gq-at-jetpack/lightbeam/data/index.html
collusion firefox
Lightbeam for Firefox
VISUALIZATION
Graph
Clock
List
DATA
Save Data
Reset Data
Give Us Feedback
mozilla.org/lightbeam
DATA GATHERED SINCE
NOV 17, 2013
YOU HAVE VISITED
7 SITES
YOU HAVE CONNECTED WITH
33 THIRD PARTY SITES
CONTRIBUTE DATA
OFF
All Sites
40 sites
Type Prefs Website First Access Last Access Sites Connected
Visited mozilla.org Nov 17, 2013 Nov 17, 2013 3
Third Party mozilla.net Nov 17, 2013 Nov 17, 2013 1
Third Party google-analytics.com Nov 17, 2013 Nov 17, 2013 5
Third Party google.com Nov 17, 2013 Nov 17, 2013 4
Visited google.cz Nov 17, 2013 Nov 17, 2013 5
Visited bandzone.cz Nov 17, 2013 Nov 17, 2013 20
Third Party ajax.googleapis.com Nov 17, 2013 Nov 17, 2013 1
Third Party sitelement.sk Nov 17, 2013 Nov 17, 2013 1
Third Party bzmedia.cz Nov 17, 2013 Nov 17, 2013 1
Third Party gstatic.com Nov 17, 2013 Nov 17, 2013 2
Third Party youtube.com Nov 17, 2013 Nov 17, 2013 2
Third Party addthis.com Nov 17, 2013 Nov 17, 2013 1
Third Party bbelements.com Nov 17, 2013 Nov 17, 2013 2
SITE PREFERENCES
Hide
Block Site
Hide Site
Watch Site
Clear Preference
Hide Hidden Sites


Lightbeam - Mozilla Firefox
Soubor Úpravy Zobrazení Historie Záložky Nástroje Nápověda
HTML5
Zombie cookie - Wikipedia, the free e...
Lightbeam for Firefox :: Add-ons for F...
Lightbeam
resource://jid1-f9uj2thwoam5gq-at-jetpack/lightbeam/data/index.html
collusion firefox
Lightbeam for Firefox
VISUALIZATION
Graph
Clock
List
DATA
Save Data
Reset Data
Give Us Feedback
mozilla.org/lightbeam
DATA GATHERED SINCE
NOV 17, 2013
YOU HAVE VISITED
7 SITES
YOU HAVE CONNECTED WITH
33 THIRD PARTY SITES
CONTRIBUTE DATA
OFF
All Sites
40 sites
Type Prefs WebsiteFirst Access Last Access Sites Connected
Third Party google.com Nov 17, 2013 Nov 17, 2013 4
Visited google.cz Nov 17, 2013 Nov 17, 2013 5
Visited bandzone.cz Nov 17, 2013 Nov 17, 2013 20
Third Party ajax.googleapis.com Nov 17, 2013 Nov 17, 2013 1
Third Party sitelement.sk Nov 17, 2013 Nov 17, 2013 1
Third Party bzmedia.cz Nov 17, 2013 Nov 17, 2013 1
Third Party gstatic.com Nov 17, 2013 Nov 17, 2013 2
Third Party youtube.com Nov 17, 2013 Nov 17, 2013 2
Third Party addthis.com Nov 17, 2013 Nov 17, 2013 1
Third Party bbelements.com Nov 17, 2013 Nov 17, 2013 2
SITE PREFERENCES
Hide
Block Site
Hide Site
Watch Site
Clear Preference
Hide Hidden Sites
gstatic.com
FIRST ACCESS Sun, Nov 17, 2013 10:11PM
LAST ACCESS Sun, Nov 17, 2013 10:16PM
Server Location
United States
Connected to 2 sites since first access.
bandzone.cz
google.com

# Jak odstranit cookies

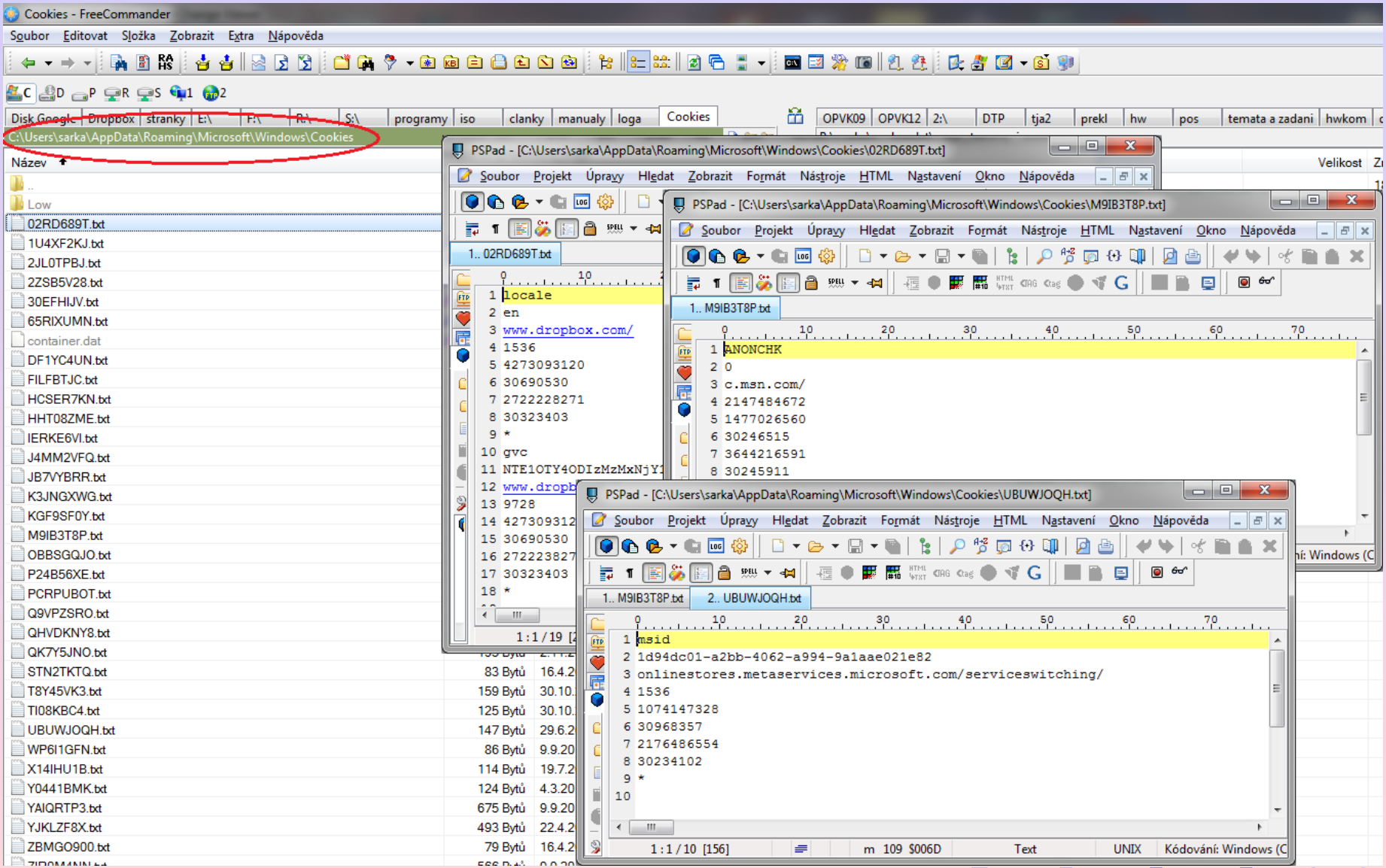
## HTML cookies

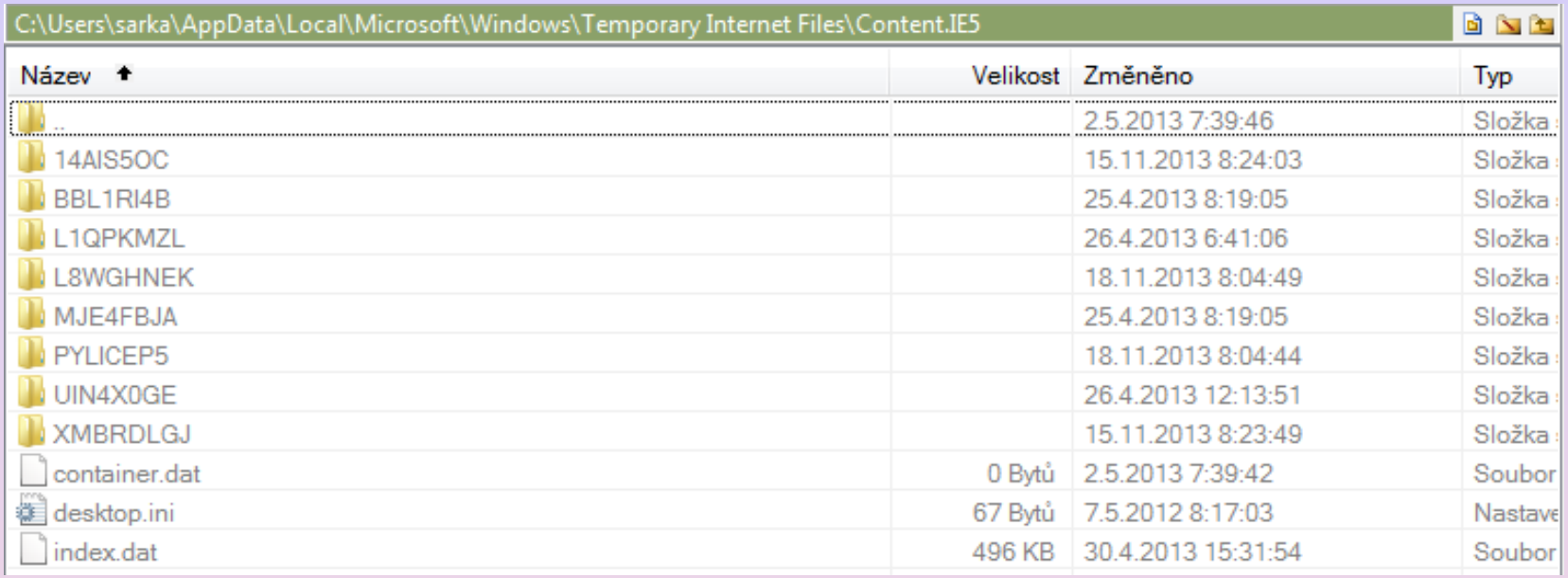
- IE: Nástroje, Odstranit historii procházení, Cookies, Odstranit
- Firefox: Nástroje, Vymazat nedávnou historii
- Chrome: Přizpůsobení a ovládání Google Chrome, Historie, Vymazat všechny údaje o prohlížení, Smazat soubory cookie.....

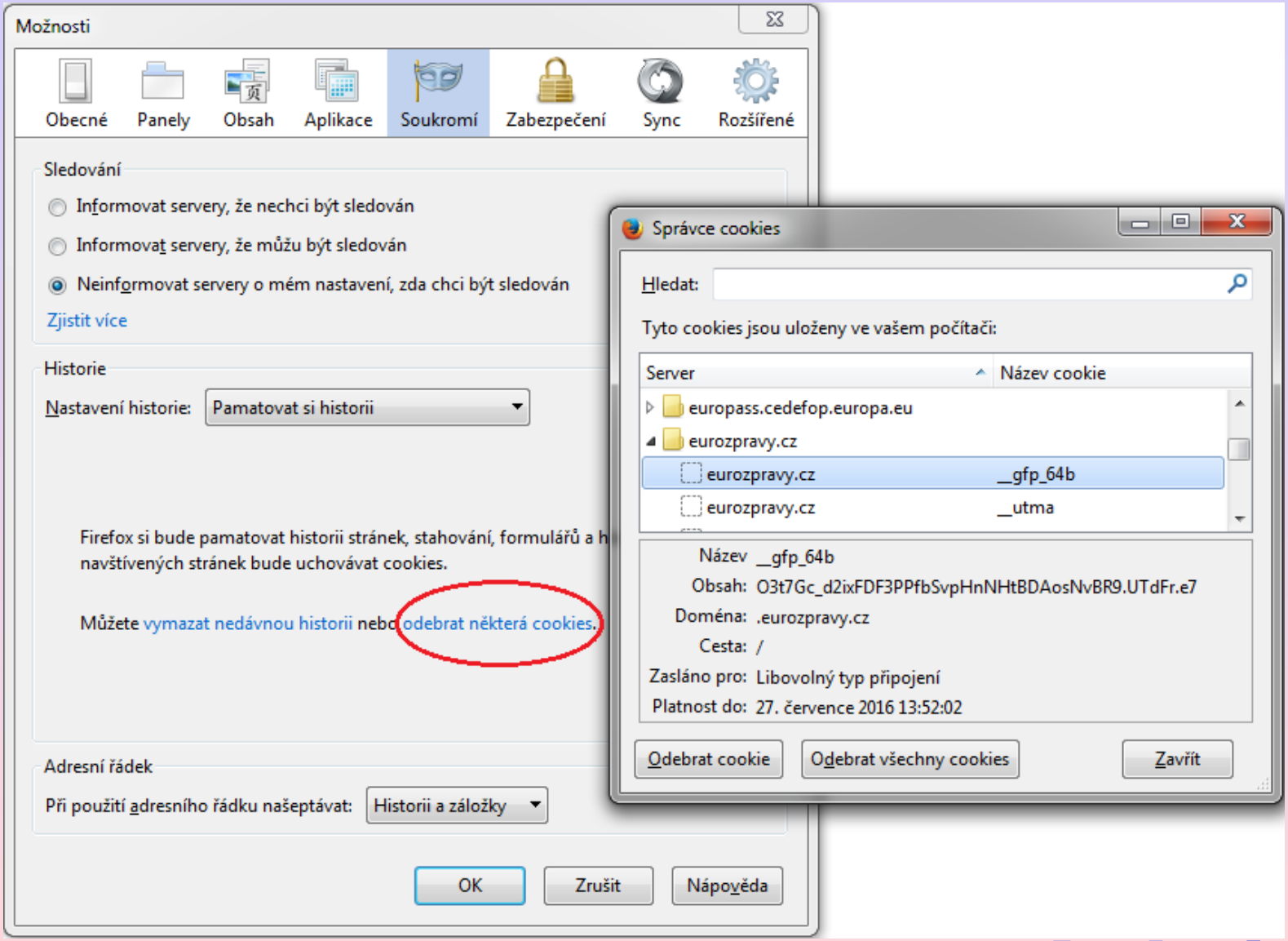
## Flash cookies

- Firefox: doplněk BetterPrivacy
- Chrome: doplněk Click & Clean

Taky odstraní supercookies.


Cookies - FreeCommander
C:\Users\sarka\AppData\Roaming\Microsoft\Windows\Cookies
PSPad - [C:\Users\sarka\AppData\Roaming\Microsoft\Windows\Cookies\02RD689T.txt]
PSPad - [C:\Users\sarka\AppData\Roaming\Microsoft\Windows\Cookies\M9IB3T8P.txt]
PSPad - [C:\Users\sarka\AppData\Roaming\Microsoft\Windows\Cookies\UBUWJOQH.txt]


C:\Users\sarka\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5
Název
Velikost
Změněno
Typ
..
2.5.2013 7:39:46
Složka
14AIS5OC
15.11.2013 8:24:03
Složka
BBL1RI4B
25.4.2013 8:19:05
Složka
L1QPKMZL
26.4.2013 6:41:06
Složka
L8WGHNEK
18.11.2013 8:04:49
Složka
MJE4FBJA
25.4.2013 8:19:05
Složka
PYLICEP5
18.11.2013 8:04:44
Složka
UIN4X0GE
26.4.2013 12:13:51
Složka
XMBRDLGJ
15.11.2013 8:23:49
Složka
container.dat
0 Bytů
2.5.2013 7:39:42
Soubor
desktop.ini
67 Bytů
7.5.2012 8:17:03
Nastave
index.dat
496 KB
30.4.2013 15:31:54
Soubor


Možnosti
Obecné
Panely
Obsah
Aplikace
Soukromí
Zabezpečení
Sync
Rozšířené
Sledování
Informovat servery, že nechci být sledován
Informovat servery, že můžu být sledován
Neinformovat servery o mém nastavení, zda chci být sledován
Zjistit více
Historie
Nastavení historie:
Pamatovat si historii
Firefox si bude pamatovat historii stránek, stahování, formulářů a h
navštívených stránek bude uchovávat cookies.
Můžete vymazat nedávnou historii nebo odebrat některá cookies.
Adresní řádek
Při použití adresního řádku našeptávat:
Historii a záložky
OK
Zrušit
Nápověda
Správce cookies
Hledat:
Tyto cookies jsou uloženy ve vašem počítači:
Server
Název cookie
europass.cedefop.europa.eu
eurozpravy.cz
eurozpravy.cz
__gfp_64b
eurozpravy.cz
__utma
Název __gfp_64b
Obsah: O3t7Gc_d2ixFDF3PPfbSvpHnNHtBDAosNvBR9.UTdFr.e7
Doména: .eurozpravy.cz
Cesta: /
Zasláno pro: Libovolný typ připojení
Platnost do: 27. července 2016 13:52:02
Odebrat cookie
Odebrat všechny cookies
Zavřít

# Další „zvědavá“ úložiště

## Vypnutí DOM Storage

- Firefox:
  - do adresního řádku zadáme about:config
  - parametr `dom.storage.enabled`
  - poklepeme, nastavíme na `False`

Webové stránky pak nebudou moci DOM storage používat.

- doplňky Adblock Plus, NoScript, Tracking protection list, atd.
- v mobilním zařízení je lepší mít vypnutou GPS lokaci, pokud ji zrovna nepotřebujeme
- CCleaner

## Zdroje


- http://www.zdrojak.cz/clanky/minulost-soucasnost-a-budoucnost-lokalniho-uloziste-pro-html5-aplikace/
- http://www.aspnet.cz/articles/344-local-storage-sbohem-cookies-sbohem-session
- http://www.root.cz/zpravicky/zombie-cookies-preziji-diky-html5/
- http://earchiv.chip.cz/cs/earchiv/vydani/r-2011/chip-05-2011/mazani-cookies.html
- http://www.ictmanazer.cz/2011/12/pripravte-se-na-hrozby-spojene-s-html5/
- http://en.wikipedia.org/wiki/Zombie_cookie
- https://addons.mozilla.org/en-US/firefox/addon/lightbeam/?src=search

# Možnosti anonymního surfování

## 1. Anonymní režimy v prohlížečích

Obvykle jde o skrytí některých identifikačních znaků, vypnutí zaznamenávání historie, cookies, stažených souborů.

- Firefox: Ctrl+Shift+P, ale lepší je použít specializované doplňky (Open in Private Browsing Mode, také NoScript a BetterPrivacy)
- Chrome: Ctrl+Shift+N
- IE (služba InPrivate): Ctrl+Shift+P

Přímo v prohlížečích je na tom asi nejlépe IE, ale Firefox má zase pro tento účel kvalitní doplňky.

# Možnosti anonymního surfování

## 2. Webové proxy

- maskování IP adresy
- např. http://www.samair.ru
- může být rizikové
- komunikace jde přes servery, z nichž mnohé mohou být napadené počítače jiných uživatelů (bez vědomí majitelů)
- zpomaluje, není stabilní

# Možnosti anonymního surfování

## 3. Anonymizační software

- data jdou přes sérii proxy serverů (kaskádu)
- na vyšší úrovni než předchozí, ale taky ne 100% účinné
- sítě TOR, JAP, Jondo (na základě JAP)
- také nízká rychlost

# Reset hesla Windows

- nabootujeme SystemRescueCD
- zjistíme, jak je označen oddíl s instalací Windows, zde např. `/dev/sda2`
- připojíme oddíl, na kterém jsou nainstalovány Windows
  `mkdir /mnt/windows`
  `ntfs-3g /dev/sda2 /mnt/windows` (nebo použijeme `mount`)
- přesuneme se do složky, ve které je registr Windows
  `cd /mnt/windows/Windows/System32/config`
- spustíme program, který umožní resetovat heslo
  `chntpw -u username SAM`

http://onubuntu.blogspot.cz/2011/08/reset-your-windows-password-with.html