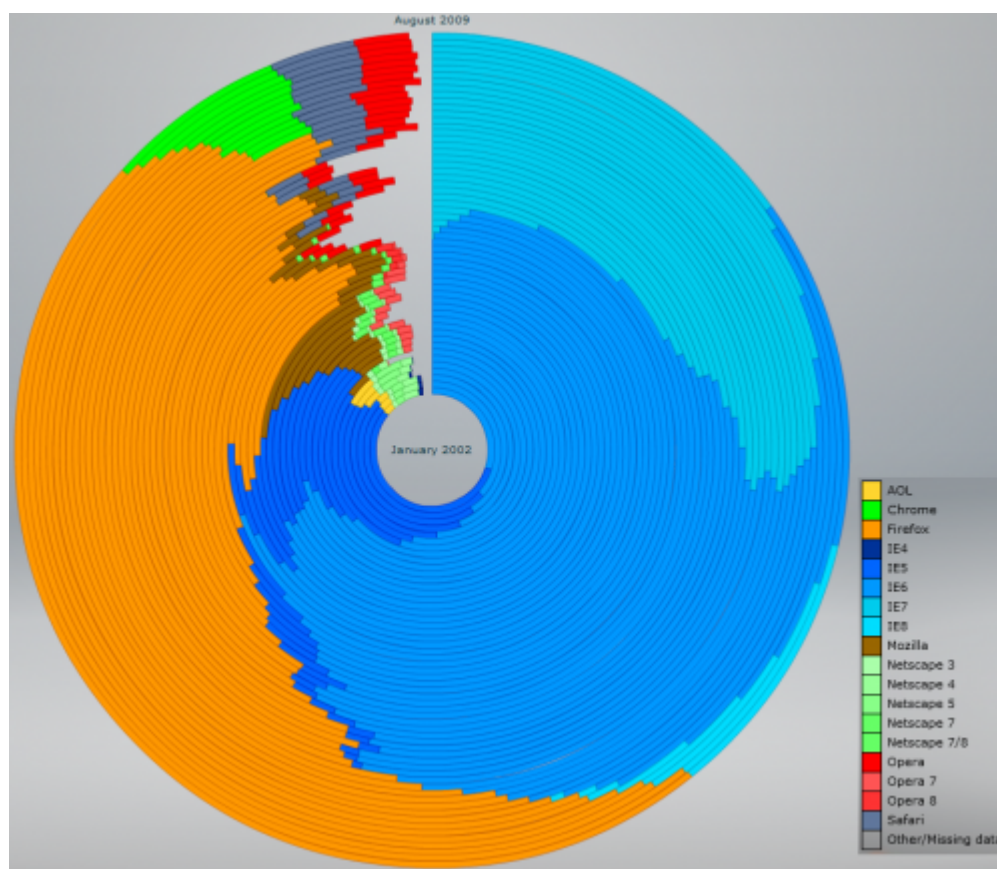


Analiza web aktivnosti

Forenzika web preglednika uključuje sve podatke koji se mogu otkriti o korisnikovoj aktivnosti na Internetu, od e-mail poruka (u slučaju da se koristio web klijent za pristup sandučiću elektroničke pošte), preuzetih datoteka, kronološkog popisa posjećenih stranica, pa do lozinke za razne web stranice. S obzirom da se računala danas uglavnom koriste baš zbog mogućnosti povezivanja na Internet i razmjenu podataka sa svijetom, ovo područje je jedno od jako bitno za računalne istražitelje. Slika ispod prikazuje popularnost pojedinih web preglednika među korisnicima. Može se primjetiti da su Internet Explorer i Mozilla Firefox najpopularniji te će se stoga u nastavku detaljnije opisati njihov način rada. Uz njih Google Chrome ima najbržu stopu širenja od trenutka pojave pa će se i njega uključiti u analizu.



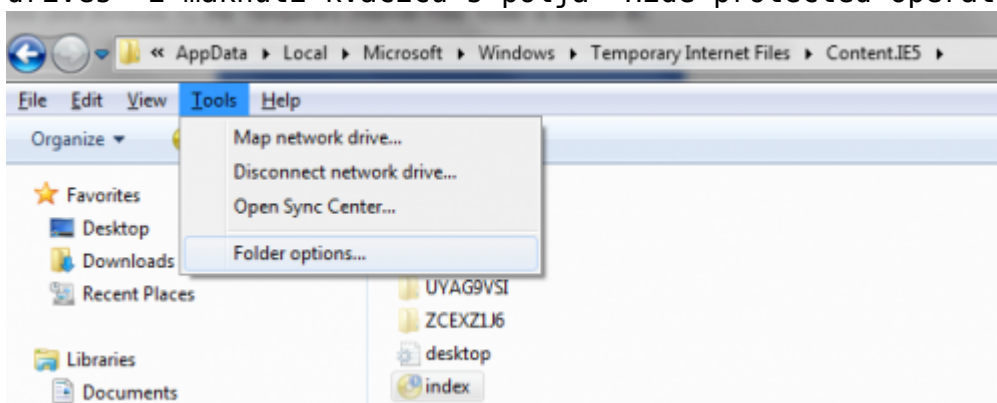
Dok korisnik posjećuje stranice na Internetu, njegov preglednik pohranjuje sve podatke o posjetama u određene datoteke na korisnikovom računalu (npr. index.dat za Internet Explorer). Web forenzičari prilikom istrage moraju obratiti pažnju na više elemenata kroz koje mogu saznati različite stvari o korisniku. To su:

- povijest pregledavanja stranica (eng. *browsing history*),
- webmail (*web based e-mail*),
- kolačići (eng. *cookies*),
- ključne riječi (eng. *keywords*) korištene u pretragama,
- preuzete/pokrenute datoteke (eng. *download history*),
- lozinke,
- podaci koje je korisnik upisivao u formulare (eng. *form history*).

[Saznaj više o alatima za analizu web aktivnosti](#)

Kako bi se tražene datoteke mogle naći, u novijim verzijama operacijskog sustava Windows (Vista i 7) potrebno je promijeniti postavke vidljivosti. Microsoft je naime odlučio sakriti datoteke i mape koje nisu potrebne standardnom korisniku kako ne bi slučajno promijenio neki bitni podatak potreban za rad sustava. Kako bi se mogli izvesti postupci opisani u ovom dokumentu, potrebno je provesti sljedeće korake:

- pozicionirati se u prozor Windows Explorera,
- pritisnuti tipku Alt na tipkovnici da se pojavi skrivena izborna traka (File, Edit, View, Tools, Help),
- odabrati "Folder options...",
- u kategoriji "View" označiti kvačicom polje "Show hidden files, folders, or drives" i maknuti kvačicu s polja "Hide protected operating system files"



Povijest pregledavanja stranica

Posjećene stranice puno govore o namjerama korisnika. Polako se postavlja pitanje da li su ljudi postali previše ovisni o tražilicama. Gotovo sve što ih zanima, od recepata za kolače do medicinskih dijagnoza traže na Internetu. Stoga ni ne čudi što se računalna forenzika proširila i na analizu povijesti posjećениh stranica. Ne pohranjuju svi preglednici podatke na isti način. Internet Explorer (IE) zapisuje podatke u binarnom formatu u datoteku index.dat, Mozilla/Firefox/Netscape obitelj koristi ASCII format u datoteci places.sqlite (verzije prije Firefox 3.0 koriste history.dat), a Google Chrome koristi datoteku history.file.

Internet Explorer

IE sprema podatke o posjećivanju stranica u datoteku naziva index.dat. Njena lokacija ovisi o verziji operacijskog sustava Windows. Za operacijske sustave Windows Vista i 7 nalazi se na adresi:

```
C:\Users\<User's ID>\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5
```

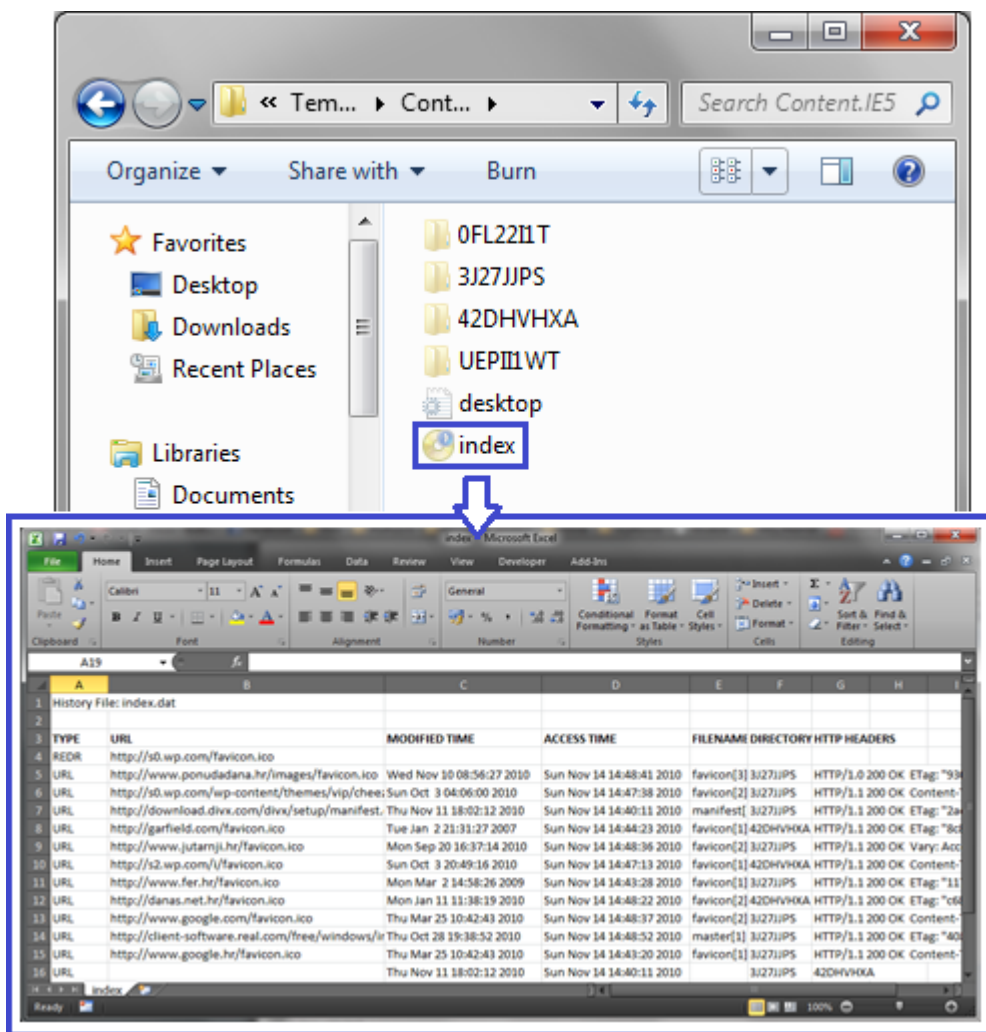
U slučaju ranijih inačica operacijskog sustava Windows (XP i ranije), datoteka se nalazi na adresi:

```
C:\Documents and Settings\<User's ID>\Local Settings\Temporary Internet
```

Files\Content.IE5

Index.dat je datoteka specifična za program koji ju je napravio (u ovom slučaju IE) i u tom obliku se ne može otvoriti drugim alatima. Zato se koriste programi koji će ili pročitati sadržaj datoteke direktno iz memorije (heksadecimalni uređivači) ili će iščitati podatke datoteke i prepisati ih u pogodniji format (npr. Pasco). Na slici ispod je prikazan sadržaj mape Content.IE5.

Osim datoteke index.dat, u mapi Content.IE5 se nalaze još (obično) 4 mape nejasno odabranih imena koje se koriste za pohranjivanje podataka s posjećenih stranica (eng. *cached files*). Ti su podaci popisani u index.dat, a nalaze se u jednoj od 4 mape nejasnih imena. Radi usporedbe, u slučaju drugih preglednika svaka kategorija podataka (lozinke, preuzete datoteke, ...) ima svoju zasebnu datoteku koju treba pojedinačno analizirati (iako postoje alati koji mogu obuhvatiti sve odjednom).



Firefox/Mozilla/Netscape

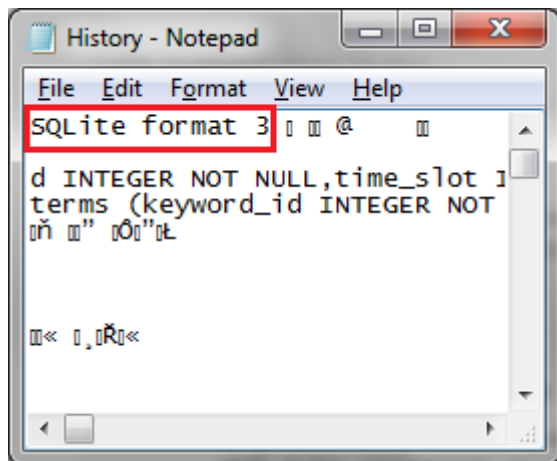
U preglednicima Firefox 2, Mozilla Suite/Sea Monkey 1.x i ranijim verzijama, povijest pregledavanja se pohranjivala u datoteci history.ico.dat. U lipnju 2008. se pojavila verzija Firefox 3.0 s kojom se ime datoteke promijenilo u places.sqlite. Ona se u Windows Vista i 7 nalazi na adresi:

C:\Users\'s ID>\AppData\Roaming\Mozilla\Firefox\Profiles\

U ranijim inačicama Windowsa se nalazi na adresi:

Google Chrome

Preglednik Google Chrome podatke pohranjuje u datoteci `history.file` iz čije se ekstenzije ne može otkriti kojim programom se može analizirati. Ako se datoteka otvori jednostavnim tekstualnim uređivačem (npr. Notepad), može se vidjeti da je riječ o SQL datoteci, kao i kod Mozille (vidi sliku).



To znači da se za pregledavanje datoteke može koristiti isti tip programa kao i za Mozillu (npr. [SQLite Database Browser](#)), kao i posebni forenzički programi (npr. [Web Historian](#)).

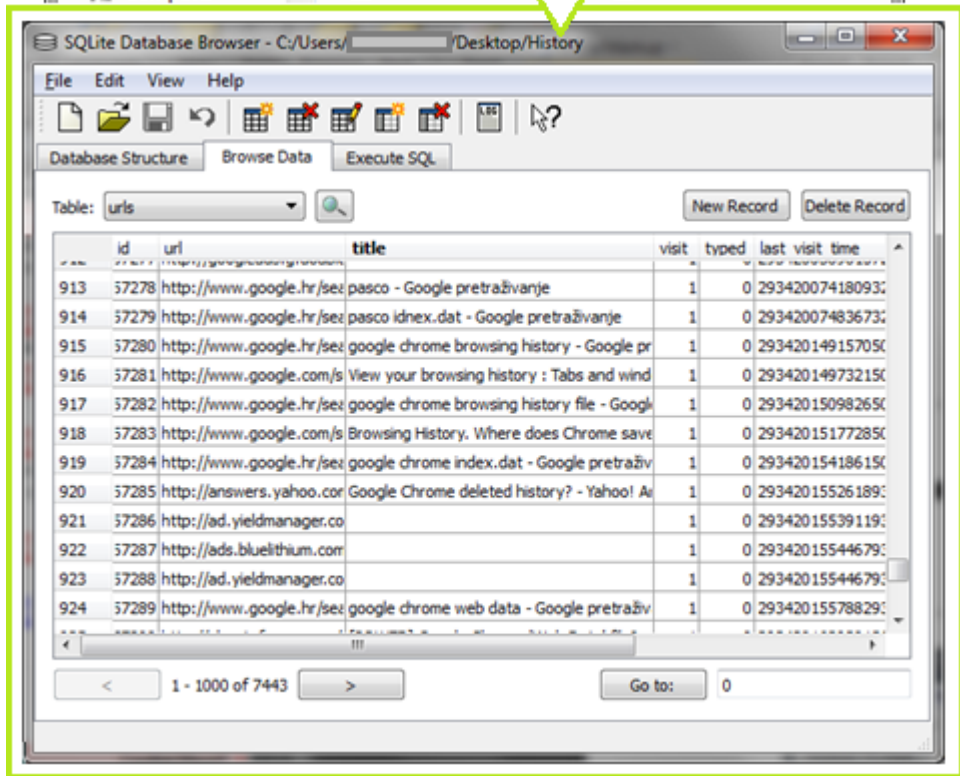
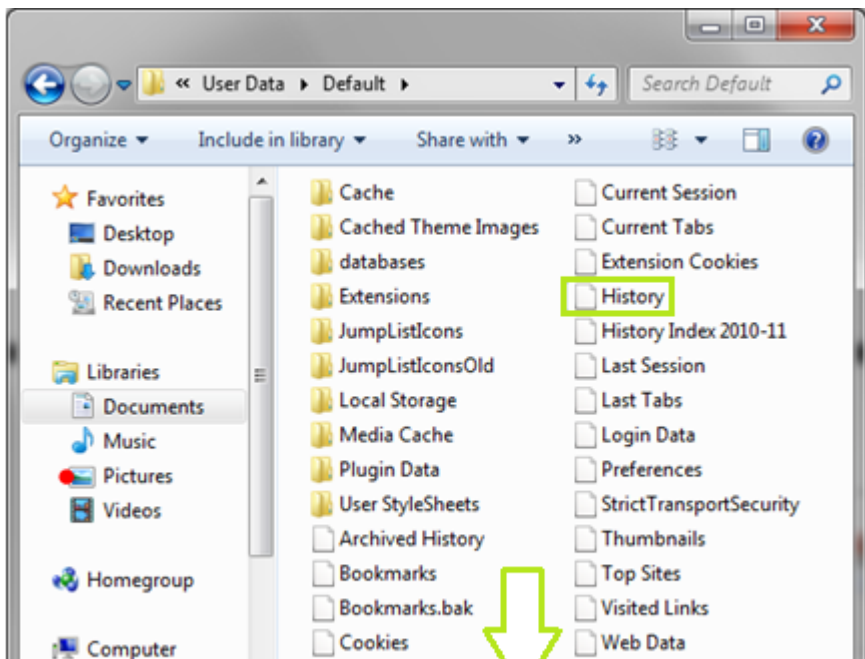
Operacijski sustavi Windows Vista i 7 pohranjuju ovu datoteku na adresi:

```
C:\Users\\AppData\Local\Google\Chrome\User Data\Default
```

Windows XP i starije inačice koriste adresu:

```
C:\Documents and Settings\\Local Settings\Application Data\Google\Chrome\User Data\Default
```

Google Chrome koristi drugačije nazive datoteka za pohranjivanje podataka o posjećivanju stranica od Mozille. Tako na primjer `History.file` sadrži podatke o posjećenim stranicama, `Cookies.file` pohranjuje vrijednosti kolačića, u datoteci `Bookmarks.file` su pohranjene adrese zapamćenih (eng. *bookmarked*) stranica itd. Sve datoteke se mogu otvoriti alatima za čitanje SQL baza podataka.



From: <https://www.cis.hr/WikiS/> - **wikiS**

Permanent link: https://www.cis.hr/WikiS/doku.php?id=old_zalbrisati:web_forenzika

Last update: **2015/01/21 13:37**

