Alati za analizu web aktivnosti

Profesionalni računalni forenzičari u pravilu koriste licencirane alate koji imaju širi spektar mogućnosti, ne samo u vidu forenzike web preglednika nego i za analizu baza podataka, mrežnu forenziku i druge grane računalne forenzike. Osim što pružaju profesionalnu tehničku podršku korisnicima, istražitelj može biti siguran da instaliranjem licenciranog programskog paketa nije izložio računalo zloćudnim programima (što je bitno za prihvatljivost dokaza otkrivenih tim računalom na sudu). Neki od poznatijih licenciranih alata su:

- EnCase
- Forensic ToolKit
- COFFEE

U vidu demonstracije mogućnosti forenzike web preglednika, u ovom poglavlju će biti opisani neki od brojnih besplatnih alata dostupnih besplatno:

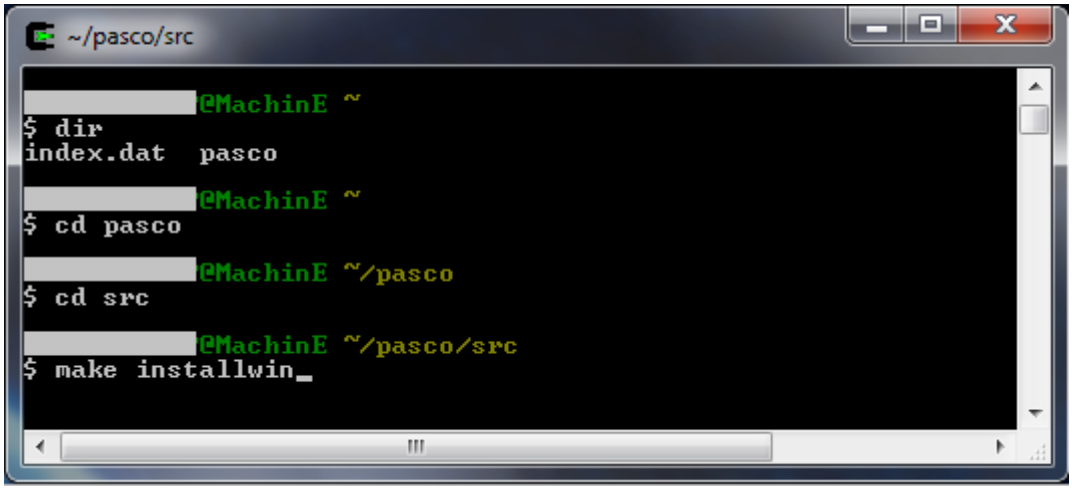
- Pasco
- Heksadecimalni uređivači
- Web Historian
- Alati proizvođača Nirsoft
- FireMaster

Pasco

Ideja iza stvaranja ovog alata je bila, dok postupci u računalnoj forenzici moraju biti dobro dokumentirani i ponovljivi, previše bitnih Microsoft Windows datoteka ima nedokumentiranu strukturu. Tako je, na primjer, ekstenzija datoteke index.dat specifična i prepoznatljiva jedino alatu koji je stvorio datoteku (IE). Pasco radi tako da prolazi kroz datoteku index.dat, čita podatke (parsira) i ispisuje ih u formatu koji je moguće čitati s većinom tekstualnih uređivača, stvarajući pritom datoteku index.txt. Dok je dobivenu datoteku moguće otvoriti alatima za uređivanje teksta (npr. Notepad, MS Word, ...), otvaranjem u alatu za rad s proračunskim tablicama (npr. MS Excel) se dobije pregledniji, tablični oblik.

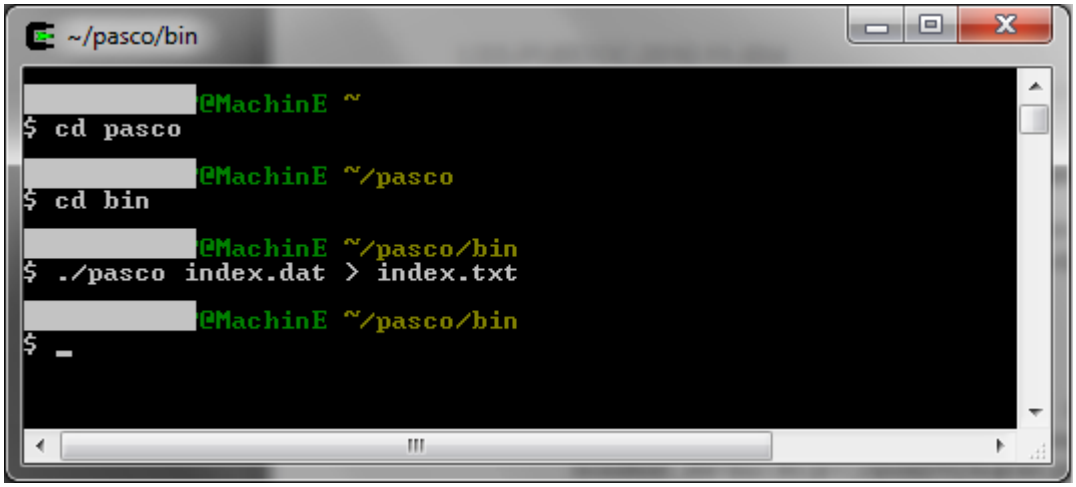
S obzirom da je namijenjen korisnicima operacijskog sustava Linux, korisnici Windows operacijskog sustava prvo moraju osigurati virtualno UNIX okruženje, primjerice alat Cygwin. Za instalaciju je potrebno je slijediti korake:

1. instalirati alat Cygwin,
2. preuzeti Pasco alat,
3. u Cygwin komandnom prozoru se smjestiti u mapu gdje je pohranjen Pasco paket,
4. ući u mapu /src te
5. utipkati naredbu “make installwin”, čime se u mapi /Pasco/bin stvorila aplikacija Pasco.exe.

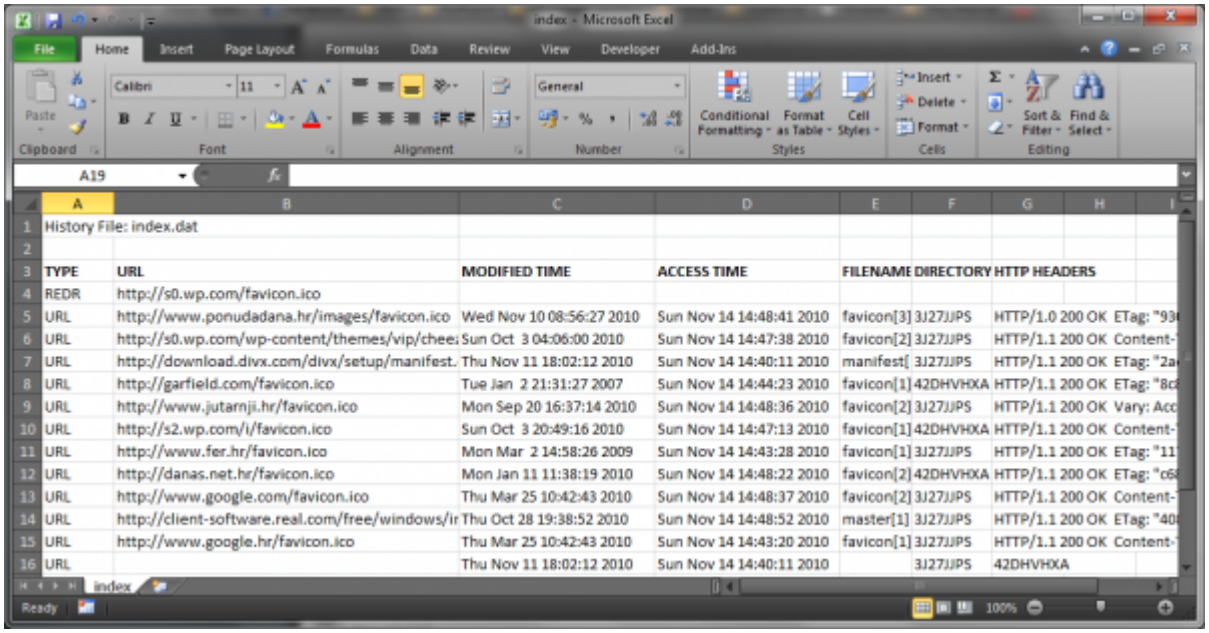


Nakon instalacije korisnik treba u mapu /bin kopirati datoteku index.dat (čija je lokacija objašnjena ovdje). U Cygwin komandnom prozoru je potom potrebno upisati naredbu:

```
./pasco index.dat > index.txt
```



Dobivenu datoteku index.txt je moguće otvoriti i pregledati alatom MS Excel ili nekim drugim programom kojim se mogu obrađivati proračunske tablice, kao i uobičajenim alatima za uređivanje teksta (iako je u tom obliku manje pregledna nego u tablici).

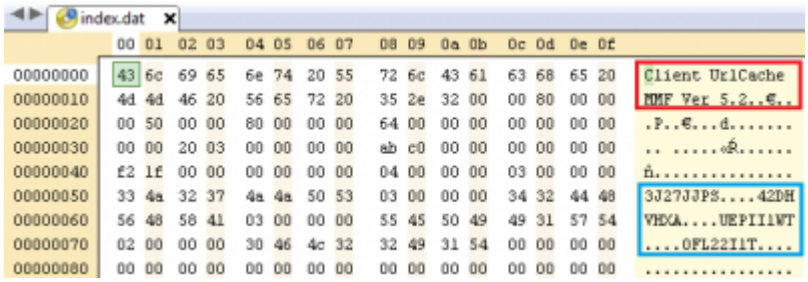


Sad su vidljivi podaci koje IE zapisuje u datoteku index.dat:

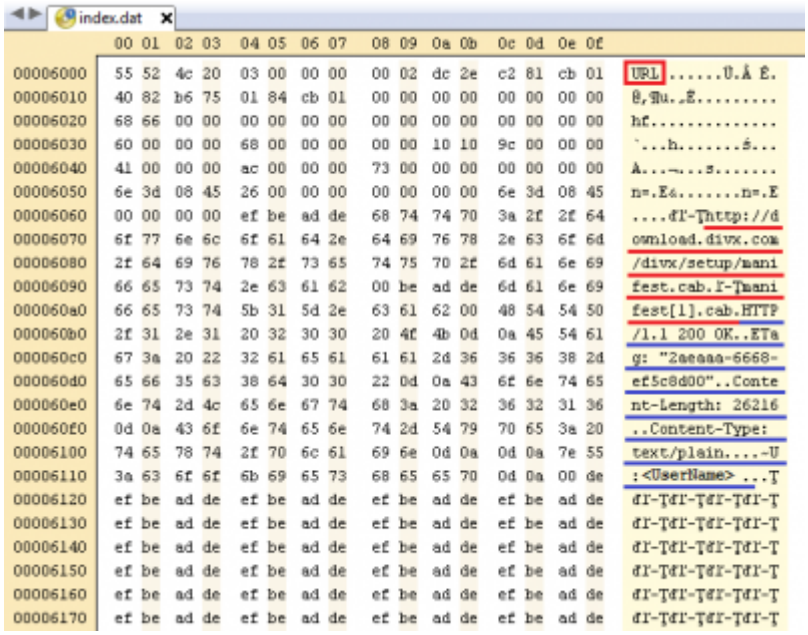
- **Type** – tip zapisa. Moguće vrijednosti su:
  - URL (adresa web stranice),
  - REDR (eng. redirect), prikazuje URL stranice na koju je korisnik automatski preusmjeren),
  - LEAK (javlja se prilikom pogreške),
  - HASH (hash indeksi, ne sadrže privatne podatke),
- **URL** – adresa posjećene web stranice,
- **Modified Time** – vrijeme zadnje izmjene posjećene stranice,
- **Access Time** – vrijeme zadnjeg pristupa stranici,
- **Filename** – datoteka pohranjena na računalu u mapi čije je ime u stupcu „Directory“ (npr. slike, ikone, css kodovi, ...)
- **Directory** – jedna od (standardno) 4 datoteke slučajnog imena u mapi Content.IE5 i
- **HTTP Headers** – poruke korištenog protokola (npr. “404 error page not found” kad je klijent uspio uspostaviti vezu s poslužiteljem, ali poslužitelj ne može pronaći traženu stranicu ili “200 OK” za uspješnu vezu), detalji o sadržaju (veličina, tip), korišteni antivirusni program te ime korisnika.

Hex Editori

Heksadecimalni uređivač je još jedan tip programa koji se koristi za analizu index.dat. U sljedećim primjerima se koristi alat Free Hex Editor Neo. Taj tip programa se koristi kada se želi izravno pristupiti memoriji ili pregledati zaglavlje datoteke u potrazi za metapodacima.



Slika iznad prikazuje zaglavlje datoteke index.dat. Prvi podaci u zaglavlju govore o verziji datoteke (crveni okvir na slici), nakon čega su zapisana imena datoteka u kojima su sačuvani podaci s otvaranih stranica (eng. *cached files*). Te datoteke se nalaze u istoj mapi kao i index.dat.



S određenim odmakom u memoriji od zaglavlja se pojavljuje prvi zapis korisnih podataka. Crveno i plavo su podcrtani dijelovi koji su vidljivi i prilikom otvaranja datoteke index.txt.

Web Historian

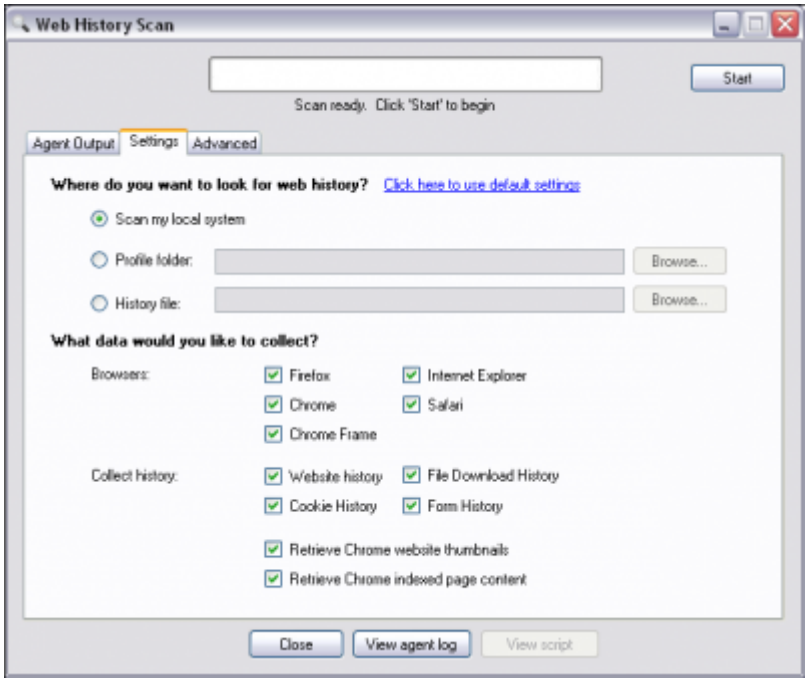
Web Historian je program s jednostavnim korisničkim sučeljem što ga čini pogodnim za amatere. Prije instalacije, potrebno je provjeriti da li se koriste podržani operacijski sustav i preglednik trenutnom verzijom programa. U trenutku pisanja ovog dokumenta, aktualna je verzija Web Historian 2.0. Podržan je Windows operacijski sustav i to sljedeće inačice:

- 2000 SP4+,
- XP SP2+ (32-bitni),
- 2003 SP2+ (32-bitni/64-bitni),
- Vista SP0-SP2 (32-bitni) te
- 7 (64-bitni).

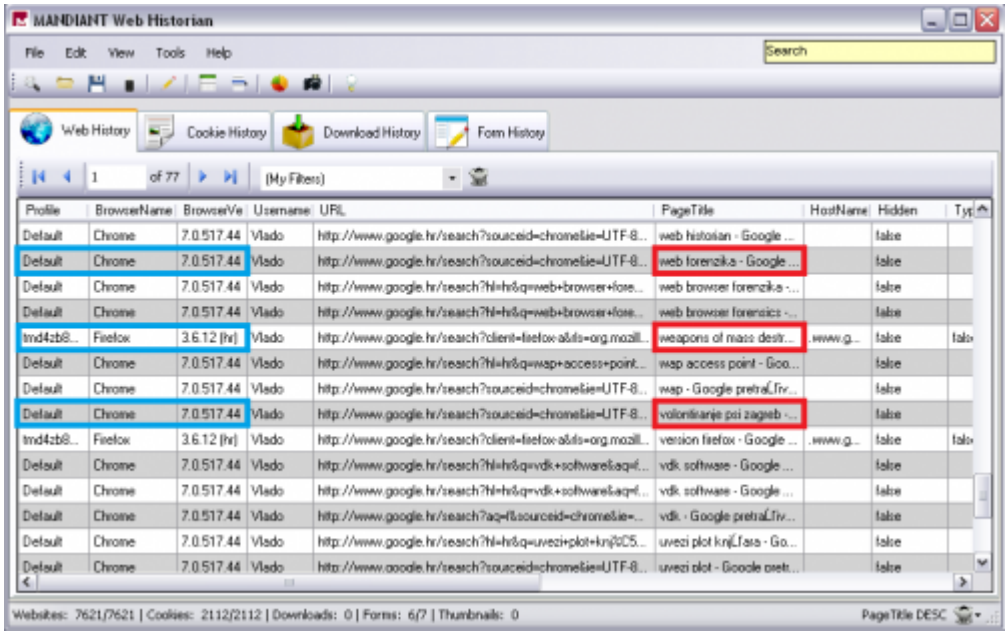
Podržani preglednici su:

- Firefox 2, Firefox 3+,
- Chrome 3+,
- Internet Explorer 5-8 i
- Safari 3+.

Pomoću Web Historiana, može se analizirati povijest posjećenih stranica (Website History), podaci koje su pohranile posjećene stranice (Cookie History), preuzete datoteke (File Download History) i podaci koje je korisnik unosio u formulare (Form History).

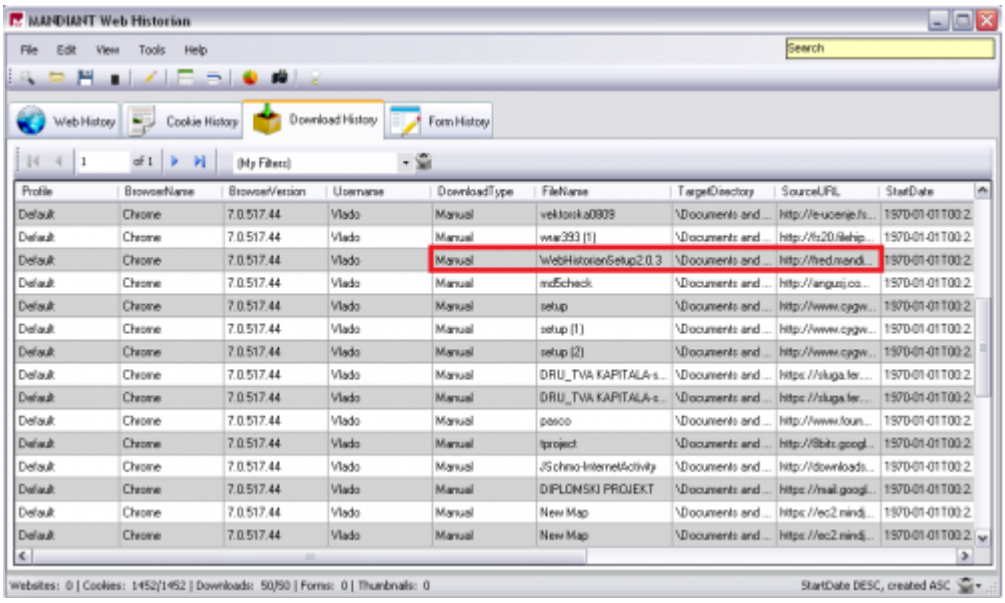


Nakon određivanja parametara pretrage, traženi podaci se prikazuju u tabličnom obliku. Svaki redak sadrži detaljne informacije o korištenom pregledniku, njegovoj inačici, korisničkom imenu osobe, URL adresi, datumu pristupa, i sl. Web Historian će prikazati i podatke koje je korisnik izbrisao naredbom “clear history” u pregledniku (čime se podaci brišu i iz datoteka u kojima se pohranjuje povijest pregledavanja web stranica – index.dat, places.sqlite i history.file). Podaci neće biti prikazani jedino ako se prekoračila dozvoljena veličina datoteke (u tom se slučaju novi podaci pišu preko starih) ili ako je disk formatiran (pri čemu se brišu svi podaci s diska računala, ne samo povijest pregledavanja).



Analizirajući povijest pregledavanja stranica, može se primijetiti da se korisnik htio informirati o web forenzici, oružju masovnog uništavanja te da ga zanima volontiranje sa psima. Vidi se da mu je Google Chrome glavni preglednik (Profile stupac – oznaka default) i da se korisnik Windows profila zove Vlado. Pregledom povijesti preuzimanja datoteka može se, između ostalog, vidjeti koji korisnik je preuzeo koju datoteku, otkud i gdje je pohranjena. Tako slika ispod pokazuje da je korisnik Vlado pomoću preglednika Chrome, verzije 7.0.517.44, ručno preuzeo datoteku imena “WebHistorianSetup2.0.3”, sa stranice koja počinje s `http://fred.mandi…` (cijela adresa se može vidjeti proširivanjem polja) i pohranio negdje u mapu `C:\Documents and Settings\ ..`

(apsolutna putanja može se vidjeti proširivanjem polja). Detalja ima još, ali za ilustraciju su prikazani samo osnovni podaci.



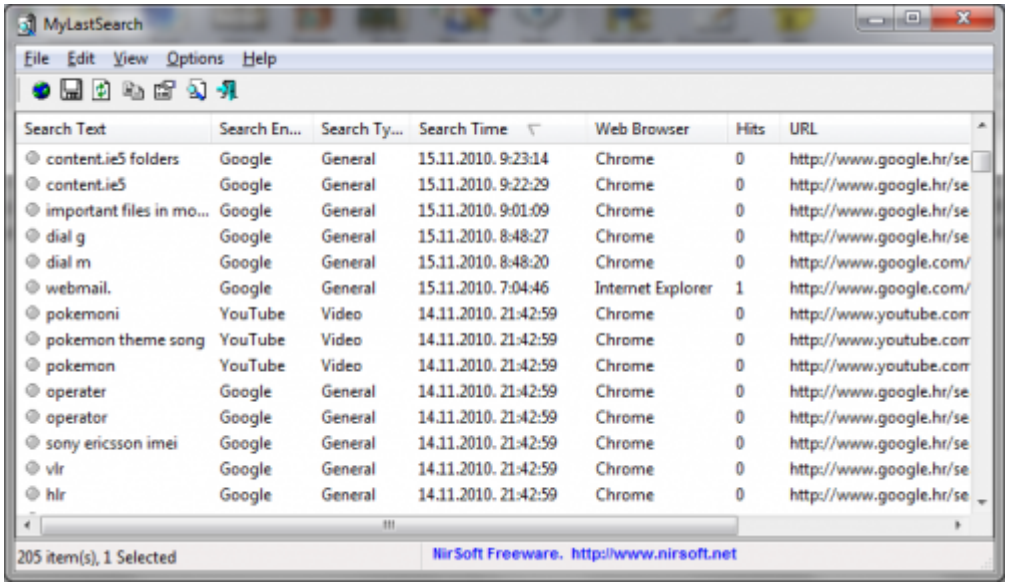
NirSoft alati

Kao što je već spomenuto, postoje profesionalni alati koji su zbog cijene dostupniji forenzičarima zaposlenima u vladinim organizacijama ili privatnim tvrtkama. No na Internetu su dostupni mnogi besplatni alati s ograničenim, ali dostatim mogućnostima za amatere. Kako bi se prikazalo koji se sve podaci mogu otkriti na računalu, prikazani su alati tvrtke NirSoft koji je samo jedan iz mora ponuđača, a njegova ponuda se sastoji od sljedećih alata:

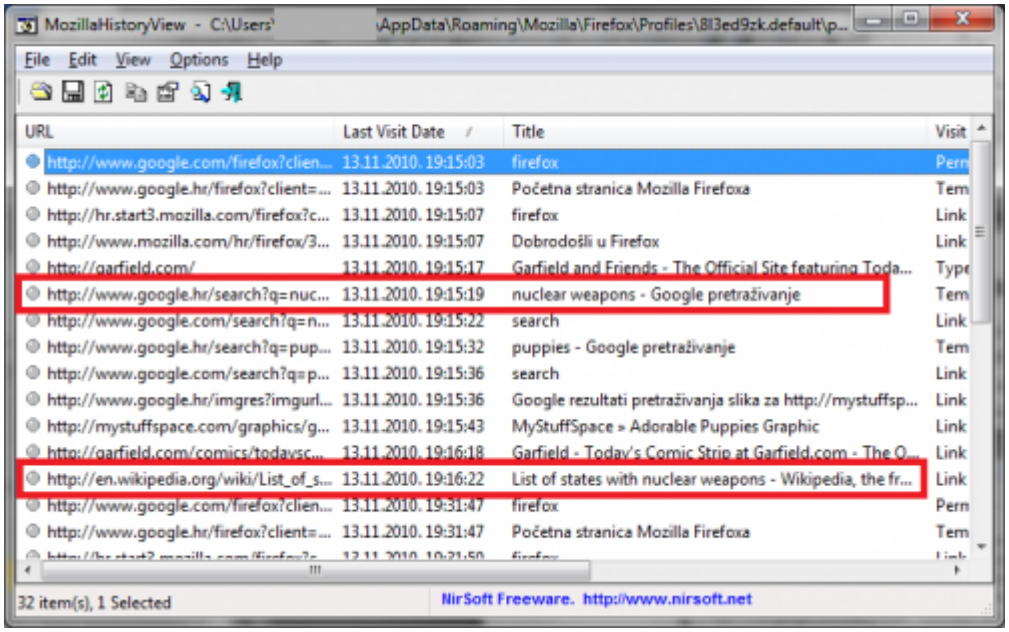
- **IEHistoryView** – prikazuje posjećene stranice prilikom korištenja preglednika IE,
- **IECacheView** – prikazuje podatke spremljene prilikom korištenja preglednika IE,
- **IECookiesView** – prikazuje pohranjene kolačiće prilikom korištenja preglednika IE,
- **IEPassView** – prikazuje zapamćene lozinke u pregledniku IE,
- **MozillaHistoryView** – prikazuje posjećene stranice prilikom korištenja preglednika Mozilla,
- **MozillaCacheView** – prikazuje podatke spremljene prilikom korištenja preglednika Mozilla,
- **MozillaCookiesView** – prikazuje pohranjene kolačiće prilikom korištenja preglednika Mozilla,
- **PasswordFox** – prikazuje zapamćene lozinke u pregledniku Firefox,
- **ChromeCacheView** – prikazuje podatke spremljene prilikom korištenja preglednika Chrome,
- **MyLastSearch** – skenira sačuvane cache i history datoteke od preglednika IE, Firefox, Opera i Chrome i pronalazi pojmove upisivane u tražilice Google, Yahoo i MSN, te pretrage socijalnih mreža Facebook, Twitter i MySpace.

Navedeni programi su vrlo jednostavni za korištenje. Korisnik samo treba preuzeti paket sa željenim alatom i pokrenuti aplikaciju. S obzirom da su traženi podaci (npr. stranice posjećene Firefox preglednikom) pohranjeni na standardnim lokacijama ovisno o korištenom pregledniku i samom operacijskom sustavu, aplikacija zna gdje tražiti pojedine podatke.

Slika ispod prikazuje prozor alata **MyLastSearch** u kojem se mogu vidjeti pojmovi koje je korisnik pretraživao, zajedno sa tražilicom i web preglednikom koje je koristio.

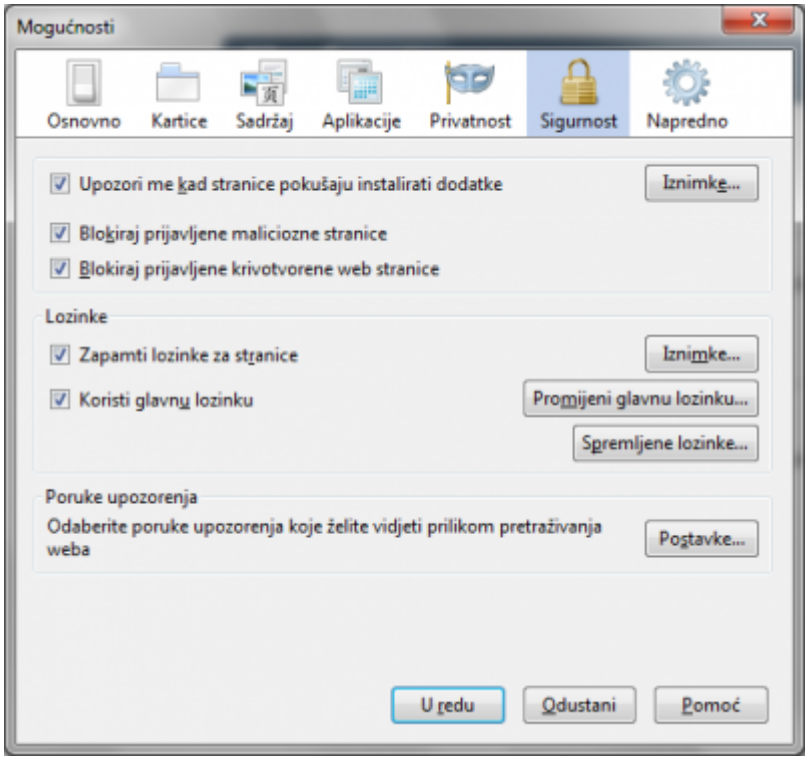


Na slici niže je primjer prikaza povijesti pregledavanja korištenjem tražilice Firefox pomoću alata **MozillaHistoryView**. Iz priloženog se može uočiti da je osumnjičeni istraživao nuklearno oružje što bi išlo u prilog istražiteljima kad bi osumnjičeni bio optužen za npr. terorizam.



FireMaster

Mozilla Firefox preglednik omogućava korisniku postavljanje jedne glavne lozinke (*Master Password*) koja će zaštititi sve ostale lozinke pohranjene u Firefox pregledniku. Ova se opcija može postaviti otvaranjem preglednika te odabirom `Alati` → `Opcije` odnosno `Tools` → `Options`. Nakon toga se izabere kartica `Sigurnost` te se označi polje `Koristi glavnu lozinku` nakon čega korisnik određuje lozinku.



U slučaju da korisnik zaboravi glavnu lozinku, ima dva izbora.
Prvi izbor je poništavanje lozinke upisivanjem adrese chrome://pippki/content/resetpassword.xul u preglednik, čime se brišu i sve pohranjene lozinke koje su bile zaštićene glavnom lozinkom. U slučaju kad se pokušava doznati nečija tuđa kako bi se pristupilo njegovim podacima, ova opcija je beskorisna.
Drugi izbor je *brute force* napad alatom FireMaster. Ovaj postupak može trajati prilično dugo, pogotovo ako se ne zna ništa o strukturi lozinke (duljina, korišteni znakovi, ...). Biti će opisan način korištenja FireMaster alata u Windows operacijskom sustavu, iako postoji i inačica alata za Linux.

Prvo je potrebno preuzeti alat FireMaster. Nakon instalacije se alat pokreće iz komandne linije (`Start` → Run → "`cmd`"). Pokretanjem će se u komadnom prozoru ispisati slijedeće (vidi sliku):

Brute force napad

Ako se pretpostavi da je korisnik imao glavnu lozinku duljine 10 znakova u kojoj su samo mala slova engleske abecede, naredba u komandnoj liniji će izgledati ovako:

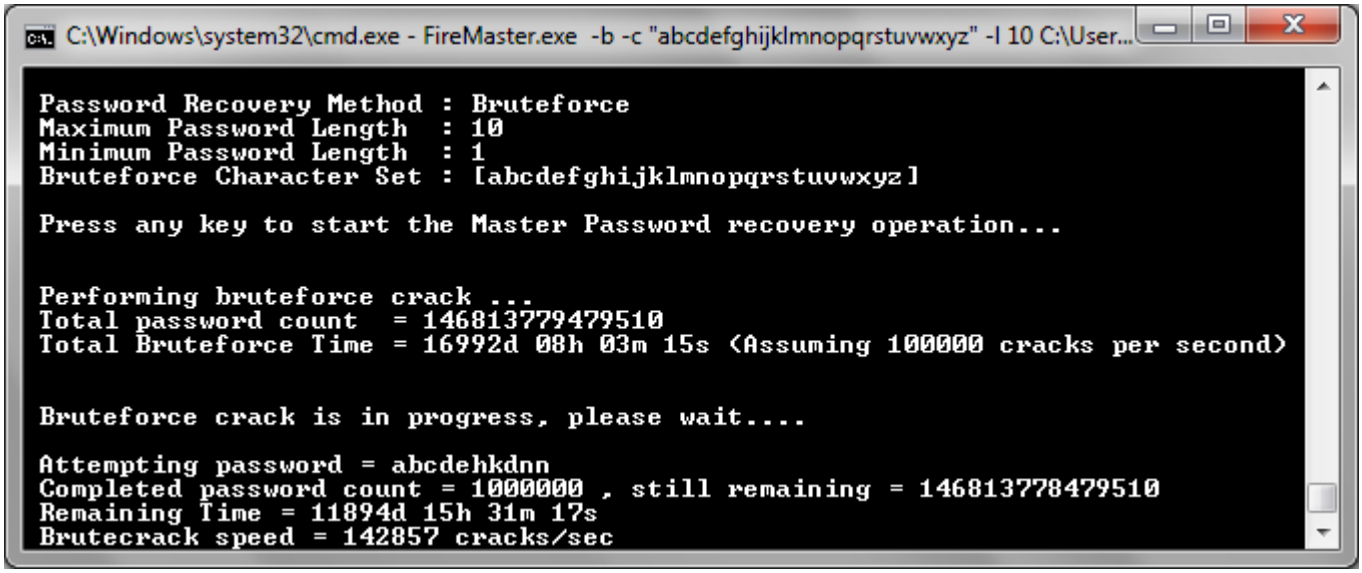
```
FireMaster.exe -b -c “abcdefghijklmnopqrstuvwxyz” -l 10 %AppData%\Mozilla Firefox\Profiles\<broj profila>.default
```

Gornja naredba radi slijedeće:

- -b znači da je riječ o *brute force* napadu

- `-c` daje niz znakova od kojih je sastavljena lozinka
- `-l` označava maksimalnu duljinu lozinke
- `%AppData%\Mozilla Firefox\Profiles\<broj profila>.default` je adresa na kojoj se nalazi datoteka key3.db (vidi poglavlje o datotekama u Firefox profile mapi)

Kao što se može vidjeti na slici ispod, predviđeno vrijeme za provjeru svih mogućih lozinki je 16992 dana (46 godina!!) 8 sati 3 minute i 15 sekundi uz provjeravanje 100000 lozinki po sekundi.



U slučaju kad se zna format (*pattern*) lozinke, postupak se ubrzava. Za naredbu:

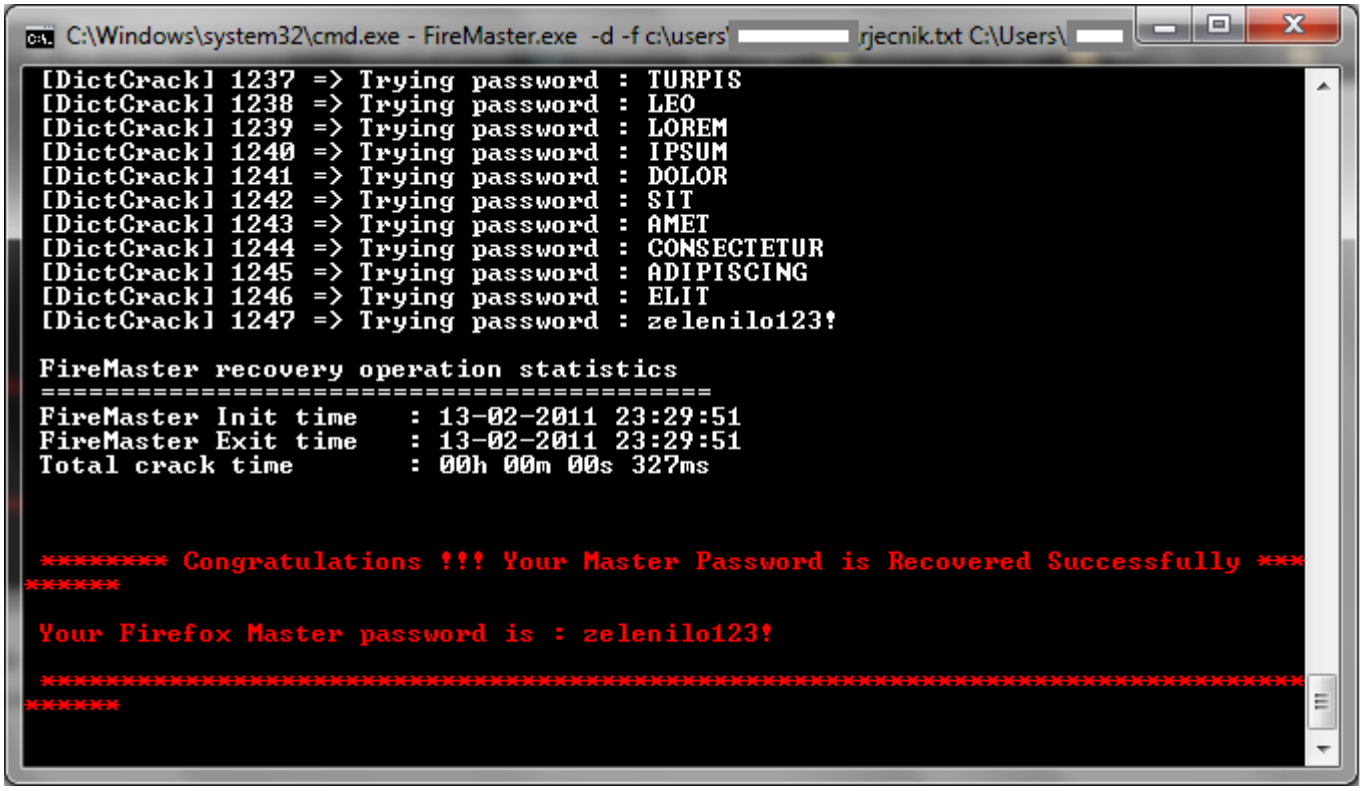
```
FireMaster.exe -b -c “abcdefghijklmnopqrstuvwxyz” -l 10 -p “z???????o”
%AppData%\Mozilla Firefox\Profiles\<broj profila>.default
```

vrijeme pretrage se smanjuje na 24 dana 4 sata 4 minute i 31 sekundu.

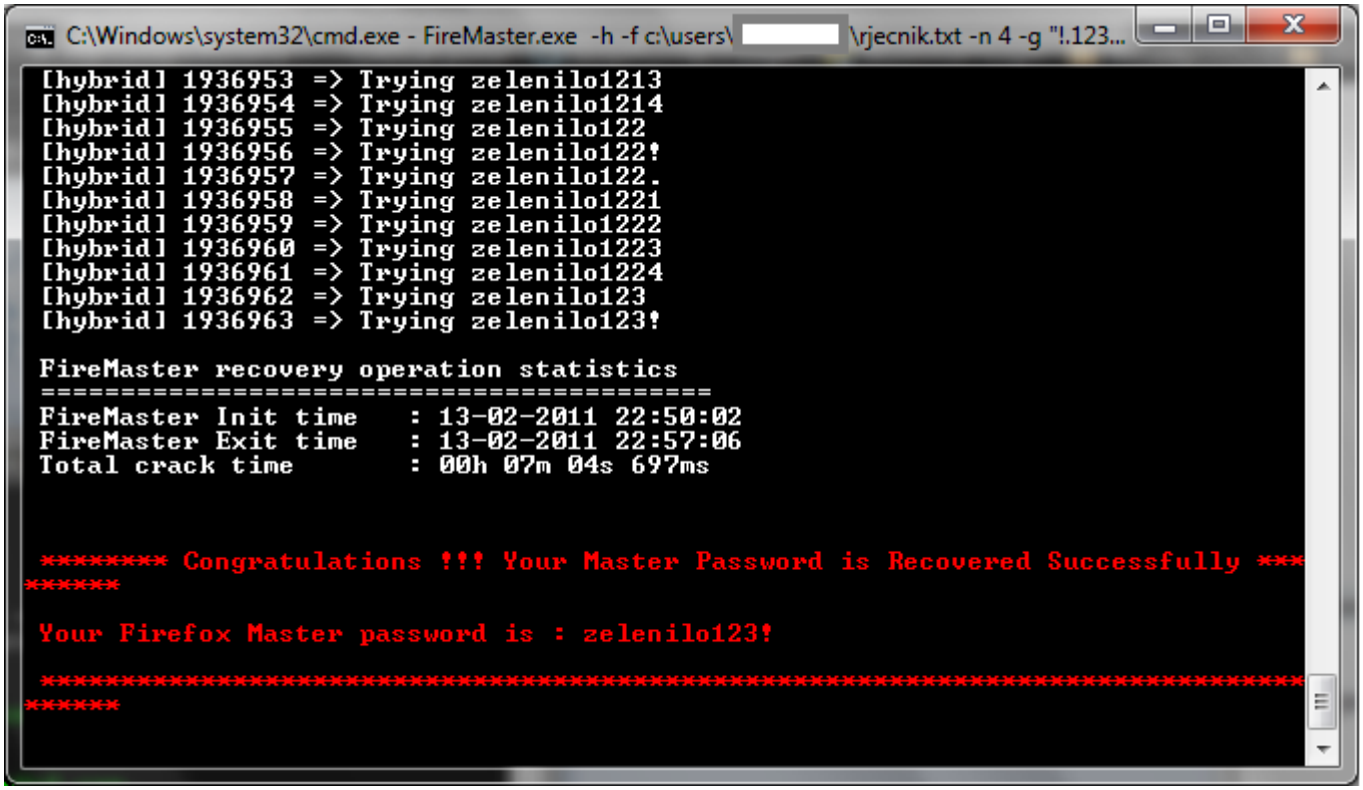
Dictionary i hybrid napad

Postoji još jedan način probijanja lozinke ovim alatom, a to je napad rječnikom (eng. *dictionary attack*). Za to je potrebna datoteka (rječnik) sa svim mogućim lozinkama koje se provjeravaju. U tom slučaju postoje 2 opcije:

- provjeravanje samo riječi iz rječnika naredbom
  `FireMaster.exe -d -f c:rjecnik.txt %AppData%\Mozilla Firefox\Profiles\<broj profila>.default`
  - `-d` označava *Dictionary* napad
  - `-f` označava lokaciju rječnika



- provjeravanje riječi iz rječnika da bi se našao dio lozinke uz zadani skup znakova koji mogu sačinjavati preostali dio lozinke
  `FireMaster.exe -h -f c:rjecnik.txt -n 3 -g “123” -s %AppData%\Mozilla Firefox\Profiles\<broj profila>.default`
  - `-h` označava *Hybrid* napad
  - `-f` označava lokaciju rječnika
  - `-n` je maksimalna duljina nizova koji će se generirati kao dodatak lozinki iz rječnika
  - `-g` je skup (eng. *group*) znakova koji sačinjavaju dodatak lozinki
  - `-s` (eng. *suffix*) označava da će se dodatak dodati nakon lozinke (`pass123`) → `-p` (eng. *prefix*) bi značilo da će se dodatak dodati prije lozinke (`123pass`)



Usporedba korištenih alata

	Internet Explorer	Mozilla Firefox	Google Chrome
Pasco	Prepisuje index.dat u razumljiviji .txt format	-	-
Hex editori	Korisni za pregled svih podataka iz index.dat ako korisnik zna što traži, gdje to naći i pod kojim imenom	Moguće koristiti, ali ima puno lakših načina pregleda (npr. SQLite Manager)	Moguće koristiti, ali ima puno lakših načina pregleda (npr. SQLite Manager)
Web Historian	Povijest pregledavanja, podaci iz formulara, preuzete datoteke, kolačići	Povijest pregledavanja, podaci iz formulara, preuzete datoteke, kolačići	Povijest pregledavanja, podaci iz formulara, preuzete datoteke, kolačići
NirSoft alati	Povijest pregledavanja, kolačići, lozinke, cache memorija	Povijest pregledavanja, kolačići, lozinke, cache memorija	Povijest pregledavanja, kolačići, lozinke, cache memorija