Sveučilište u Splitu

Fakultet elektrotehnike, strojarstva i brodogradnje

ANALIZA POVIJESTI PRETRAŽIVANJA U BROWSERU

Seminarski rad

Josip Barbir

Filip Volarević

Split, srpanj 2023.

Sadržaj

[1 Uvod 1](#_Toc139225882)

[2 Chrome iz forenzičke perspektive 2](#_Toc139225883)

[2.1 Problematika 2](#_Toc139225884)

[2.2 Pohrana 3](#_Toc139225885)

[2.3 Mjere zaštite 5](#_Toc139225886)

[2.4 Forenzički alati 6](#_Toc139225887)

[3 Implementacija 8](#_Toc139225888)

[3.1 Motivacija 8](#_Toc139225889)

[3.2 Struktura projekta 8](#_Toc139225890)

[3.3 Back-end 9](#_Toc139225891)

[3.4 Front-end 11](#_Toc139225892)

[4 Zaključak 14](#_Toc139225893)

# Uvod

Kod forenzičke analize, preglednici (*engl. browser*) predstavljaju „gold mine“ sa količinom informacija koje sadrže.

Izvori incidenata i malware-a se često mogu uhvatit koristeći se artefaktima koji se nalaze u browseru. Od povijesti pretraživanja pa sve do preuzetih datoteka, browseri imaju ključnu ulogu u svakoj forenzičkoj analizi.

Kada pričamo o artefaktima u browseru, oni su zapravo sve ono što neki browser sprema u posebne foldere u operacijskom sustavu. Ovisno o kojem je browseru riječ, svaki ima svoja pravila gdje sprema i kako imenuje te artefakte, ali su oni u principu uvijek isti tip podataka.

Neki od uobičajenih artefakata su:

* **Povijest pretraživanja** – sadrži podatke o stranicama koje je korisnik posjećivao
* **„Autocomplete“ podaci** – podaci koje browser predlaže na osnovu onoga što korisnik najčešće pretražuje
* **Bookmarks**
* **Ekstenzije i Addon-i**
* **Cache** – podaci koji se spremaju radi, najčešće, bržeg učitavanja. Cache podaci mogu biti raznih vrsti, poput slika, javascript datoteka itd.
* **Logins**
* **Downloads**

U ovom radu je fokus na analizi povijesti pretraživanja. Cilj je iz artefakata browsera izvući podatke i napraviti statistiku posjećivanja web stranica. U radu je korišten jedan od najpopularnijih pretraživača danas – Google Chrome

# Chrome iz forenzičke perspektive

## Problematika

Sigurnost i forenzika web preglednika, poput Google Chromea, predstavljaju ključne aspekte za očuvanje privatnosti i zaštite korisničkih podataka. Povijest pretraživanja igra ključnu ulogu u ovom kontekstu, budući da ona otkriva informacije o internetskim aktivnostima korisnika tijekom vremena.

Google Chrome je jedan od najpopularnijih web preglednika koji se ističe po brzini, jednostavnosti i integraciji s raznim Google uslugama. Međutim, korisnici često zaboravljaju da preglednik čuva podatke o njihovim aktivnostima u obliku povijesti pretraživanja. Svaka posjećena web stranica, pretraživanje ili uneseni podaci zabilježeni su i pohranjeni u povijesti, olakšavajući korisnicima kasniji pristup stranicama koje su posjetili.

S aspekta sigurnosti, ova povijest pretraživanja može predstavljati ozbiljan izazov, posebno ako neovlašteni korisnici imaju pristup računalu ili uređaju s instaliranim preglednikom. Zlonamjerni pojedinci ili kibernetički napadači mogu iskoristiti tu ranjivost kako bi pristupili osjetljivim podacima korisnika, poput osobnih informacija, lozinki ili bankovnih podataka.

Forenzička analiza povijesti pretraživanja postaje ključna u slučajevima istraživanja kibernetičkih incidenata, sumnjivih aktivnosti ili pravosudnih postupaka. Stručnjaci za forenziku web preglednika mogu ekstrahirati, analizirati i interpretirati podatke iz povijesti pretraživanja kako bi otkrili tragove kriminalnih radnji, digitalnih dokaza ili potencijalnih prijetnji sigurnosti.

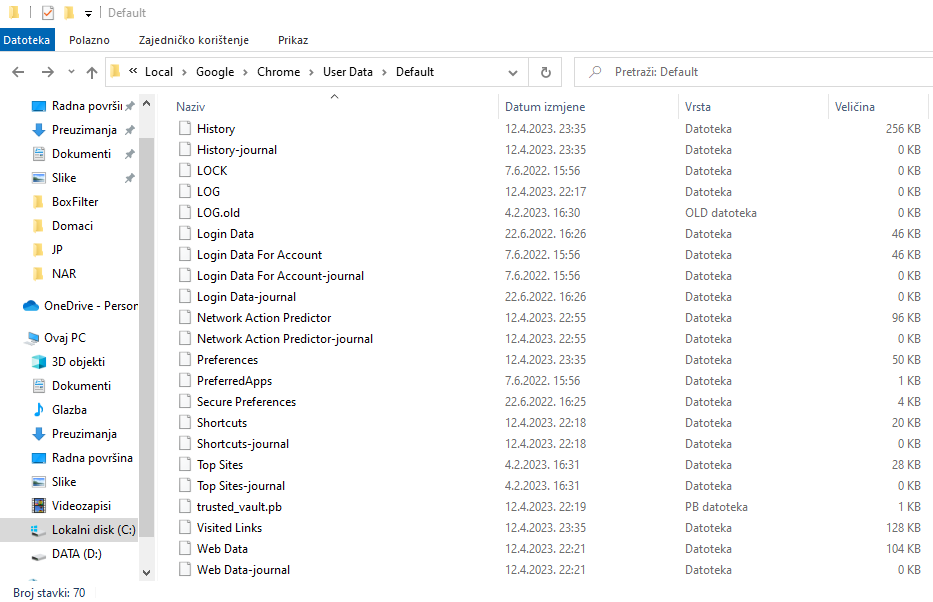
U cilju zaštite korisnika i očuvanja privatnosti, Google Chrome i drugi moderni preglednici uvode napredne sigurnosne značajke koje omogućuju korisnicima da kontroliraju koliko podataka preglednik bilježi i kako s njima postupa. Istovremeno, razvijaju se i alati za forenzičku analizu kako bi se osiguralo da istražitelji i stručnjaci za sigurnost mogu učinkovito raditi u sučelju između privatnosti korisnika i otkrivanja potencijalnih prijetnji.

Uzimajući u obzir rastući broj kibernetičkih prijetnji i važnost privatnosti na internetu, razumijevanje sigurnosti i forenzike Google Chromea postaje ključno za sve korisnike i stručnjake u području informacijske sigurnosti i digitalne forenzike.

## Pohrana

Chrome preglednik pohranjuje artefakte o povijesti pretraživanja na različitim lokacijama na računalu korisnika. Ovi artefakti uključuju datoteke koje sadrže informacije o posjećenim web stranicama, URL-ovima, vremenskim oznakama i drugim metapodacima vezanim uz pretraživanje.

Jedno od ključnih mjesta gdje se ti artefakti mogu pronaći je SQLite baza podataka koja se koristi za pohranjivanje povijesti pretraživanja. Ova baza podataka nalazi se u korisničkom direktoriju u mapi AppData (na Windows operativnim sustavima) ili u direktoriju ~/Library/Application Support/Google/Chrome (na macOS sustavima). Unutar ove baze podataka, tablice poput "urls", "keyword\_search\_terms" i "visits" sadrže informacije o povijesti pretraživanja.



Slika 2.1 - Chrome artefakti

Osim SQLite baze podataka, Chrome također koristi datoteke poput "History" i "Archived History" koje su zapisane u obliku datoteka baze podataka. Ove datoteke obično se nalaze u istim direktorijima kao i SQLite baza podataka. Također, Chrome koristi datoteku "Last Tabs" kako bi pohranio informacije o posljednje otvorenim karticama u pregledniku.

## Mjere zaštite

Zaštita korisničkih podataka u Google Chromeu je ključna kako bi se osigurala privatnost i sigurnost korisnika. Evo nekoliko načina na koje korisnici mogu zaštititi svoje podatke u Chrome pregledniku:

1. Redovito ažuriranje: Održavanje Chrome preglednika ažurnim s najnovijim sigurnosnim zakrpama i ažuriranjima može pomoći u zaštiti od poznatih sigurnosnih propusta. Redovito provjeravajte dostupnost novih ažuriranja i instalirajte ih što je prije moguće.
2. Upotreba snažne lozinke: Korištenje snažne lozinke za Chrome račun može otežati neovlašten pristup vašim podacima. Lozinka bi trebala biti kombinacija slova, brojeva i posebnih znakova te biti jedinstvena za Chrome račun.
3. Omogućavanje dvofaktornog provjere: Dvofaktorni provjeru dodaje dodatni sloj sigurnosti pri prijavi u Chrome račun. Osim unosa lozinke, korisnik će morati pružiti dodatni oblik autentifikacije, poput jednokratnog koda poslanog putem SMS-a ili upotrebe autentifikacijske aplikacije.
4. Kontrola postavki privatnosti: Chrome pruža opcije za upravljanje postavkama privatnosti. Korisnici mogu kontrolirati koliko informacija preglednik pohranjuje, poput povijesti pretraživanja, kolačića i privremenih datoteka. Preporučuje se pregledavanje i prilagođavanje tih postavki prema vlastitim preferencijama.
5. Korištenje privatnog načina rada: Chrome ima način rada zvan "Incognito" ili "Privatni pregled". U ovom načinu rada preglednik ne pohranjuje povijest pretraživanja, kolačiće ili privremene datoteke. Privatni način rada koristan je kada korisnici žele provesti pretraživanje bez ostavljanja tragova na računalu.
6. Provjera i upravljanje proširenjima: Korisnici trebaju pregledati i upravljati instaliranim proširenjima u Chrome pregledniku. Nepoznata ili sumnjiva proširenja mogu predstavljati rizik za sigurnost podataka. Preporučuje se uklanjanje nepotrebnih proširenja i povremena provjera autentičnosti i recenzija proširenja prije instalacije novih.
7. Korištenje sigurnih mreža i VPN-a: Kada koristite Chrome na javnim mrežama, preporučuje se korištenje sigurnih Wi-Fi mreža i virtualnih privatnih mreža (VPN) kako bi se enkriptirali podaci koji putuju između računala i web stranica koje posjećujete.
8. Upotreba sigurnih web stranica: Budite oprezni prilikom pristupa web stranicama koje zahtijevaju unos osjetljivih podataka poput lozinki ili financijskih informacija. Provjerite ima li web stranica ikonu zaključanog lokota (SSL certifikat) i koristite samo pouzdane i sigurne web stranice.

Ovi koraci mogu pomoći korisnicima u zaštiti njihovih podataka prilikom korištenja Google Chrome preglednika. Međutim, važno je napomenuti da nijedna metoda nije apsolutno sigurna, stoga je uvijek preporučljivo biti svjestan sigurnosnih rizika i paziti na vlastitu privatnost prilikom korištenja interneta.

Bitno je napomenuti da Chrome koristi tehnike enkripcije kako bi zaštitio artefakte pretraživanja. To uključuje šifriranje podataka koji se pohranjuju na računalu korisnika. Enkripcija osigurava da samo ovlašteni korisnik može pristupiti i dešifrirati te podatke.

## Forenzički alati

Forenzički alati za Chrome su specijalizirani softveri ili skupovi tehnika koje koriste stručnjaci za digitalnu forenziku kako bi proučili artefakte pretraživanja i ekstrahirali relevantne podatke za istrage, analize ili oporavak iz Chrome preglednika. Ovi alati pružaju dublji uvid u korisničke aktivnosti, povijest pretraživanja, kolačiće, privremene datoteke i druge artefakte koji su povezani s Chrome preglednikom.Forenzički alati za Chrome mogu pružiti sljedeće funkcionalnosti:

1. Analiza povijesti pretraživanja: Alati za forenziku Chromea omogućuju stručnjacima da analiziraju i rekonstruiraju korisničku povijest pretraživanja. To uključuje informacije o posjećenim web stranicama, pretraživanim pojmovima, vremenskim žigovima i drugim metapodacima koji su povezani s pretraživanjem.

2. Ekstrakcija kolačića: Forenzički alati omogućuju izdvajanje kolačića (eng. cookies) iz Chrome preglednika. Kolačići su male datoteke koje web stranice pohranjuju na računalu korisnika i sadrže informacije o korisničkim sesijama, preferencijama i drugim relevantnim podacima. Analiza kolačića može pružiti uvid u aktivnosti korisnika na web stranicama.

3. Analiza privremenih datoteka: Forenzički alati mogu analizirati privremene datoteke koje Chrome preglednik koristi za pohranjivanje podataka tijekom pregledavanja. To mogu biti slike, skripte, stranice predmemorije (cache) i druge vrste datoteka. Analiza privremenih datoteka može pružiti dodatne informacije o pregledanim web stranicama i aktivnostima korisnika.

4. Rekonstrukcija sesija: Forenzički alati mogu pomoći u rekonstrukciji korisničkih sesija u Chrome pregledniku. Sesija se odnosi na vremenski okvir kada je korisnik bio aktivno povezan s web stranicom ili izvršavao određene radnje. Rekonstrukcija sesija može pomoći u razumijevanju korisničkih aktivnosti, interakcija s web stranicama i identifikaciji relevantnih podataka.

5. Analiza proširenja: Chrome preglednik podržava proširenja, dodatne softverske komponente koje pružaju dodatne funkcionalnosti. Forenzički alati mogu analizirati instalirana proširenja kako bi identificirali njihove funkcije, aktivnosti i potencijalne sigurnosne rizike.

Važno je napomenuti da su svi ovi alati namijenjeni stručnjacima za digitalnu forenziku i zahtijevaju odgovarajuće znanje i vještine za njihovu primjenu.

# Implementacija

## Motivacija

Motivacija izrade projekta je pokazati koliko forenzičar može saznati o korisniku iz datoteke „History“ koju sprema Chrome. Back-end projekta je realiziran u python programskom jeziku te je zadužen za analizu datoteke te pripremu podataka u JSON formatu. Podaci se čitaju na front-endu koji je napravljen u Angular frameworku.

## Struktura projekta

U ovom poglavlju ćemo razraditi datoteke koje se nalaze u projektu, te analizirati pojedinačno što rade i kod koji je napisan u njima. Source datoteka projekta izgleda kao na sljedećoj slici.

A picture containing text, screenshot, software, multimedia software

Description automatically generated

Slika 2 - Struktura projekta

* \_pycache\_ - datoteka koja se automatski kreira od strane python kompajlera i ubrzava rad programa
* GUI – datoteka koja sadrži kompletan Angular kod (typescript), detaljnije obrađena u nastavku
* data.html i data.json – pomoćne datoteke zadužene za prijenos podataka od back-enda do front-enda
* script.js – pomoćna datoteka za data.html
* main.py – sadrži python main funkciju, ovdje se pokreće sama aplikacija, u njoj se nalaze „helper“ funkcije
* helperFunctions.py – funkcije zadužene za analizu history datoteke
* History – lokalna kopija history baze podataka koju zapisuje Chrome, napravljena kako bi se izbjegao „concurrency error“ u slučaju da je Chrome pokrenut

## Back-end

Back-end projekta je pisan u programskom jeziku Python, te se cjelokupno nalazi u dvije datoteke: main.py i helperFunctions.py. Main.py pokreće program kao konzolnu aplikaciju sa menijem u kojem korisnik (forenzičar) bira opcije. Nakon što se svaka od opcija izvrši aplikacija se vraća u izvorno stanje, tj. originalni meni.

A picture containing text, screenshot, font, software

Description automatically generated

Slika 3 - main.py menu

Opcije su sljedeće:

1. Analyse history file – zadužena za analizu baze podataka, poziva sve „helper“ funkcije te sprema dohvaćene podatke u objekt.
2. Export to JSON – dohvaća objekt, parsira podatke u JSON te ga zapisiva u lokalnu datoteku
3. Open analysis file – otvara html stranicu koja predstavlja analizirane podatke

Osim main.py spomenili smo i helperFunctions.py datoteku. Ona sadrži nekolicinu pomoćnih funkcija koje se pozivaju iz main-a, svaka od njih prati sljedeću strukturu: otvori database connection, pogledaj što piše u stupcima u tablici, spremi te podatke u željeni format te naposlijetku zatvori database connection. Primjer jedne od funkcija je na sljedećoj slici.

A screen shot of a computer program

Description automatically generated with low confidence

Slika 4 - Calculate\_top\_visits helper funkcija

## Front-end

Front-end dio aplikacije je pisan u Angular framework-u koji je odabran zbog svoje jednostavnosti u prikazu komponenti koje se mijenjaju u realnom vremenu. Aplikacija ima dvije komponente vrijedne spomena, to su dugme koje pokreće spremanje podataka u lokalni GUI folder te analysis komponentu koja je zadužena za prikaz podataka.

Prikaz podataka je izveden na jednostavan način uz pomoć „čistog“ html-a i CSS-a, budući da dizajn nije prioritet ovog projekta.

Struktura projekta prikazana je na sljedećoj slici:

A screenshot of a computer

Description automatically generated

Slika 5 - Struktura front-end aplikacije

Datoteke koje su bitne za projekt su sljedeće (ostale su automatski generirane od strane Angulara CLI-a ili su config datoteke):

* Src/app – sadrži Angular komponente, u ovoj aplikaciji je to samo jedna – analysis
* data.txt – sadrži JSON preuzet iz back-enda zapisan u tekstualnom formatu zbog činjenice da se JSON zbog sigurnosnih razloga i postavki u browseru ne može čitati lokalno osim ako ga ne servira dedicirani server (tj. ako se ne koristi HTTP metoda)
* userData.ts – sadrži interface za objekt koji se koristi za prikaz podataka

Typescript datoteka glavne komponente koja je zadužena za čitanje i prikaz podataka izgleda ovako:

A picture containing text, screenshot, software

Description automatically generated

Slika 6 - analysis.ts komponenta

Najprije se inicijaliziraju potrebne varijable, koje se pune podacima u „hook“ funkciji ngOnInit koja se izvodi čim se komponenta učita na stranici. U njoj se za čitanje podataka koristi HTTP get metoda na koju se pretplatimo, što znači da će svaka promjena u podacima uzrokovati osvježavanje vrijednosti koje su prikazane na stranici. Ovi podaci se koriste u HTML datoteci za prikaz na sljedeći način:



Slika 7 - HTML za prikaz podataka

# Zaključak

U ovom radu smo obradili glavne karakteristike Web Browsera iz forenzičke perspektive, od vrsti i tipova podataka o korisniku koje čuvaju pa do iskorištavanja tih podataka u svrhu forenzičke analize. Fokus je postavljen na Google Chrome, jedan od najpopularnijih pretraživača danas, koji je kao takav detaljnije obrađen u tekstu.

U svrhu demonstracije napravljen je i praktični dio koji čita „History“ SQL bazu podataka koju Chrome zapisuje na lokalnoj mašini te analizira pročitane podatke i prikazuje ih u obliku web stranice (koristeći HTML).

Iz analize se može zaključiti da se u današnje vrijeme u modernim Web Browserima svaka korisnička aktivnost negdje zapisuje, pa je veoma teško ostati anoniman ili sakriti svoje postupke, bili oni legalni u vidu forenzičkog istraživanja ili ilegalni.