

Seminarski rad

Predmet: Digitalna forenzika

Tema: Digitalna forenzika društvenih mreža

|  |  |
| --- | --- |
| Student: |  |
| Jelena Đikić, br.ind. 1488 |  |

Niš, april 2024. godina

Sadržaj

[1. Uvod 3](#_Toc162203953)

[2. Pojam digitalne forenzike 4](#_Toc162203954)

[2.1. Podoblasti digitalne forenzike 4](#_Toc162203955)

[3. Digitalna forenzika društvenih mreža 7](#_Toc162203956)

[3.1. Ograničenja sa kojima se susreće digitalna forenzika društvenih mreža 8](#_Toc162203957)

[3.2. Potrebne funkcionalnosti digitalne forenzike društvenih mreža 8](#_Toc162203958)

[3.3. Trenutno aktuelno stanje u digitalnoj forenzici društvenih mreža 9](#_Toc162203959)

[3.4. Pregled postojećih softverskih rešenja 10](#_Toc162203960)

[3.4.1. Jatheon 11](#_Toc162203961)

[3.4.2. WebPreserver 13](#_Toc162203962)

[3.4.3. Pipl 13](#_Toc162203963)

[3.4.4. Social Links 14](#_Toc162203964)

[3.4.5. Makeawebsitehub 14](#_Toc162203965)

[3.4.6. TinEye 15](#_Toc162203966)

[3.5. Koraci u postupku digitalne forenzike društvenih mreža 15](#_Toc162203967)

[4. Praktična implementacija alata za analizu i vizuelizaciju zavisnosti na Twitter-u 18](#_Toc162203968)

[4.1. Preuzimanje arhiva podataka sa Twitter naloga 18](#_Toc162203969)

[4.2. Analiza podataka 19](#_Toc162203970)

[4.2.1. Analiza i vizuelizacija zavisnosti između kontakata na Twitter-u 20](#_Toc162203971)

[4.2.2. Generisanje izveštaja o konverzacijama korisnika 25](#_Toc162203972)

[4.2.3. Vizuelizacija statistike aktivnosti (broj objavljenih postova) 27](#_Toc162203973)

[4.2.4. Pretraga objavljenih tvitova po ključnoj reči 29](#_Toc162203974)

[5. Zaključak 31](#_Toc162203975)

[6. Literatura 31](#_Toc162203976)

# Uvod

Ovaj rad istražuje digitalnu forenziku kao disciplinu koja se bavi proučavanjem, analizom i istraživanjem digitalnih uređaja i podataka radi pronalaženja dokaza koji se mogu koristiti u pravnom ili istražnom kontekstu. U današnjem digitalnom dobu, gde se gotovo sve aktivnosti odvijaju online, digitalna forenzika postaje sve važnija za otkrivanje, istraživanje i rešavanje različitih kriminalnih i neetičkih aktivnosti.

Pojam digitalne forenzike obuhvata širok spektar metoda, tehnika i alata koji se koristi za prikupljanje, analizu i interpretaciju digitalnih podataka. Ova disciplina je primenjena na različite vrste digitalnih medija, uključujući računare, mobilne uređaje, memorijske kartice, ali i društvene mreže.

U kontekstu digitalne forenzike društvenih mreža, fokus je na istraživanju aktivnosti i komunikacije korisnika na platformama kao što su Twitter, Facebook, Instagram i drugi. Ova podoblast digitalne forenzike suočava se sa specifičnim izazovima i ograničenjima, kao što su brzina promene podataka, privatnost korisnika, kao i kompleksnost algoritama i tehnologija koje se koriste na društvenim mrežama.

U ovom radu istražena su ograničenja sa kojima se susreće digitalna forenzika društvenih mreža, kao i potrebne funkcionalnosti i trenutno aktuelno stanje u ovoj oblasti. Takođe, da je pregled postojećih softverskih rešenja koja se koriste za analizu podataka sa društvenih mreža, uključujući alate poput Jatheon, WebPreserver, Pipl, Social Links, Makeawebsitehub i TinEye.

U praktičnom delu rada, fokus je na implementaciji alata za analizu i vizualizaciju zavisnosti na Twitter-u. Koraci u postupku digitalne forenzike društvenih mreža, uključujući preuzimanje arhive podataka sa Twitter naloga, analizu podataka i generisanje izveštaja, detaljno su opisani i prikazani kroz praktične primere.

# Pojam digitalne forenzike

Digitalna forenzika, koja se često naziva kompjuterska forenzika, je grana forenzičke nauke koja se fokusira na oporavak, istraživanje i analizu digitalnih podataka sa elektronskih uređaja i digitalnih medija u cilju prikupljanja dokaza u pravne svrhe. Ova oblast se prvenstveno bavi identifikacijom, očuvanjem, ispitivanjem i prezentacijom digitalnih dokaza na način koji je prihvatljiv na sudu.

Digitalna forenzika se primenjuje u širokom spektru scenarija, uključujući:

* Kriminalne istrage - Digitalni dokazi mogu biti ključni u slučajevima koji uključuju sajber zločine, prevaru, hakovanje, krađu intelektualne svojine i još mnogo toga.
* Građanski sporovi - Koristi se u građanskim predmetima, kao što su sporovi oko intelektualne svojine, sporovi o zapošljavanju i elektronsko otkrivanje (e-otkrivanje) u pravne svrhe.
* Odgovor na incidente - U sajber bezbednosti, digitalna forenzika se koristi za istraživanje i reagovanje na kršenje bezbednosti i podataka.
* Korporativne istrage - Preduzeća koriste digitalnu forenziku da istraže nedolično ponašanje zaposlenih, interne prevare i kršenja podataka.
* Sprovođenje zakona - Agencije za sprovođenje zakona koriste tehnike digitalne forenzike za prikupljanje dokaza u vezi sa različitim kriminalnim aktivnostima.

Stručnjaci za digitalnu forenziku igraju vitalnu ulogu u pomaganju agencijama za sprovođenje zakona i organizacijama da otkriju i analiziraju digitalne dokaze, obezbeđujući da pravda bude zadovoljena i da se kršenje podataka i sajber zločini na odgovarajući način rešavaju.

## Podoblasti digitalne forenzike

Digitalna forenzika obuhvata različite specijalizovane oblasti, od kojih se svaka fokusira na određene vrste digitalnih uređaja, tehnologija ili istražne svrhe. Neke od istaknutih potkategorija digitalne forenzike uključuju:

1. Računarska forenzika

Ovo je najpoznatija potkategorija, koja se bavi ispitivanjem računara (stonih računara, laptopova, servera) i njihovih uređaja za skladištenje podataka. Uključuje analizu podataka, operativnih sistema, sistema datoteka i aplikacija za oporavak dokaza.

2. Forenzika mobilnih uređaja

Mobilna forenzika se fokusira na pametne telefone, tablete i druge prenosive uređaje. To uključuje izdvajanje podataka sa ovih uređaja, uključujući evidencije poziva, tekstualne poruke, fotografije, GPS informacije i podatke aplikacija. To je ključno u istrazi zločina koji uključuju mobilnu tehnologiju.

3. Mrežna forenzika

Mrežna forenzika uključuje praćenje i analizu mrežnog saobraćaja i paketa podataka radi otkrivanja bezbednosnih incidenata, upada i sajber napada. Pomaže u razumevanju obima i uticaja incidenata povezanih sa mrežom.

4. Forenzika memorije

Ovo potpolje uključuje analizu nestabilne memorije (RAM) računara ili uređaja da bi se identifikovali pokrenuti procesi, otvorene datoteke, ključevi za šifrovanje i artefakti zlonamernog softvera. Forenzika memorije može biti neophodna u istraživanju naprednih sajber napada.

5. Forenzička analiza podataka

Ovo uključuje ispitivanje i analizu velikih skupova podataka i baza podataka da bi se otkrili obrasci, anomalije i dokazi u vezi sa finansijskim prevarama, sajber zločinima i drugim istragama zasnovanim na podacima.

6. Digitalna forenzika slika

Stručnjaci za digitalnu forenziku kreiraju forenzičke slike ili kopije digitalnih uređaja i medija za skladištenje kako bi sačuvali i analizirali podatke uz održavanje njihovog integriteta. Ovo je fundamentalni proces u mnogim digitalnim forenzičkim istragama.

7. Forenzika u oblaku

Uz sve veću upotrebu usluga računarstva u oblaku, forenzika u oblaku se fokusira na prikupljanje dokaza sa platformi zasnovanih na oblaku, kao što su Amazon Veb Services (AVS), Microsoft Azure, Google Cloud i SaaS (softver kao a Service) aplikacije.

8. Forenzika ugrađenih uređaja

Ovo potpolje se bavi analizom digitalnih uređaja ugrađenih u različite sisteme, uključujući uređaje Interneta stvari (IoT), automobilske sisteme i industrijske kontrolne sisteme (ICS).

9. Audio i video forenzika

Stručnjaci u ovoj oblasti analiziraju audio i video snimke da bi potvrdili autentičnost, poboljšali ili razjasnili dokaze digitalnih medija. Ovo se često koristi u krivičnim istragama, nadzoru i autentifikaciji multimedijalnog sadržaja.

10. Forenzičko računovodstvo i finansijska analiza

Fokusirajući se na istrage finansijskih prevara, ova potkategorija uključuje analizu finansijskih zapisa, transakcija i podataka elektronskog bankarstva kako bi se otkrili dokazi o pronevjeri, pranju novca i kriminalnim radnjama.

11. Forenzička analiza e-pošte

Ova oblast uključuje ispitivanje komunikacije putem e-pošte radi praćenja identiteta pošiljaoca, analize zaglavlja e-pošte, vraćanja izbrisanih e-poruka i identifikovanja dokaza vezanih za e-poštu u sajber kriminalu i korporativnim istragama.

12. Forenzika društvenih medija

Uz široku upotrebu platformi društvenih medija, ovo potpolje se fokusira na prikupljanje i analizu podataka društvenih medija da bi se istražilo maltretiranje, uznemiravanje, onlajn pretnje i digitalni otisci.

13. Automatizovana digitalna forenzika

Nove tehnologije, kao što su veštačka inteligencija (AI) i mašinsko učenje, sve se više koriste u digitalnoj forenzici za automatizaciju analize podataka i efikasnije identifikovanje obrazaca i anomalija.

Ove potkategorije digitalne forenzike zadovoljavaju specifične istražne potrebe i vrste digitalnih dokaza, odražavajući raznovrsnu i evoluirajuću prirodu sajber kriminala i digitalnih tehnologija. Stručnjaci za digitalnu forenziku se često specijalizuju u jednoj ili više ovih oblasti na osnovu svoje stručnosti i zahteva svojih istraga.

# Digitalna forenzika društvenih mreža

Digitalna forenzika društvenih mreža postaje sve značajnija u digitalnom dobu, gde su društvene mreže postale ključni kanal za komunikaciju, interakciju i deljenje informacija među korisnicima. Motivacija za istraživanje i implementaciju alata za analizu i vizualizaciju zavisnosti između kontakata na socijalnim mrežama, kao što su Twitter ili Facebook, proizilazi iz nekoliko ključnih faktora.

Prvo, u današnjem digitalnom svetu, društvene mreže su postale nezaobilazni deo svakodnevnog života miliona ljudi širom sveta. Korisnici aktivno koriste ove platforme za razmenu informacija, uspostavljanje konekcija i izražavanje svojih stavova. Stoga, analiza ponašanja korisnika na ovim platformama postaje važna kako bi se razumela njihova interakcija, socijalni odnosi i aktivnosti.

Raznovrsnost društvenih mreža, poput Facebooka, Twittera i Instagrama, pruža različite forme interakcije i sadržaja korisnicima. Svaka mreža ima svoje specifičnosti, od tekstualnih i slikovnih postova do razmene direktnih poruka među korisnicima. Svi ovi oblici komunikacije stvaraju digitalne dokaze koji mogu biti ključni u digitalnoj forenzici.

Sa porastom broja korisnika društvenih mreža, raste i broj kriminalnih aktivnosti koje se odvijaju na ovim platformama. Od lažnih profila i prevara, do cyberbullyinga i terorističke propagande, društvene mreže su postale prostor za različite oblike zloupotrebe. Stoga, alati za digitalnu forenziku društvenih mreža postaju neophodni za detekciju, analizu i suzbijanje ovih aktivnosti.

U pravosudnom sistemu, digitalni dokazi dobijeni iz društvenih mreža postaju sve važniji u procesu istrage i suđenja. Analiza zavisnosti između kontakata može pružiti uvid u komunikaciju između osoba, njihove međusobne veze i aktivnosti na platformi. Vizualizacija ovih podataka u obliku grafova i statistika omogućava istražiteljima da bolje razumeju situaciju i pravilno interpretiraju dokaze.

Razvoj naprednih tehnologija za analizu podataka i vizualizaciju omogućava efikasno procesuiranje velike količine informacija sa društvenih mreža. Implementacija alata koji može automatski analizirati i vizualizovati zavisnosti između kontakata može znatno olakšati rad istražiteljima i pružiti im dragocene uvide u digitalne forenzičke analize.

Uzimajući u obzir ove faktore, motivacija za istraživanje i implementaciju alata za forenziku socijalnih mreža postaje sve važnija kako bi se omogućilo efikasno reagovanje na digitalne izazove i pružila podrška pravosudnom sistemu u borbi protiv kriminalnih aktivnosti na internetu. [3]

## Ograničenja sa kojima se susreće digitalna forenzika društvenih mreža

Ograničenja u oblasti digitalne forenzike društvenih mreža su neizbežna i zahtevaju pažljivo razmatranje kako bi se postigla pouzdanost i tačnost analiza. Prvo ograničenje predstavlja složenost prikupljanja podataka sa društvenih mreža, posebno u slučaju ograničenog pristupa podacima zbog privatnosti korisnika ili zakonskih regulativa. Osim toga, brz tempo promena na društvenim mrežama često dovodi do problema sa ažuriranjem alata i tehnika za digitalnu forenziku, što može dovesti do zastarelih ili nepotpunih rezultata istraživanja.

Sledeće ograničenje proizlazi iz kompleksnosti analize podataka sa društvenih mreža, gde se susrećemo sa velikim količinama nepovezanih informacija koje zahtevaju sofisticirane tehnike obrade i interpretacije. Ovo može dovesti do poteškoća u identifikaciji relevantnih digitalnih dokaza i otežati njihovo adekvatno tumačenje. Takođe, variranje u načinu predstavljanja podataka na različitim društvenim mrežama dodatno komplikuje proces analize i interpretacije.

Još jedno ograničenje odnosi se na izazove u autentičnosti i integritetu digitalnih dokaza. Budući da korisnici društvenih mreža mogu manipulisati svojim profilima i objavama, postoji rizik od falsifikovanja ili izmena dokaza, što može dovesti do netačnih ili pristrasnih rezultata forenzičke analize. Pored toga, brisanje ili modifikacija digitalnih dokaza od strane korisnika takođe predstavlja značajan izazov za istražitelje.

Konačno, nedostatak standardizovanih metoda i procedura za digitalnu forenziku socijalnih mreža može dovesti do nedoslednih ili nekompatibilnih rezultata istraživanja. Nedostatak zajedničkih standarda i smernica može otežati upoređivanje i validaciju rezultata između različitih istraživača ili sudskih stručnjaka, čime se smanjuje pouzdanost forenzičkih analiza.

## Potrebne funkcionalnosti digitalne forenzike društvenih mreža

Potrebno je jasno definisati i implementirati odgovarajuće funkcionalnosti alata za analizu i vizualizaciju podataka. Pravilno odabrane funkcionalnosti treba da omoguće efikasno prikupljanje, obradu i interpretaciju digitalnih dokaza sa društvenih mreža, uzimajući u obzir složenost, obim i dinamiku podataka.

Prva ključna funkcionalnost odnosi se na sposobnost alata da prikupi podatke sa društvenih mreža na pouzdan i siguran način, uz poštovanje pravila privatnosti i zakonskih regulativa. Ovo uključuje autentifikaciju korisnika, pristup odgovarajućim API-ima društvenih mreža i mehanizme za zaštitu podataka tokom prikupljanja i obrade.

Sledeća bitna funkcionalnost odnosi se na mogućnost analize i obrade velike količine podataka sa društvenih mreža, uz primenu naprednih tehnika obrade podataka i veštačke inteligencije. Alati treba da omoguće identifikaciju relevantnih digitalnih dokaza, analizu interakcija između korisnika, kao i detekciju nepravilnosti ili sumnjivih aktivnosti na platformama.

Neophodna funkcionalnost obuhvata vizualizaciju rezultata analize na jasan i intuitivan način, koristeći grafove, dijagrame i druge vizualne alate. Vizuelizacija podataka omogućava istražiteljima da lakše identifikuju obrasce, trendove i anomalije u ponašanju korisnika na društvenim mrežama, čime se olakšava proces tumačenja digitalnih dokaza.

Konačno, alati za digitalnu forenziku socijalnih mreža trebalo bi da obezbede mogućnost generisanja izveštaja i dokumentacije o rezultatima analize, kako bi se omogućila transparentnost, reprodukcija i validacija forenzičkih nalaza. Ove funkcionalnosti su ključne za postizanje pouzdanih i relevantnih forenzičkih analiza u oblasti društvenih mreža.

## Trenutno aktuelno stanje u digitalnoj forenzici društvenih mreža

Trenutno, digitalna forenzika društvenih mreža suočava se sa sve većim izazovima i promenama u svetu online aktivnosti. Sa porastom broja korisnika na platformama kao što su Twitter, Facebook, Instagram i LinkedIn, takođe dolazi i povećanje različitih oblika kriminalnih aktivnosti. Prevare, cyberbullying, distribucija nelegalnog sadržaja i teroristička propaganda samo su neki od primera zloupotrebe društvenih mreža.

Ovaj rast kriminalnih aktivnosti postavlja potrebu za sveobuhvatnim forenzičkim istraživanjem kako bi se identifikovali počinioci, prikupili dokazi i osigurala sigurnost korisnika. Međutim, prikupljanje digitalnih dokaza sa društvenih mreža može biti izuzetno složeno zbog obima podataka, različitih formata i privatnosti korisnika. Dodatno, promene u algoritmima i pravilima platformi često dodaju složenost ovom procesu.

Pored tehničkih izazova, postoje i pravna pitanja i etičke dileme koje prate forenzička istraživanja na društvenim mrežama. Pitanja privatnosti korisnika, pristupa podacima i korišćenja prikupljenih dokaza u pravosudnim procesima zahtevaju pažljivo razmatranje i poštovanje zakonskih regulativa.

Ipak, uz sve ove izazove, postoji i kontinuirani razvoj tehnologija, alata i metoda za prikupljanje, analizu i interpretaciju digitalnih dokaza sa društvenih mreža. Softverske platforme, algoritmi za analizu podataka, tehnike vizualizacije i alati za otkrivanje i analizu kriminalnih aktivnosti predstavljaju deo napretka u ovoj oblasti. [1], [2]

## Pregled postojećih softverskih rešenja

Iako je istraživanje društvenih medija odlično za prikupljanje dokaza, dolazi sa nizom prepreka koje odbijaju ljude od korišćenja društvenih medija u pravnim slučajevima. Konkretno, prikupljanje dokaza može biti dugotrajno sa svojim brojnim zadacima:

* Obim - Pročešljavanje desetina (ili stotina) kanala društvenih medija za srodne profile
* Ručni rad - Ručno proširivanje odgovora i komentara kako bi se locirala relevantna informacija
* Dokazivanje autentičnosti - Praćenje porekla slike ili datoteka koje se istražuju
* Pravljenje bezbroj snimaka ekrana - Ručno prikupljanje čitavih tvitova, Facebook postova, razgovora ili čitavih naloga kao dokaza

Ovi procesi mogu trajati toliko dugo da sprovođenje istrage jednostavno nije isplativo. Istražitelji mogu da provode dane na društvenim medijima - ali da li bi klijent bio spreman da plati vaše vreme?

Na sreću, postoje alati za istraživanje društvenih medija koji značajno smanjuju zadatke koji se ponavljaju, pa čak i automatizuju prikupljanje podataka. Pomoću ovih alata možete znatno proširiti svoja istraživanja društvenih medija i prikupiti vitalne dokaze mnogo brže pre nego što budu uklonjeni ili uređeni. [1], [2]

Neki od najkorišćeniji alata za i istragu zločina na društvenim medijima su:

* Jatheon
* WebPreserver
* Pipl
* Social Links
* Makeawebsitehub
* TinEye

### Jatheon

 Jatheon je softver za arhiviranje društvenih medija koji se koristi za automatsko snimanje i zadržavanje zvaničnih kanala društvenih medija. Omogućava korisnicima da brzo pretražuju sve glavne zapise društvenih medija sa jednog ekrana sa 20+ naprednih kriterijuma za pretragu. Svi njegovi zapisi na društvenim mrežama su uhvaćeni sa svojim kompletnim metapodacima i zaštićeni naprednom enkripcijom što ih čini potpuno privatnim.

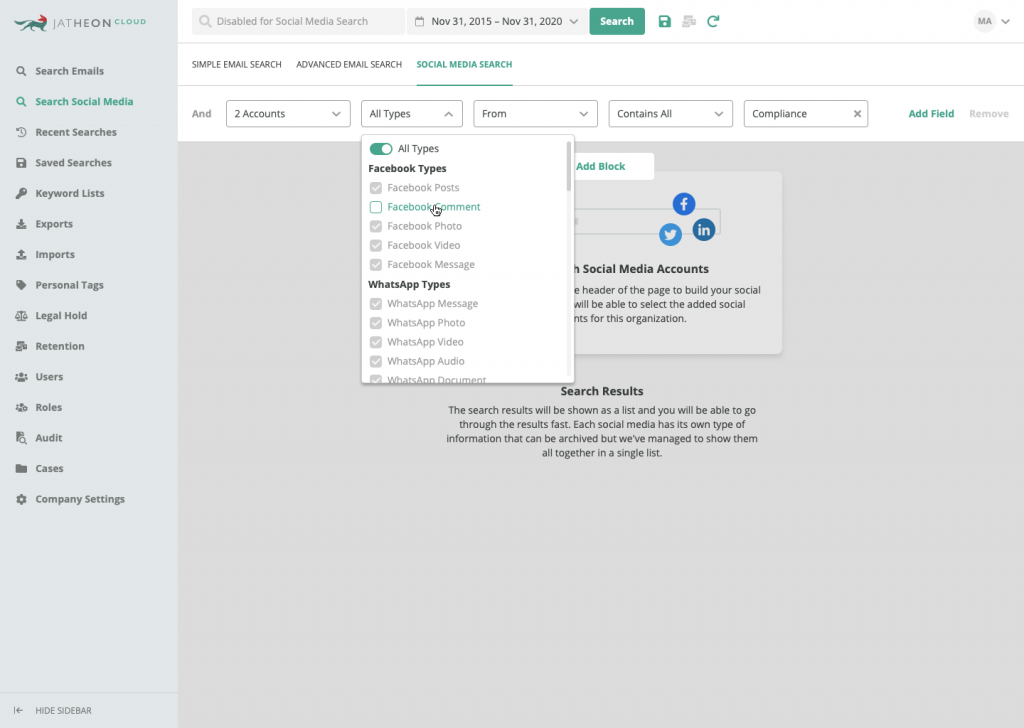
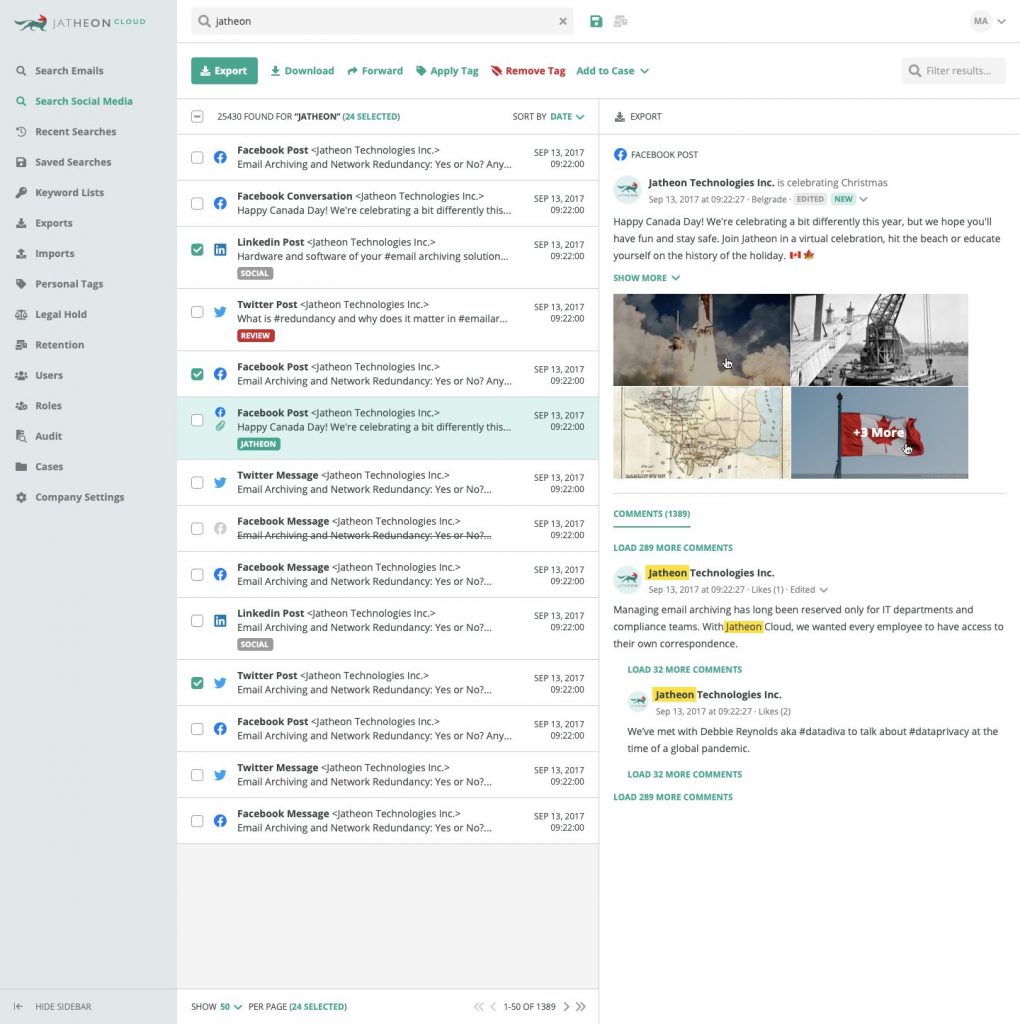
Slika 1. Jatheon logo

Koriste ga pravni timovi, timovi za usklađenost i ljudske resurse za rešavanje sporova i slučajeva nedoličnog ponašanja zaposlenih, za dokazivanje usklađenosti sa zakonima o zadržavanju društvenih medija koje je nametnula vlada, kao i za podršku otkrivanju društvenih medija pomoću autentičnih zapisa.

Jatheonovo rešenje povezuje se sa nalogom na društvenim mrežama (Facebook, Instagram, LinkedIn ili Tvitter) i snima sve postove, komentare, odgovore, multimediju itd. (u zavisnosti od društvene mreže), uključujući sve izmene ili izbrisane postove/poruke. Na slici 2 može se videti odabir uvoza podataka sa konkretne društvene mreže.

Jednom snimljen, omogućava naprednu pretragu sa 20+ filtera i prilagođenih formula da biste pronašli tačno ono što tražite.

Još jedna dodatna prednost Jatheona je to što ima integrisanu funkciju redigovanja, tako da je lako redigovati osetljive i lične informacije pre nego što izvezete zapise na pregled. [1], [2]



Slika 2. Jatheon – odabir tipa podataka koji će se snimiti [1]

Slika 3. Jatheon – prikaz preuzetih objava [1]

### WebPreserver

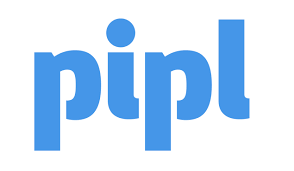
 WebPreserver je automatizovani alat za forenzičko očuvanje društvenih medija koji može prikupiti nedelje dokaza za samo sat vremena. Njegova funkcija automatskog proširenja automatski proširuje dugačke skupljene članke, niti komentara i odgovore, osiguravajući da se zakopani materijal snimi bez potrebe da ručno širite ove oblasti.

Slika 4. Web preserver logo

Kada se dokaz pronađe, WebPreserver omogućava lak izvoz navedenih dokaza u različite formate datoteka kao što su OCR PDF ili WARC, štedeći vreme na ručnim snimcima ekrana.

Kao dodatak zasnovan na pretraživaču, WebPreserver je kompatibilan sa korisnicima Chrome-a i Edge-a. Može se preuzeti sa Chrome veb prodavnice, ali da bi se koristio, korisnik mora da kupi licencu sa zvaničnog veb-sajta. [1], [2]

### Pipl

 Pipl je verovatno najnapredniji lični pretraživač dostupan istražiteljima društvenih medija. Pipl prikuplja podatke iz javnih dokumenata, malih oglasa, listinga, imenika i onlajn arhiva na Internetu, ali ima i svoje ekskluzivne izvore podataka.

Slika 5. Pipl logo

Sa preko tri milijarde onlajn identiteta (telefonskih brojeva i adresa e-pošte) i 25 milijardi pojedinačnih identifikacionih zapisa na raspolaganju, sa sigurnošću se može reći da Pipl ima pokrivenost širom sveta kada je u pitanju istraživanje društvenih medija.

Za početak, Pipl zahteva jednu tačku podataka o osobi koju tražite i ona će vam pružiti sve dostupne informacije, od njihovih naloga na društvenim mrežama do zaposlenja i istorije obrazovanja. [1], [2]

### Social Links

 Social Links objedinjuje podatke sa društvenih medija, aplikacija za razmenu poruka i blok lanaca omogućavajući uvid u digitalni otisak osobe na vizuelno privlačan način.

Slika 6. Social Links logo

Unosom jedne tačke podataka, korisnik može da generiše veze između date osobe i onoga što radi na internetu. Svaki korak u procesu istraživanja otkriva više informacija o osobi kao što su njeni nalozi, prijatelji/veze, lični podaci, postovi, lajkovi i mnoge druge informacije. [1], [2]

### Makeawebsitehub

Iako se može činiti da platforme kao što su Facebook, Instagram, Twitter i Youtube dominiraju scenom društvenih medija, nove aplikacije i platforme se stalno razvijaju.



Slika 7. Makeawebsitehub logo

Makeawebsitehub rutinski održava listu najnovijih aplikacija, što može biti veoma korisno za proširenje internet istraživanja i lociranje onih manje poznatih sajtova koji možda kriju važne podatke.

Ljudi koji pokušavaju da nanesu drugima štetu ili nešto nezakonito obično komuniciraju na platformama kojih niko nije svestan. Sa Makeawebsitehub-ovom listom, dobija se ideja o tome gde bi se ova komunikacija mogla odvijati i koristiti druge alate za pronalaženje dokaza. [1], [2]

### TinEye

 TinEye je jednostavan, ali efikasan alat za praćenje originalnih slika i obrnutih pretraga slika. Samo treba da otpremite sliku na TinEye, a aplikacija će pronaći sva mesta na kojima se pojavljuje na Internetu. Pomaže u lociranju izvora internetske slike, obrnuto pretraživanje slika.

Slika 8. TinEye logo

Ako se određena slika pojavi na Facebook profilu, možete koristiti TinEye da otkrijete gde se ta slika još koristi na mreži, uključujući druge platforme društvenih medija kao što su YouTube, Pinterest ili Twitter. [1], [2]

## Koraci u postupku digitalne forenzike društvenih mreža

Proces forenzike društvenih medija uključuje niz sistematskih koraka za prikupljanje, očuvanje, analizu i predstavljanje digitalnih dokaza sa platformi društvenih mreža. Evo ključnih koraka uključenih u forenziku društvenih medija:

1. Identifikacija slučaja i ciljeva

Prvo je neophodno odrediti prirodu i obim slučaja koji zahteva forenziku društvenih medija. Zatim treba definisati specifične ciljeve istrage, kao što je identifikacija sajber nasilnika, prikupljanje dokaza za klevetu ili praćenje pretnji na mreži.

2. Pravna i etička razmatranja

Potrebno je obezbediti usklađenost sa zakonskim zahtevima i pribaviti neophodne dozvole ili naloge za prikupljanje podataka. Neophodno je pridržavati se etičkih smernica, poštujući privatnost korisnika i zakone o zaštiti podataka.

3. Prikupljanje podataka

Podrazumeva identifikovanje relevantnih platformi društvenih medija i korisničkih naloga povezanih sa slučajem. Koriste se specijalizovani forenzički alati i tehnike za prikupljanje podataka sa ovih platformi. Ovo može uključivati web-scraping, pristup API-ju ili druge metode. Neophodno je snimiti informacije kao što su profili korisnika, postovi, komentari, poruke, slike, video snimci i metapodaci.

4. Očuvanje dokaza

Neophodno je napraviti forenzičke kopije ili slike prikupljenih podataka društvenih medija da bi se sprečilo neovlašćeno menjanje. Zatim je potrebno uspostaviti lanac nadzora za praćenje rukovanja i čuvanja dokaza.

5. Obrada i priprema podataka

Podrazumeva organizovanje i katalogiziranje prikupljenih podataka, obezbeđujući da su pravilno označeni i kategorisani. Potrebno je normalizovati i očistiti podatke, uklanjajući nebitne ili duplirane informacije.

6. Analiza podataka

Treba analizirati sadržaj društvenih medija da bi se identifikovale relevantne informacije i obrasci. Traže se ključne reči, hashtagovi i interakcije korisnika u vezi sa slučajem. Neophodno je proceniti kredibilitet korisničkih profila i autentičnost sadržaja.

7. Pripisivanje korisnika

Utvrditi identitet korisnika društvenih medija koji su uključeni u slučaj. Treba povezati onlajn ličnosti sa stvarnim pojedincima kroz različite istražne tehnike, kao što je praćenje IP adresa ili unakrsne reference sa drugim digitalnim dokazima.

8. Analiza metapodataka

Podrazumeva ispitivanje metapodatka povezanih sa sadržajem društvenih medija da bi se utvrdili vremenski okviri, lokacije i informacije o uređaju. Takođe treba proceniti da li su metapodaci u skladu sa narativom slučaja.

9. Provera autentičnosti sadržaja

Provera autentičnosti digitalnog sadržaja, kao što su slike i video snimci, da bis se potvrdilo da li je njima manipulisano ili su menjani. Potrebno je koristiti specijalizovani softver i alate za analizu digitalnog sadržaja.

10. Generisanje izveštaja

Potrebno je napraviti sveobuhvatne izveštaje koji dokumentuju nalaze, metodologiju analize i zaključke. Uključiti relevantne snimke ekrana, snimke podataka i informacije o metapodacima u izveštaj.

11. Veštačenje

Ako je potrebno, treba se pripremiti da se pruži veštačenje na sudu, objašnjavajući nalaze i značaj dokaza na društvenim mrežama za slučaj.

12. Pravni postupci

Potrebno je sarađivati sa agencijama za sprovođenje zakona, pravnim stručnjacima ili drugim zainteresovanim stranama kako bi se podržala pravnu akcija ili zaštitne mere na osnovu dokaza.

13. Dokumentacija i arhiviranje

Potrebno je održavati detaljnu evidenciju o celom procesu forenzike društvenih medija, uključujući metode prikupljanja podataka i komunikacije u vezi sa slučajem. Takođe, treba arhivirati sve dokaze i izveštaje za buduću upotrebu i potencijalne žalbe.

Važno je napomenuti da specifični koraci i metodologije koje se koriste u forenzici društvenih medija mogu varirati u zavisnosti od prirode slučaja, uključenih platformi i dostupnih alata i resursa. Pored toga, održavanje integriteta dokaza i pridržavanje pravnih i etičkih standarda su kritični tokom celog procesa.

# Praktična implementacija alata za analizu i vizuelizaciju zavisnosti na Twitter-u

U kontekstu implementacije alata za analizu i vizuelizaciju zavisnosti na društvenim mrežama, pristupanje i prikupljanje podataka je od ključnog značaja. Kao prvi korak, preuzimanje podataka sa društvenih mreža, poput Twittera (sada X), zahteva pažljivo planiranje kako bi se osigurala potpuna i pouzdana analiza.

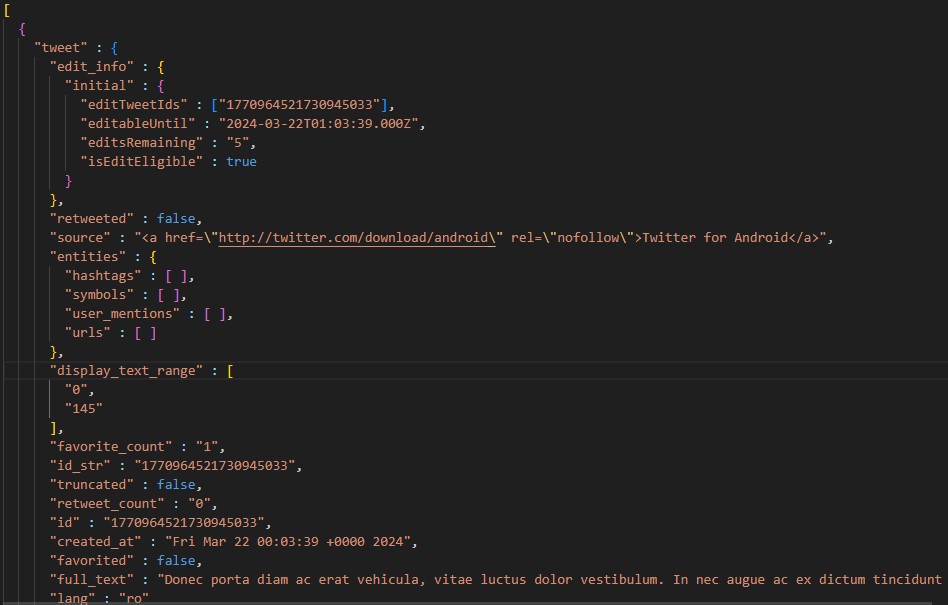
Koraci koji se preduzimaju za pristupanje podacima sa Twittera su ključni za početak procesa digitalne forenzike društvenih mreža. Kroz ovaj proces, prvo se identifikuje slučaj i definišu specifični ciljevi istrage. Na primer, možda je zadatak identifikovati sajber nasilnika ili prikupiti dokaze za određeni incident na mreži. Nakon toga, važno je uzeti u obzir pravna i etička pitanja, osiguravajući usklađenost sa zakonima i etičkim smernicama u vezi sa prikupljanjem i korišćenjem podataka.

## Preuzimanje arhiva podataka sa Twitter naloga

Prvo je potrebno preuzeti arhivu podataka sa Twittera kako bi se omogućila analiza i vizuelizacija zavisnosti na društvenim mrežama. Ovo se može postići putem procesa koji uključuje preuzimanje arhive podataka u HTML i JSON formatima.

Da bi se preuzela arhiva podataka, prvo je potrebno prijaviti se na svoj Twitter nalog putem web-a. Zatim, potrebno je kliknuti na opciju "More" u glavnom navigacionom meniju sa leve strane vremenske linije. Nakon toga izabrati "Settings and privacy", pa zatim "Your account". Klikom na opciju "Download an archive of your data" potrebno je potvrditi lozinku, a zatim odabrati opciju "Request archive". Nakon toga, Twitter će poslati e-mail sa linkom za preuzimanje arhive.

Arhiva podataka preuzetih sa Twittera obuhvata širok spektar informacija koje se smatraju najrelevantnijim i korisnim. To uključuje osnovne informacije o profilu, kao što su korisničko ime, biografija i lokacija, kao i sve objave koje je korisnik podelio na platformi, uključujući tekstualne tweet-ove (objave), fotografije, video zapise i GIF-ove. Takođe, arhiva sadrži podatke o komunikacijama putem direktnih poruka. Dodatno, u arhivi se nalaze spiskovi pratilaca korisnika i naloga koje korisnik prati, adresar kontakata, kao i informacije o interesovanjima i demografskim karakteristikama korisnika. Sve ove informacije omogućavaju detaljnu analizu aktivnosti i interakcija na Twitteru, pružajući bolji uvid u korisničko prisustvo na ovoj društvenoj mreži. [5]

 Primer fajla *tweets.js* iz preuzete arhive podataka koji je kasnije potreban za analizu podataka prikazan je na slici 9. Fajl sadrži informacije o pojedinačnim tvitovima gde svaki tvit ima tekst (*full\_text*), datum i vreme kreiranja (*created\_at*), jedinstveni ID (*id ili id\_str*), broj lajkova (*favorite\_count*), broj retvitova (*retweet\_count*), informaciju o izvoru tvita (*source*) i slično. Ove informacije omogućavaju analizu, filtriranje i vizualizaciju aktivnosti i sadržaja na Twitteru.

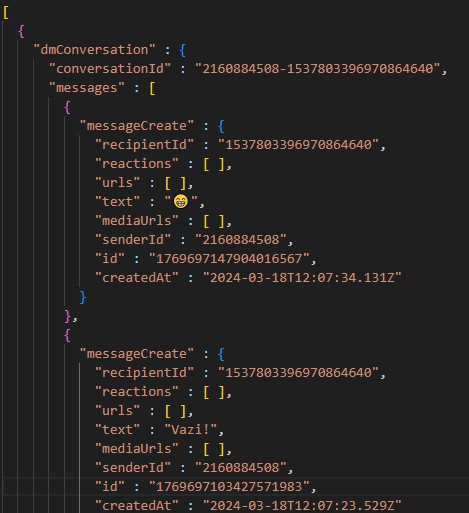
Slika 9. tweets.js fajl iz arhive podataka

Nakon uspešnog prikupljanja podataka, sledeći korak je njihova obrada i priprema. Centralna tačka ovog koraka je normalizacija podataka, što uključuje pretvaranje podataka u standardni format i uklanjanje nekonzistentnosti ili duplikata informacija. Ovaj proces čisti podatke od suvišnih informacija i priprema ih za dalju analizu i interpretaciju, omogućavajući efikasnu upotrebu podataka u sledećim fazama istraživanja.

## Analiza podataka

Nakon uspešno obavljenog procesa prikupljanja i pripreme podataka, sledeća ključna faza je analiza podataka. Ovaj korak podrazumeva dubinsko istraživanje sadržaja društvenih medija radi identifikacije relevantnih informacija i prepoznavanja ključnih obrazaca. U okviru ovog rada izvršena je implementacija alata koji za nalog na društvenoj mreži Twitter vrši analizu i vizuelizaciju zavisnosti između kontakata (praćenja). Analiza i vizuelizacija se radi za odabrani vremenski period i uključuje vizuelizaciju u obliku grafa jačine veza između kontakata (broj razmenjenih poruka). Takođe je urađena vizuelizacija statistike aktivnosti tj broj objavljenih tweet-ova u po satima u danu, danima u mesecu i mesecima u godini. Takođe obrađene se poruke koje je korisnik razmenjivao sa svojim pratiocima i kreiran je izveštaj u .txt formatu. Takođe izvršena je analiza objavljenih tvitova po ključnoj reči i vremenskom periodu.

### Analiza i vizuelizacija zavisnosti između kontakata na Twitter-u

 Nakon uspešno obavljenog procesa prikupljanja i pripreme podataka, sledeća faza je analiza podataka. Analiza i vizuelizacija u ovom slučaju podrazumeva crtanje grafa zavisnosti između kontakata, tako što čvorovi u grafu predstavljaju korisnike, a grane zavinost praćenja. Težine na granama predstavljaju broj razmenjenih poruka između 2 korisnika, koje ta grana povezuje. Podaci koji su u ovom slučaju neophodni za analizu i vizuelizaciju zavisnosti između kontakata na Twitter-u su fajlovi account.js, following.js, followers.js i direct-messages.js. Fajl koji je u ovom slučaju ključan za obradu je direct-messages.js, čija struktura je prikazana na slici 10, koji sadrži konverzacije korisnika sa kontaktima.

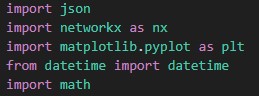
Slika 10. Fajl direct-messages.js

Svaki objekat u listi predstavlja jednu konverzaciju i sadrži ključ *dmConversation* koji opisuje detalje o konverzaciji. Svaka konverzacija ima svoj jedinstveni identifikator *conversationId* i listu poruka *messages*. Svaka poruka u konverzaciji predstavljena je objektom sa ključem messageCreate, koji sadrži informacije o samoj poruci, kao što su sadržaj teksta, URL-ovi, mediji, identifikatori pošiljaoca i primaoca, identifikator poruke, vreme slanja itd. Osim toga, poruke mogu sadržati i reakcije, kao što su lajkovi, predstavljene u listi reakcija pod ključem reactions. Struktura fajla omogućava lako učitavanje i obradu podataka o konverzacijama koristeći Python biblioteku **json**.

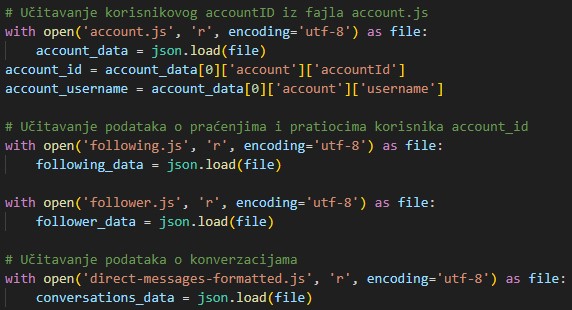
Fajlovi following.js i followers.js sadrže informacije o korisnicima koje korisnik čije su osnovne informacije u fajlu account.js prati odnostno koji ga prate.

Za analizu i vizuelizaciju neopodne su biblioteke prikazane na slici 11. Ove biblioteke su vrlo korisni alate u Pythonu za rad sa grafovima i vizualizaciju podataka:

* **NetworkX** je Python biblioteka koja omogućava kreiranje, manipulaciju i analizu složenih mreža ili grafova. Ova biblioteka omogućava rad sa različitim tipovima grafova, uključujući usmerene i neusmerene grafove, kao i težinski i netežinski grafovi.
* **Matplotlib** je popularna biblioteka u Pythonu koja se koristi za vizualizaciju podataka. Omogućava kreiranje različitih vrsta grafova, uključujući linije, stubiće, krugove i mnoge druge vrste grafika. Matplotlib je fleksibilan alat koji omogućava prilagođavanje izgleda i stilova grafova, kao i dodavanje oznaka, legendi i drugih elemenata koji poboljšavaju čitljivost vizualizacija.

 U kodu, *networkx* se koristi za manipulaciju grafa praćenja korisnika, dok se *matplotlib.pyplot* koristi za crtanje samog grafa sa svim njegovim čvorovima, granama i etiketama. Ove biblioteke zajedno omogućavaju analizu i vizualizaciju podataka o praćenju korisnika na društvenoj mreži.

Slika 11. Neophodne biblioteke za vizuelizaciju podataka

 Deo koda sa slike 12 vrši učitavanje podataka iz JSON fajlova: account.js, following.js, follower.js i direct-messages.js. Prvo se otvaraju ovi fajlovi u režimu čitanja koristeći *open*() funkciju. Kodiranje UTF-8 se koristi kako bi se osiguralo da se podaci ispravno interpretiraju ako sadrže specijalne znakove. Nakon otvaranja fajlova, *json.load(file)* funkcija se koristi za učitavanje sadržaja fajlova i pretvaranje JSON formata u Python objekte. Ova funkcija čita fajl i dekodira JSON podatke u Python rečnik.

Slika 12. Učitavanje podataka iz .js fajlova

U prvom delu koda sa slike 12, podaci o korisnikovom nalogu se učitavaju iz account.js fajla. JSON objekat se čuva u promenljivoj account\_data. Zatim se iz ovog objekta izvlače informacije o korisnikovom accountID i korisničkom imenu (username) i smeštaju se u odgovarajuće promenljive account\_id i account\_username.

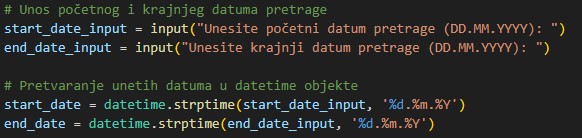
 U drugom delu koda sa slike 12, podaci o korisnicima koje korisnik prati i korisnicima koji prate korisnika se učitavaju iz following.js i follower.js fajlova. Podaci o korisnicima koje korisnik prati smeštaju se u promenljivu following\_data, dok se podaci o korisnicima koji prate korisnika smeštaju u promenljivu follower\_data.

Slika 13. Kreiranje grafa zavisnosti

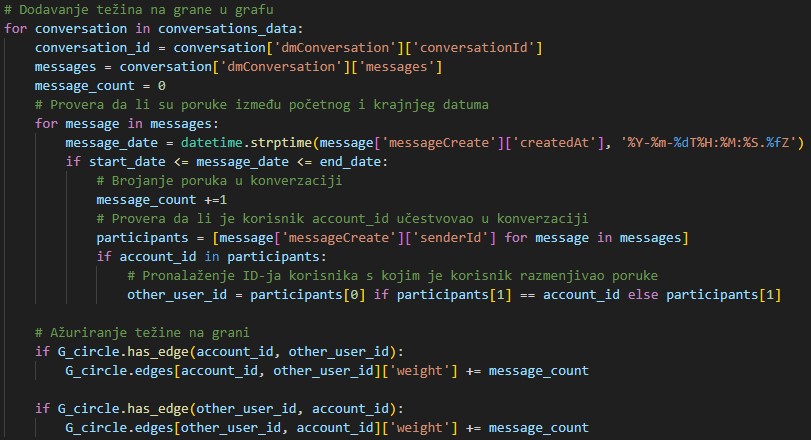
Deo koda sa slike 13 kreira usmereni graf koji ilustruje odnos između korisnika na Twitteru. Prvo se prazan graf kreira koristeći *nx.DiGraph()* funkciju iz NetworkX biblioteke. Zatim se dodaje centralni čvor za korisnika čiji je identifikator *account\_id*.

Da bi se osigurala jedinstvenost čvorova, pravi se skup *unique\_users* u koji se dodaju svi identifikatori korisnika koje korisnik prati i koji prate korisnika. Zatim se prolazi kroz podatke o praćenjima i dodaju se čvorovi za svakog korisnika koje prati korisnik, postavljajući ih na odgovarajuće pozicije na krugu. Svaki od ovih korisnika se povezuje sa centralnim čvorom korisnika čiji je identifikator *account\_id*. Isti postupak se primenjuje i za korisnike koji prate korisnika. Ukoliko čvor korisnika koji prati korisnika već nije dodat u graf, on se dodaje i povezuje sa centralnim čvorom.

Ovim postupkom se konstruiše graf koji jasno prikazuje odnos između korisnika koje korisnik prati i pratilaca korisnika na Twitteru, pružajući uvid u mrežu interakcija na platformi.

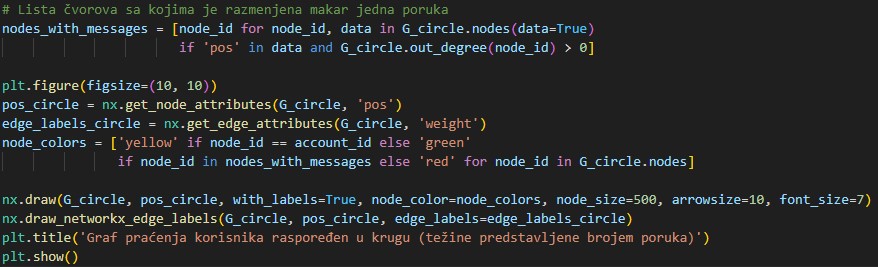
 Deo koda sa slike 14 koristi se za definisanje datuma početka i kraja analize podataka. Korisnik unosi početni i krajnji datum analize podataka. Ova dva datuma koriste se kao referentne tačke za analizu podataka unutar određenog vremenskog perioda.

Slika 14. Definisanje vremenskog perioda analize podataka

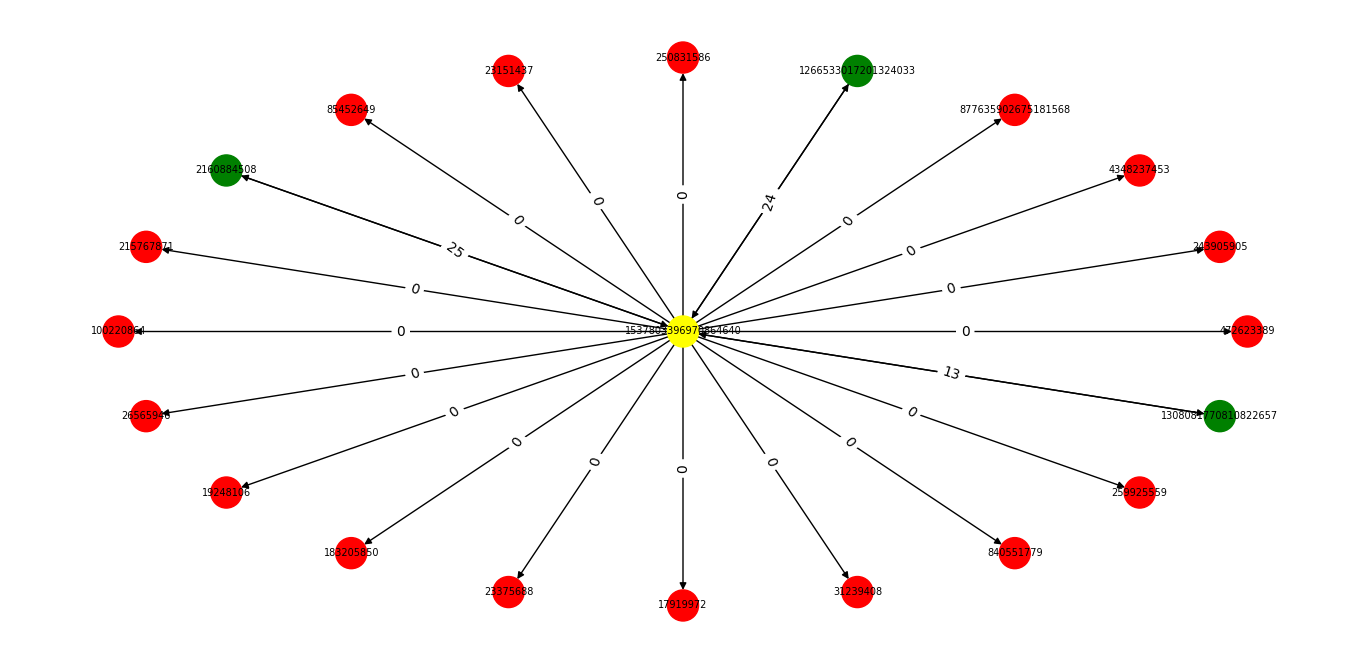
 Kod sa slike 15 prolazi kroz sve konverzacije u podacima o konverzacijama. Za svaku konverzaciju, prvo se izvlači ID konverzacije i lista poruka. Zatim se proverava da li su poruke poslate između početnog i krajnjeg datuma. Ako jesu, broji se broj poruka u toj konverzaciji i proverava se da li je korisnik *account\_id* učestvovao u njoj. Ako jeste, pronalazi se ID drugog korisnika s kojim je korisnik razmenjivao poruke. Nakon toga, ažuriraju se težine grana u grafu dodajući broj poruka na odgovarajuće grane koje povezuju korisnika *account\_id* sa drugim korisnikom i obrnuto.

Slika 15. Brojanje razmenjenih poruka između korisnika

U delu koda sa slike 16 vrši se crtanje grafa koji je prethodno konstruisan. Prvo se postavlja veličina prozora za crtanje grafa. Zatim se poziva funkcija *nx.get\_node\_attributes()* kako bi se dobili atributi pozicija čvorova u grafu. Ova funkcija uzima graf i atribut (u ovom slučaju poziciju pos) i vraća rečnik čiji su ključevi identifikatori čvorova, a vrednosti njihove pozicije. Slično tome, funkcija *nx.get\_edge\_attributes()* se koristi za dobijanje težina grana iz grafa.

 Nakon toga, graf se crta koristeći funkciju *nx.draw(),* pri čemu su podešeni odgovarajući parametri za označavanje čvorova, bojenje, veličinu čvorova i strelice. Boje čvorova određene su na osnovu određenih kriterijuma - žuti čvor predstavlja centralnog korisnika za čiji nalog je vršena analiza, zeleni čvorovi su korisnici sa kojima je razmenjena barem jedna poruka, dok su crveni čvorovi ostali korisnici.

Slika 16. Crtanje grafa

 Ovim postupkom se dobija vizuelna reprezentacija grafa praćenja korisnika sa dodatnim informacijama o broju razmenjenih poruka na težinama grana, što omogućava lakše razumevanje mreže interakcija među korisnicima na Twitteru. Rezultat prikazan je na slici 17, gde se može videti čvor u sredini koji je obojen žutom bojom i predstavlja korisnika čiji podaci se obrađuju, zatim crveni čvorovi koji predstavljaju korisnike koji prate ili koje korisnik prati, a sa kojima korisnik nije razmenjivao poruke, i na kraju zeleni čvorovi koji predstavljaju korisnike koji prate ili koje korisnik prati sa kojima je korisnik razmenjivao poruke. Na granama koje spajaju korisnika sa ostalim korisnicima može se videti, da je korisnik razmenjivao poruke i to 25, 24 i 13 poruka sa 3 različita korisnika.

Slika 17. Rezultat crtanja grafa

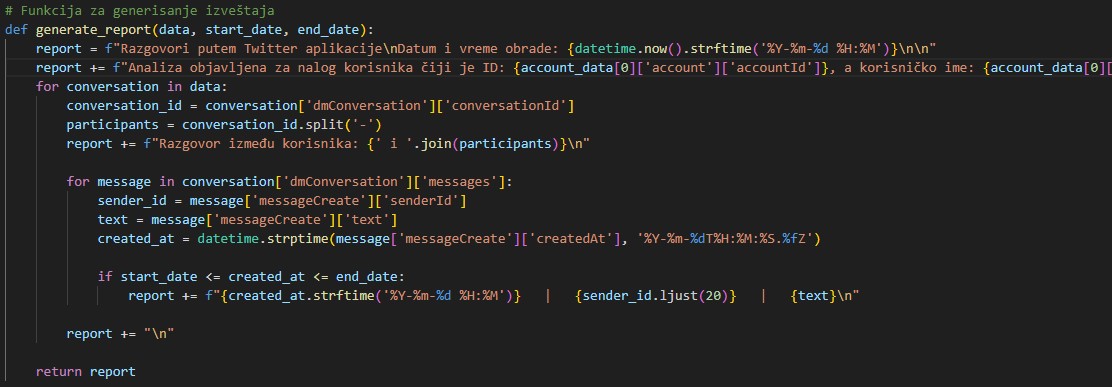
### Generisanje izveštaja o konverzacijama korisnika

Sledeća analiza obuhvata obradu podataka iz direktne komunikacije na Twitteru. Na osnovu učitanog JSON fajla sa podacima o razgovorima i podacima o nalogu, generiše se izveštaj koji sadrži informacije o razgovorima, uključujući datum i vreme, učesnike u razgovoru, vreme slanja poruka, korisnička imena pošiljalaca i sadržaj poruka. Generisani izveštaj se zatim čuva u tekstualnu datoteku.

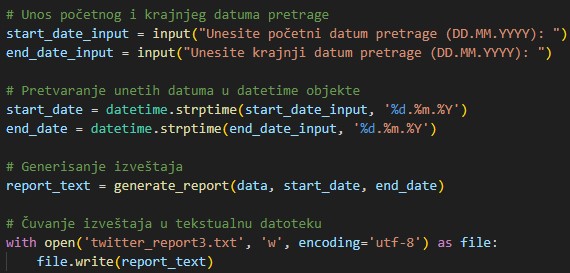
 Kod sa slike 18 učitava podatke iz dva JSON fajla: *direct-messages.js* i *account.js*. Prvi fajl sadrži podatke o direktnim porukama, dok drugi fajl sadrži podatke o korisničkom nalogu. Nakon učitavanja, podaci se mogu koristiti za dalju obradu ili analizu.

Slika 18. Učitavanje podataka

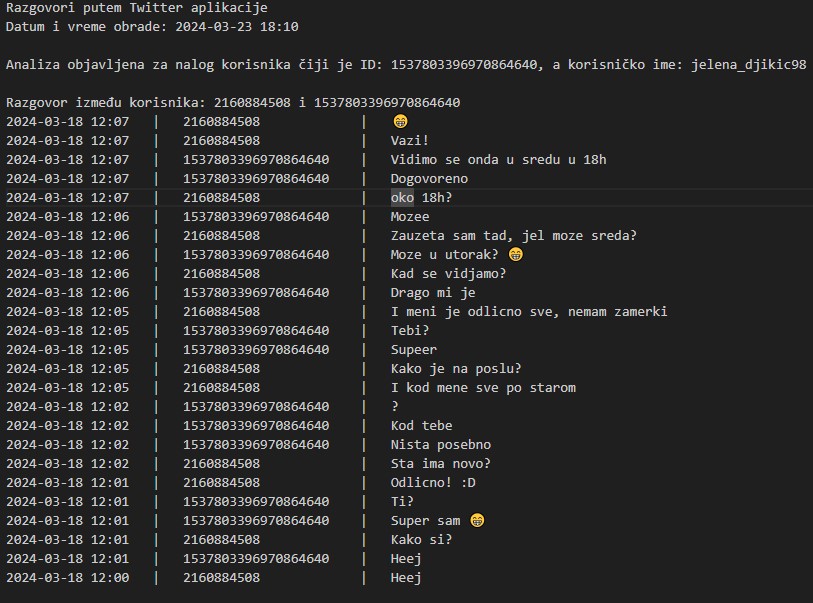
Deo koda sa slike 19 definiše funkciju *generate\_report* koja generiše izveštaj o razgovorima putem Twitter aplikacije. Funkcija prolazi kroz listu podataka o konverzacijama i za svaku konverzaciju formira detaljan izveštaj koji uključuje korisnička imena učesnika, vremenske oznake, korisnička imena pošiljalaca poruka i same poruke. Korisnik unosi početni i krajnji datum pretrage, kao na slici 20, te se izveštaj generiše tako da obuhvati samo poruke koje su razmenjene između ta dva datuma. Na kraju, generisani izveštaj se čuva u tekstualnu datoteku "twitter\_report3.txt".

 Na slici 21 prikazan je deo generisanog izveštaja, za unete datume 1.3.2024. i 20.3.2024, gde se mogu videti poruke koje je korisnik razmenjivao u traženom periodu.

Slika 19. Funkcija za generisanje izveštaja



Slika 20. Unošenje datuma pretrage i generisanje izveštaja



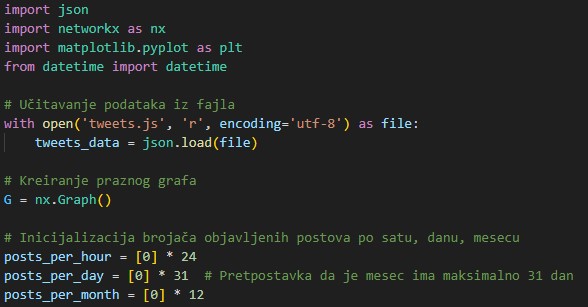
Slika 21. Deo generisanog izveštaja

### Vizuelizacija statistike aktivnosti (broj objavljenih postova)

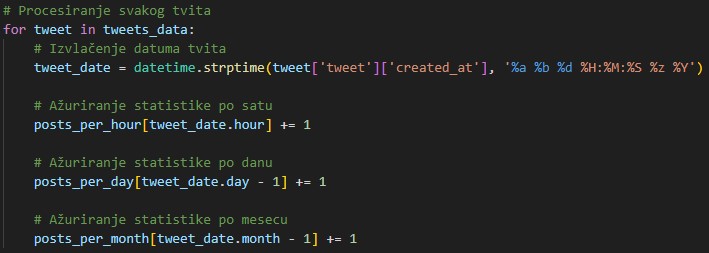
U ovoj analizi istraženo je kako se aktivnost na Twitteru raspoređuje tokom vremena. Počinje se sa prikupljanjem podataka iz JSON fajla *tweets.js* koji sadrži informacije o objavljenim tvitovima korisnika. Zatim se pristupa analizi ovih podataka kako bi se razumelo kako se ponašanje korisnika menja tokom dana, meseca i godine.

Kroz ovu analizu, istražuje se kako se broj objavljenih tvitova menja u različitim vremenskim periodima. Korišćenjem grafičkih prikaza, otkrivaju se obrasci aktivnosti na Twitteru. Ova analiza pruža uvid u to kako se korisnik angažuje na Twitteru tokom različitih vremenskih perioda i pomaže boljem razumevanju dinamike njegove online prisutnosti.

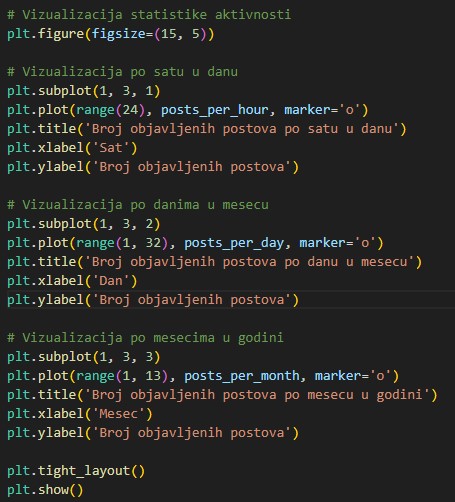
Deo koda sa slike 22 služi za analizu podataka iz fajla *tweets.js,* koji je prikazan na slici 9 i čija je struktura objašnjena u poglavlju 4.1., koji sadrži informacije o tvitovima koje je korisnik čiji su podaci preuzeti objavio. Koristi se biblioteka json za rad sa JSON podacima, networkx za manipulaciju grafom i matplotlib.pyplot za crtanje grafova. Učitani podaci se smeštaju u promenljivu *tweets\_data*. Zatim se kreira prazan graf pomoću *nx.Graph().* Dalje, inicijalizuju se brojači koji će pratiti broj objavljenih postova po satu, danu i mesecu. Na primer, *posts\_per\_hour* je lista sa 24 nule, gde svaki indeks predstavlja jedan sat u danu, a vrednosti će biti ažurirane tokom analize. Analogno tome, *posts\_per\_day* ima 31 element koji predstavljaju dane u mesecu, a *posts\_per\_month* ima 12 elemenata koji predstavljaju mesece u godini. Ova inicijalizacija je potrebna kako bi se kasnije pratila distribucija objavljenih postova po vremenskim intervalima.



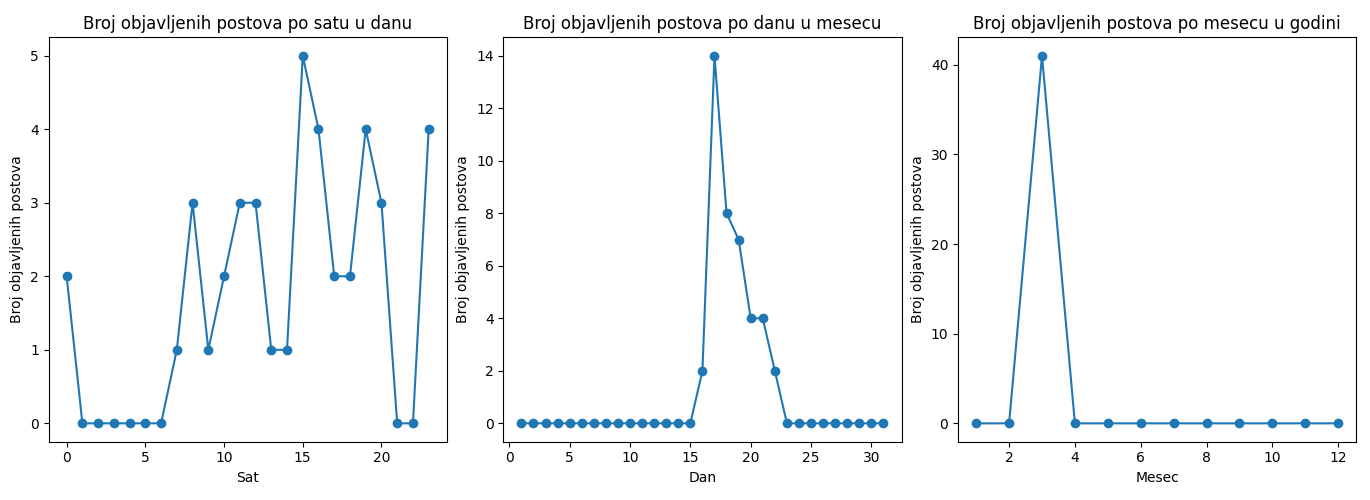
Slika 22. Učitavanje objavljenih tvitova i inicijalizacija promenljivih

 Deo koda sa slike 23 prolazi kroz svaki tvit u skupu učitanih podataka *tweets\_data* i obrađuje ih. Za svaki tvit, izvlači se datum objavljivanja tvita. Zatim se ažuriraju tri statističke promenljive: *posts\_per\_hour*, *posts\_per\_day* i *posts\_per\_month*. Ova obrada omogućava praćenje distribucije objavljenih tvitova tokom vremena.

Slika 23. Obrada tvitova

 Deo koda sa slike 24 se bavi vizualizacijom statistike aktivnosti na Twitteru. Prvo se kreira nova slika *figure* sa dimenzijama 15x5. Zatim se vrši podela na tri podgrafika, pri čemu se svaki od njih odnosi na različite vremenske periode: po satu u danu, po danima u mesecu i po mesecima u godini. Na svakom od ovih podgrafika prikazuje se broj objavljenih postova u određenom vremenskom periodu. Ovo omogućava vizualnu analizu aktivnosti korisnika na Twitteru tokom različitih vremenskih intervala. Nakon što su svi podgrafici definisani, koristi se *plt.tight\_layout()* kako bi se osiguralo da su svi podaci pravilno raspoređeni, a zatim se prikazuje kompletna vizualizacija pomoću *plt.show().*

Slika 24. Isrctavanje prikaza

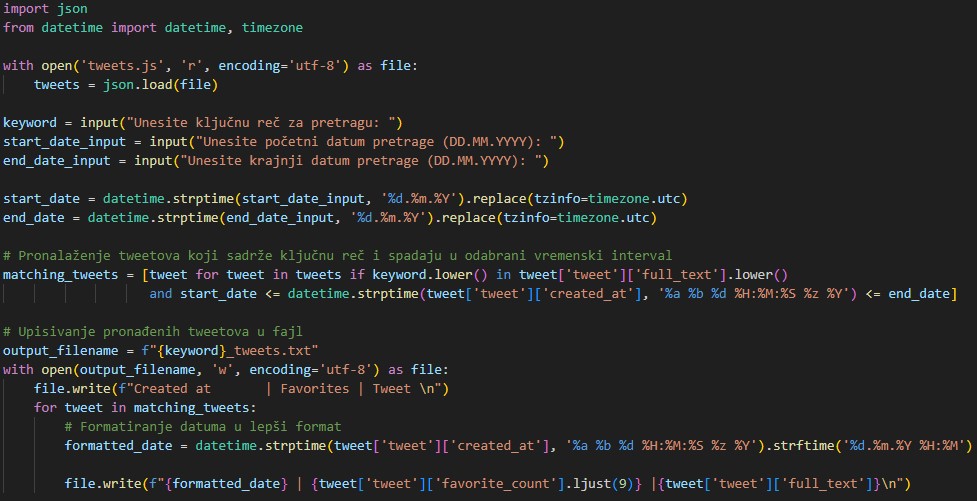
 Na slici 25 prikazan je rezultat izvršenja prethodno objašnjenog koda. Na prvom grafiku prikazan je broj objavljenih tvitova po satu u danu gde se može videti da je korisnik najviše tvitova objavljivao oko 16h. Zatim se na sledećem grafu prikazuje broj objavljenih tvitova po danu u mesecu, gde se može videti da je korisnik najviše objavljivao 17. u mesecu i to 14 tvitova. Na poslednjem grafiku prikazan je broj objavljenih tvitova po mesecu u godini gde se može videti da je korisnik objavljivao sve svoje tvitove u mesecu martu.

Slika 25. Rezultujući grafik

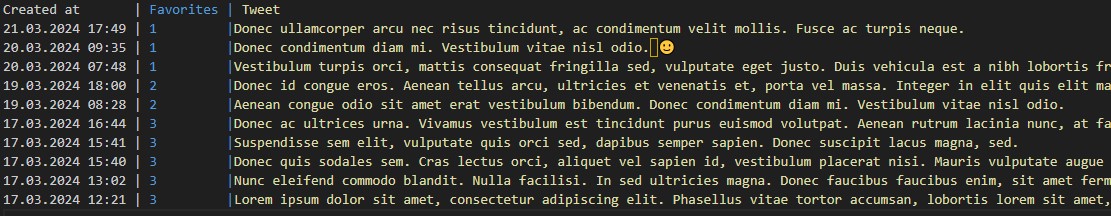
### Pretraga objavljenih tvitova po ključnoj reči

U ovom delu analize obradjuju se tvitovi korisnika sa ciljem pronalaženja onih koji sadrže određenu ključnu reč. Korisnik unosi ključnu reč za pretragu, nakon čega se podaci o tvitovima učitavaju iz JSON fajla. Zatim se prolazi kroz svaki tvit i proverava da li ključna reč koju je korisnik uneo postoji u tekstu tvita. Tvitovi koji sadrže tu ključnu reč se filtriraju. Osim toga, korisnik unosi i početni i krajnji datum kako bi se pretraga sprovela samo nad tvitovima koji su objavljeni u odabranom vremenskom periodu. Nakon filtriranja, pronađeni tvitovi se upisuju u tekstualnu datoteku zajedno sa datumom i vremenom kada su objavljeni i brojem lajkova (favorites). Ovaj postupak prikazan je na slici 26.

Tvitovi koji se nalaze na profilu korisnika koje je objavljivao, formirani su uz pomoc Lorem Ipsum generatora. Ukoliko korisnik unese ključnu reč *Donec*, i unese za početni datum 1.03.2024, a za krajnji datum 22.03.2024 u fajlu *Donec\_tweets.txt* biće upisani svi tvitovi koji sadže tu reč koji su objavljeni u odabranom vremenskom periodu. Na slici 27 prikazan je taj fajl.



Slika 26. Traženje tvitova koji sadrže konkretnu ključnu reč



Slika 27. Fajl koji sadrži sve nađene tvitove koji sadrže reč “Donec”

# Zaključak

Istraživanje digitalne forenzike društvenih mreža otkriva kompleksnost i značaj ovog područja u savremenom digitalnom dobu. Fokusiranje na analizu aktivnosti i komunikacije na platformama poput Twitter-a pruža uvid u različite aspekte forenzičke analize, uključujući identifikaciju dokaza, utvrđivanje autentičnosti, i rekonstrukciju događaja.

Praktična implementacija alata za analizu i vizualizaciju zavisnosti na Twitter-u pokazuje praktičnu primenu digitalne forenzike društvenih mreža. Ovo istraživanje naglašava važnost efikasnih alata i tehnika za obradu i interpretaciju podataka, s obzirom na izazove kao što su privatnost korisnika i brzina promene podataka.

Zaključak je da digitalna forenzika društvenih mreža igra ključnu ulogu u otkrivanju i istraživanju digitalnih tragova, pružajući osnovu za donošenje informisanih zaključaka u pravnom, istražnom, i bezbednosnom kontekstu. Dalji razvoj alata i tehnika za analizu društvenih mreža nastaviće da unapređuje efikasnost i preciznost forenzičkih istraživanja u digitalnom okruženju.

# Literatura

[1] <https://jatheon.com/blog/social-media-investigation-tools/>

[2]<https://blog.pagefreezer.com/5-social-media-investigation-tools-thatll-save-you-time-reduce-frustration>

[3] <https://www.boscolegal.org/blog/how-social-media-has-shaped-digital-forensics/>

[4] <https://www.sciencedirect.com/science/article/abs/pii/S1742287618302937>

[5] <https://help.twitter.com/en/managing-your-account/accessing-your-x-data>