UNIVERZITET U NIŠU
ELEKTRONSKI FAKULTET

Maja Stojanović

Digitalna forenzika

Tema: Forenzika socijalnih mreža- Facebook

Profesor:

Prof. dr Bratislav Predić

Student:

Maja Stojanović, br. ind. 1227

Niš, Avgust 2022.

Sadržaj

1. Uvod **3**
2. Forenzika socijalnih mreža **5**
3. Podaci socijalne mreže **6**
4. Vizualizacija **7**
5. Formalni model znanja za forenziku online socijalnih mreža **10**
5.1 Komponente socijalne mreže- fundamentalne definicije **10**
5.1.1 Društveni graf 11
5.1.2 Sadržaj 11
5.1.3 Korisnik 12
5.2 Model zasnovan na događajima za online društvene mreže **12**
6. Graph API i Facebook Artefakti **13**
6.1 Graph API **13**
6.2 Facebook Artefakti **14**
7.Postojeći softveri za analizu socijalnih mreža **16**
8. Zaključak **19**
9. Literatura **20**

1. Uvod

Naglim razvojem računarske tehnologije poslednjih godina broj korisnika računara i računarskih mreža raste vrtoglavom brzinom. Dostupnost i fleksibilnost tehnologija današnjih savremenih računarskih mreža omogućava da se sa bilo koje tačke na planeti može povezati na mrežu i doći do željenih informacija.

Digitalne informacije se koriste u svakom aspektu života, iako korišćenje ovakvih podataka donosi mnoge prednosti, takođe se javljaju i razni oblici zloupotrebe podataka koji se razmenjuju i čuvaju.

Digitalna forenzika kao disciplina ima za cilj pronalaženje, prikupljanje i dokumentovanje podataka koji se nalaze u digitalnom obliku. Bazira se na principima standardne forenzike, uzimajuću u obzir da je ovde reč o digitalnim dokazima a ne fizičkim.

Digitalni podatak je apstraktna reprezentacija informacije, predstavlja sekvencu bitova i ne poseduje neka očigledna svojstva koja bi ukazala na autentičnost ili poreklo informacija. Postoje razne vrste uređaja koji se koriste za stvaranje i snimanje digitalnih informacija, kao što su kamera, mobilni telefoni, kompjuteri... Pribavljanje podataka iz tih uređaja može biti veoma zahtevno, otežavajuće okolnosti mogu biti da su ti podaci sakriveni, fragmentovani ili kriptovani. Takođe količina podataka sa kojom se forezničar susreće je jako velika i njen pregled oduzima previše vremena. Digitalni podaci se mogu prenositi različitim kanalima pa su često raštrkani na nekoliko uređaja i mogu se javiti u različitim formatima, što analizu čini jako teškom. Ovi podaci se mogu lako brisati, modifikovati i kriptovati. Podaci mogu biti ranjivi i zahtevati brzo prikupljanje i obradu.

Ovo su neki od problema i izazova sa kojim se svakodnevno sreću forezničari. U cilju olakšavanja i rešavanja ovih izazova, razvijene su metode za rekonstrukciju i pribavljanje dokaza iz digitalnih podataka a nakon toga i za njihovu analizu. Digitalna forenzika se može definisati kao skup metoda za očuvanje, sakupljanje, validaciju, identifikaciju, analizu, interpretaciju, dokumentaciju i prezentaciju digitalnih dokaza proizašlih iz digitalnih izvora, čiji je cilj potvrđivanja ili pomoganja pri rekonstrukciji događaja koji su često kriminalne prirode.

Digitalna forenzika je disciplina koja se ubrzano menja i raste, pokušavajući da održi korak sa tehnologijom koja se stalno unapređuje i menja i razvojem novih softvera.

Vrste kompjuterskom kriminala su se proširile na razne oblasti.

Osnovne grane digitalne forenzika su: kompjuterska forenzika, mrežna forenzika, forenzika baza podataka i forenziku mobilnih uređaja. Osim osnovnih grana digitalne forenzike, postoje još i grane koje se koriste ređe ili se njihove metode istrage već koriste u osnovnim granama. Neke od tih grana su forenzika fajl sistema, forenzika malwera, forenzika elektronske pošte, live forenzika, forenzika socijalnih mreža, forenzika Interneta stvari.

Ovaj seminarski rad će se baviti temom forenzike socijalnih mreža, sa fokusom na forenziku Facebook socijalne mreže.

U prvim delovim rada biće detaljnije opisan proces forenzike socijalnih mreža, koji se podaci koriste i načini vizuelizacije koji se koristi prilikom analize socijalnih mreža, zatim će biti prikazan formalni model znanja koji se koristi a u daljim poglavljima rad će se fokusirati na Graph API i Facebook artefakte, dok će u poslednjem delu biti prikazani neki softverski alati koji se trenutno koriste za ovaj tip forenzike.

2. Forenzika socijalnih mreža

Rast socijalnih mreža tokom poslednje decenije je zapanjujući. Pored dobro poznatih brendova kao što su Facebook, LinkedIn, Tviter, Instagram i Jutjub, postoji preko 200 sajtova za društvene mreže, sve aktivne.Samo Fejsbuk ima preko milijardu korisnika koji (između ostalih informacija) objavljuju preko 350 miliona fotografija svakog dana. Društvene mreže imaju veliki uticaj na društvo, uključujući pružanje zabave, generisanje informacija i olakšavanje komunikacije, istovremeno stvarajući mnogo dokaza. Forenzika socijalnih mreža je grana digitalne forenzike koja je relativno mlada i nova.

Forenzika socijalnih mreža nije ništa drugo do primena tehnika kompjuterskog istraživanja i analize, kao što je prikupljanje informacija iz onlajn izvora (npr. Fejsbuk, Tviter, LinkedIn...) i naknadno skladištenje, analiziranje, i čuvanje tih informacija kao dokaz koji će možda morati da se iznese na sudu. Za forenziku socijalnih mreža obično postoji mnogo podataka za prikupljanje, ali problem je znati kako to učiniti. Izazov je pronaći relevantne podatke u moru informacija, jer se oni, osim na sovijalnim mrežama mogu nalaziti na povezanim stranicama, blogovima i portalima. Najveći problem forenzike društvenih mreža je prikupiti dokaze bez kršenja zakona i uredbi, poput GDPR-a (eng. General Data Protection Regulation) i ToS-a (eng. Terms of Service). Takođe, teško je raditi s podacima i mrežama koje su aktivne (eng. live) pa se forenzičari koriste alatima za arhiviranje sadržaja.

Drugi važan aspekt forenzike je pravilna vizuelizacija podataka zbog ogromne količine dostupnih podataka. Štaviše, teško je vizualizovati prikupljene podatke sa društvenih mreža na način na koji se može odgovoriti na uobičajena pitanja od interesa, tako da ljudi bez tehničke pozadine to mogu razumeti.

3. Podaci socijalne mreže

Iako se društvene mreže razlikuju po karakteristikama i arhitekturi, mogu se identifikovati generički izvori podataka koji su od interesa za forenzička ispitivanja na društvenim mrežama. Neki podaci od interesa su:

- **Društveni otisak** (eng. Social footprint): Koji je društveni graf korisnika, sa kime je povezan (''prijatelj'')?
- **Komunikacioni obrazac**: Kako se socijalna mreža koristi za komunikaciju, koja metoda se koristi i sa kime korisnk komunicira?
- **Slike i video snimci**: Koje slike i video zapise je postavio korisnik, na kojim slikama drugih ljudi se kornisik pojavljuje i na kojima je označen?
- **Vremena aktivnosti**: Kada je određeni korisnik povezan na socijalnu mrežu, kada se tačno desila određena aktivnost od interesa?
- **Aplikacije**: Koje aplikacije korisnik koristi, koja je njihova svrha i šta se može zaključiti iz informacija o aplikaciji u društvenom kontekstu?

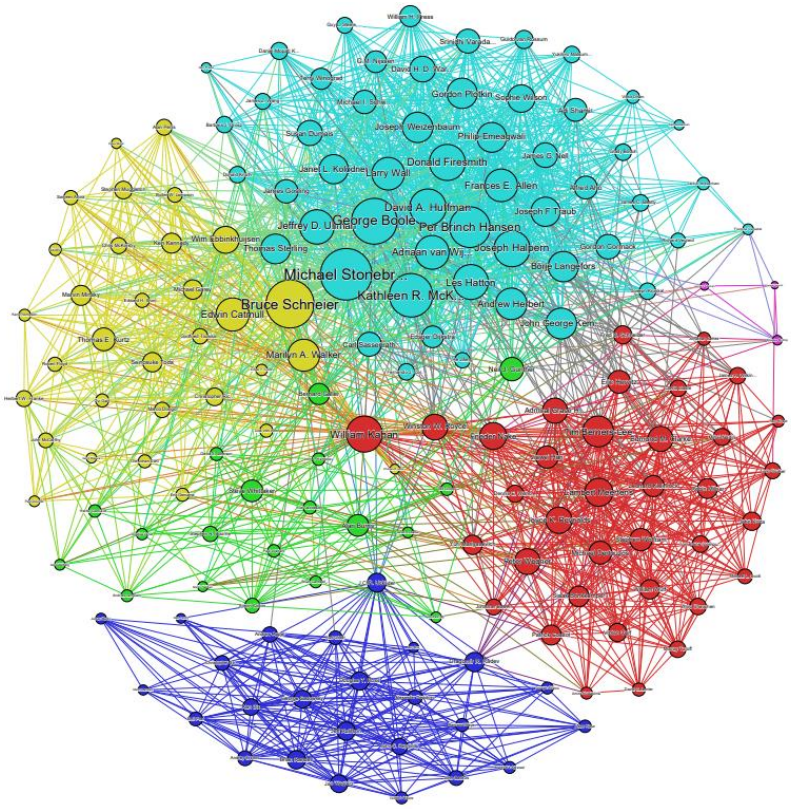
Sve ove informacije se ne mogu naći na hard disku osumnjičenog, zato što se čuvaju isključivo kod operatera socijalne mreže. Posebno kod ljudi koji koriste socijalne mrežie svakodnevno se čuva mnoštvo informacija. Fejsbuk tvrdi da više od 50% njegovih korisnika korist ga svakog dana, što bi bilo oko 400 miliona korisnika. Ponekad se informacije keširaju lokalno, ali to nije pouzdan izvor informacije jer nisu potpune niti se trajno čuvaju. Zavisno od implementacije socijalne mreže, dostupnost samih podataka i mogućnost preuzimanja podataka putem API poziva može varirati među različitim socijalnim mrežama. Međutim, većina ovih podataka može se izvući direktno, ili se izvući zaključak o ovim podacima bez saradnje operatera socijalne mreže. Kada podaci postanu dostupni istraživaču, može se sprovesti ceo spektar analize socijalne mreže. Najlakši način za dobijanje podataka je uz saglasnost korisnika, koji može dati korisničko imei lozinku. Dok se podaci mogu lako analizirati ručno nakon toga, da bi se odgovorilo na konkretna pitanja koja su od interesa, ogromna količina podataka zahteva automatizovane alate za forenzičku analizu.

4. Vizualizacija

U zavisnosti od podataka socijane mreže mogu se definisati sledeći grafovi koji su od interesa i vizuelizacije za forenziku socijalnih mreža.

Osnovne vizuelizacije:

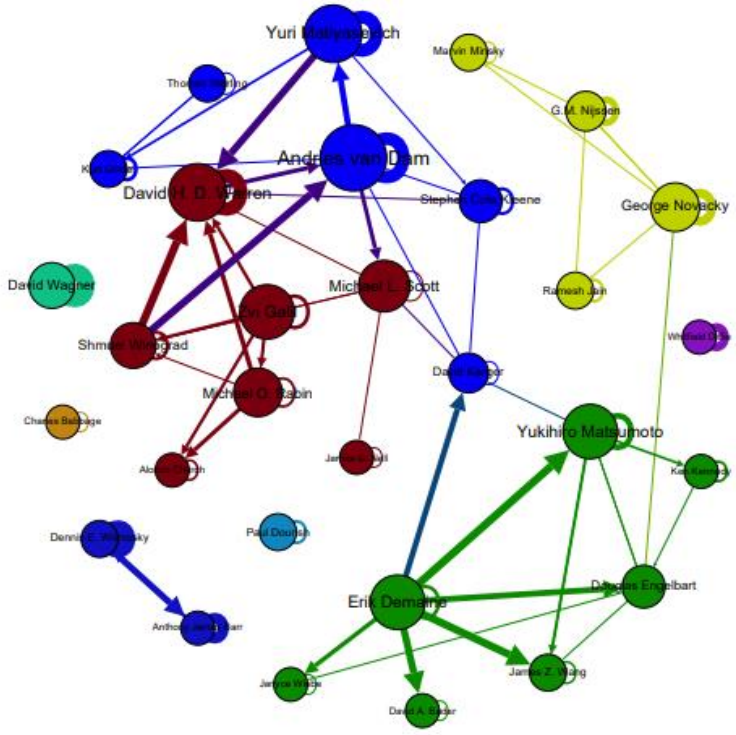
- **Graf društvene povezanost:** Trivijalno je preuzeti listu prijatelja sa društvenih mreža. U većini socijalnih mreža ovo je javna informacija, ili se može se lako prikupiti čak i bez ulaska u društveni krug naloga koji se istražuje. Međutim, nije trivijalno grupisati ove prijatelje, teško je da se sazna ko je s kim povezan (na primer: da li je određeni kontakt iz grupe prijatelja na poslu ili je kontakt direktno povezan?). Graf se može predstaviti kao neusmereni graf G =< V, E > gde je V = v1, v2, ...vn skup prijatelja korisnika, i E = (vk, vi), ... je skup ivica koji spaja dva čvora u slučaju da su prijatelji na društvenoj mreži. Visoko povezani čvorovi imaju visok stepen, predstavljaju dobro povezane prijatelje koji poznaju većinu prijatelja osumnjičenog takođe. Primer grafikona dobijenog korišćenjem softvera Gephi se nalazi na sledećoj slici:



Slika 1- Graf drustvene povezanosti

- **Graf društvenih interakcija**: Za mnoga istraživanja je od značaja da se sazna ko je sa kim komunicirao. Razni načini komunikacije mogući su među korisnicima, kao što su objave na zidu, direktne poruke, grupna komunikacija ili praćenje javnih saopštenja.

Komunikacija može biti predstavljena kao usmereni graf G =< V, E > gde su čvorovi V = v1, v2, ...vn svi prijatelji dok su ivice E = (vk, vi), ... usmerene i težina (vk, vi) se povećava za svaku poruku poslatu od vk do vi.



Slika 2- Graf društvenih interakcija korišćenjem tagova na slikama

- **Potpuna vremenska linija**: Korisnici društvenih mreža su na mreži 24/7 koristeći mobilne klijente na telefonima, vremenska linija postaje od veće važnosti. Može se izdvojiti ne samo aktivnost samog korisnika, već i aktivnosti svih njegovih prijatelja. Često se vremena aktivnosti mogu lako videti, ako se pravilno vizualizuju. Da bi analiza bila izvodljiva potrebno je da se koriste različiti slojevi podataka: aktivnost korisnika, aktivnost prijatelja, grupne aktivnosti, reakcije prijatelja na događaje... Takođe je ključno da vremenska linija može da se zumira, da bi se vizuelizovali vremenski rasponi od značaja - jedan dan može lako imati više od 500 događaja za dati profil.
- **Vizuelizacija lokacije**: Geografsko označavanje i aplikacije za lokaciju su nove karakteristike sa sve većom upotrebom koje treba da se odraze na forenzička ispitivanja. Sa Foursquare-om i Facebook lokacijama (mestima), informacije o geolokaciji koje se čuvaju u društvenim mrežama stalno rastu. Digitalne kamere kao i pametni telefoni automatski geotaguju slike snimljene sa tačnom lokacijom. Do sada, većina društvenih mreža uklanja metapodatke tokom transformacije za skladištenje slike.

Prethodne karakteristike su jako jednostavne, sledeće funkcije i komponente bi trebale da budu standardni deo alata u forenzici.

Napredne vizuelizacije:

- **Podudaranje vremenske linije:** U visoko centralizovanim sistemima kao što su onlajn socijalne mreže, istraživač ima prednost konzistentnih vremenskih oznaka koje pruža socijalna mreža. Operateri često pokreću svoju sopstvenu NTP infrastrukturu i održavajte satove doslednim na hiljadama servera. Ovo se zatim može koristiti za usklađivanje vremenskih linija različitih profila i na kraju kreirati tačnu vremensku liniju za kompletan skup prijatelja.

- **Diferencijalni snimci (Snapshot):** Jednom kada se prikupi forenzička slika korisničkog profila, kasnije slika može izgledati potpuno drugačije. Stoga, forenzički alat mora da obezbedi funkcionalnost ne samo vizuelizacija podataka društvenih mreža korisnika, ali i funkcionalnost vizuelizacije razlika sa prethodnim slikama istog korisnika.

5. Formalni model znanja za forenziku online socijalnih mreža

U nastavku je opisano kako treba da izgleda formalni model znanja za forenziku online socijalnih mreža i opisan je predloženi model znanja iz [1].

Ovaj model ima za cilj da formuliše teorijski model za objašnjenje nalaza i analize dokaza proces automatizovanim metodama. Ove metode bi bile pouzdane samo ako su zasnovane na formalnoj i objašnjivoj teoriji, koji se rigorozno može testirati; dakle, automatizovani rezultati i dokazi bi bili prihvatljivi na sudu.

Zakonski prihvatljiva upotreba automatizovanih metoda za analizu podataka zahteva snažan teorijski model za proces digitalne forenzike. Sveobuhvatan i formalan teorijski model je potreban kako bi se objasnile sve različite analize podataka i obrade podataka koje. Potreban je kohezivni skup potrebnih karakteristika koje su eksplicitno specificirane za konkretan domen (tj. društvene mreže) za objašnjenje procesa digitalne forenzike.

Jasno definisan teorijski model za istragu onlajn društvene mreže je potreban da bi se objasnile sve neophodne komponente i asocijacije među komponentama. Formalni model znanja pomaže u razumevanju i tumačenju rezultata ili dokaza dobijenih iz procesa forenzičke analize. Predloženi pristup sastoji se od četiri koraka koji su prikazani u nastavku:

- Prvo, identifikuje znanje u vezi sa onlajn društvenim mrežama i formalno definiše entitete povezane sa društvenim mrežama
- Drugo, objašnjava reprezentaciju modela znanja zasnovanog na događajima kako bi se objasnila povezanost između identifikovanih subjekata i incidenta koji su u vezi sa istragom. Ovo znanje će se koristiti za analizu podataka kako bi se pronašle najrelevantnije informacije u vezi sa incidentom. Ovaj korak osigurava ponovljivost procesa i pomaže u sticanju potrebne pouzdanosti automatizovanog procesa analize
- Treće, gradi ontologiju za formalno predstavljanje modela znanja, koji izvlači znanje iz heterogenih izvora podataka i popunjava model znanja
- Četvrto, predlaže formulaciju operatora analize za analiza informacija u vezi sa incidentom koje se izvlače i čuvaju u prethodnim koracima

5.1 Komponente socijalne mreže- fundamentalne definicije

Društvena mreža pruža platformu pojedincima za izgradnju društvenih odnosa sa drugim pojedincima (npr. oni koji imaju slične stavove ili profesionalnih interesovanja). Takođe, omogućava povezivanje sa prijateljima iz stvarnog života, kolegama i porodicom... Dakle, društveni mreža je opisana kao obiman skup interakcija. Podaci sa društvenih mreža odnose se na sadržaj generisan kao rezultat interakcija na društvenim mrežama. Interakcija predstavlja značajan koncept u socijalnim mrežama. Nekoliko ključnih koncepata koje deli većina online društvenih mreža i koji se koriste u ovom modelu su navedeni u nastavku.

5.1.1 Društveni graf

Društvena mreža se sastoji od skupa pojedinaca (društvenih aktera), kolekcije asocijacija i skupova društvenih interakcije među akterima. U ovom modelu, društveni graf (SG) je skup svi h pojedinaca, koji su međusobno povezani preko društvene mreže, SG = {sg1, sg2, sg3 . . . . . .sgn}. Sgx je skup korisnika koji se odnose (koji su povezani) na datu osobu x,

$$SG_x = \{sg_1, sg_2, sg_3 \ldots\ldots\ldots sg_n | sg_i \in U \wedge \forall sg_i \alpha x\}$$

gde i varira od 1 do n. U jednom društvenom grafikonu, x je centralni čvor; međutim, x je takođe podskup društvenog grafa SGx

$$x. \subseteq SG_{x.}$$

5.1.2 Sadržaj

Sve informacije objavljene ili deljene na online društvenim mrežama se smatraju kao sadržaj u ovom modelu. Ažuriranja koje je objavio korisnik u formi teksta (tj. blog, poruke), medija (tj. slika, video snimaka) ili bihejvioralni odgovori (tj. sviđanja) su deo sadržaja. Isto tako, interakcije koje se dešavaju među korisnicima su takođe deo sadržaja. Dakle, sadržaj C je skup svih objavljenih informacija ažuriranja **D** i interakcija **It**, pored podataka profila **P**, dakle ukupan sadržaj je

$$C = D \cdot \cup \cdot P \cdot \cup \cdot It \cdot$$

Sadržaj se dalje klasifikuje kao interakcija i aktivnost.

Interakcija: Društvena mreža je prostor gde se skup interakcija It = {i1, i2, i3 . . . ..in} odvija. Interakcija je razmena komunikacije između korisnika na društvenoj mreži. Interakcije se javljaju među korisnicima tako što korisnici odgovaraju na sadržaj komentarima, prosleđuju ili dele ponašanja i označavaju druge korisnike.

Dakle, interakcija u online društvenim mrežama se odnosi na skup objekata koje koristi subjekt (osoba) za komunikaciju (tj. Tvit, direktna poruka) sa drugim subjektom ili kao odgovor na objekat, što je komunikacija (tj. odgovor, favorit) drugog subjekta. Neka je **It** interakcija nastala između korisnika **x**, i njegov društveni graf SG

$$it_j = \{i_j \in I | i_j \alpha x \wedge \alpha sg_x\}$$

Gde j varira od 1 do n j = {1,2,….n.}. Dok je **α** veza koja povezuje **x** sa **i** i **i** takođe je povezan sa društvenim grafom.

Aktivnost: Provajder društvenih mreža beleži sve informacije povezane sa interakcijom, to se naziva aktivnost A. Ove snimljene informacije su opisane kao metapodaci **MD** u ovom modelu. Sadrži sve atribute sredine (tj. informacije o uređaju, informacije o lokaciji) i atribute o vremenu (tj. podaci i vreme) koji su povezani sa interakcijom **I** i snimljene od strane provajdera ili digitalnih uređaja.

$$MD \alpha It$$

5.1.3 Korisnik

Neka je U = {u1, u2,u3,…..un} skup pojedinaca koji predstavljaju sebe na online društvenim mrežama kreiranjem profila. Taj profil pruža osnovne informacije o toj osobi, kao što su ime, adresa, godine, interesovanja. Informacije o profilu daje osoba i vidljive su na društvenoj mreži. Jedan pojedinac se naziva **ui** i predstavlja ga profil **P** na onlajn platformama. Ova dva koncepta su otprilike slični u kontekstu društvenih medija, dakle, **ui** ≈ **Profil**. Za svakog korisnika postoji samo jedan profil na svakoj društvenoj mreži.

$$\forall u_i \exists ! \, P$$

5.2 Model zasnovan na događajima za online društvene mreže

U digitalnoj forenzici Carrier je prvobitno predložio model znanja zasnovan na događajima (Carrier i Spafford, 2004), a zatim su ga pratili (Schatz et al., 2004a; Schatz et al., 2004b; Šabot i sar., 2015). Međutim, svi ovi modeli su ograničeni u kapacitetu skladištenja količine znanja, a samim tim i analize i mogućnosti automatizacije (Chabot et al., 2015).

Ovaj model zasnovan je na događajima znanja (event-based knowledge) koja su posebno dizajnirana za automatizovanu forenziku i analizu društvenih medija. Ovaj model će biti prvi model koji pruža teorijsku osnovu za forenziku društvenih medija i prikupljanje dokaza. Ovaj model omogućava bogato predstavljanje znanja koje sadrži širok skup entiteta i odnosa iz domena društvenih medija. Precizna reprezentacija ovih entiteta omogućiće konstruisanje automatizovanih metoda analize. U ovom delu je predstavljen formalni opis modela.

Pored toga, ovaj model će pomoći da se generišu rezultati koji su lako objašnjivo u pravnom postupku. Dalje omogućava reprodukciju i validaciju istražnog procesa.

Događaj se definiše kao pojedinačna radnja koja se desila u bilo kom trenutku vreme. U ovom modelu, događaj se odnosi na skup interakcija (odgovori, lajkovi, deljenja) koje se odvijaju između nekoliko subjekata (tj. korisnika) preko različitih objekata (tj. slika, video, tvitovi). Prema tome, **E** = {e1,e2,…en} je skup od n događaja koji se odvijaju mesto na mestu zločina. Međutim, koncept mesta zločina je potpuno drugačiji u ovoj forenzici.

Ovaj model se sastoji od sledećih komponenti: **Subjekat**, **Objekat**, **Događaj**, **Dokaz**, **Relacija** (veza).

6. Graph API i Facebook Artefakti

6.1 Graph API

Graph API je primarni način za unošenje i iznošenje podataka sa Facebook platforme. API je zasnovan na HTTP-u koji aplikacije mogu da koriste za kreiranje upita podataka, objavljivanje novih priča (story), upravljanje oglasima, ubacivanje fotografija i obavljanje velikog broja drugih zadataka.

API Graph je dobio ime po ideji „društvenog grafikona"- predstavljanja informacija na Fejsbuku. Sastoji se od čvorova, ivica i polja. Obično se koriste čvorovi za dobijanje podataka o određenom objektu, ivice za dobijanje kolekcije objekata na jednom objektu i polja za dobijanje podataka o jednom objektu ili svakom objektu u kolekciji.

Komponente Graph API-ja:

Čvorovi (Nodes)- ''stvari'' kao što su Korisnik, Stranica, Komentar. Svaki čvor ima jedinstveni identifikator, neki čvorovi sadrže i korisničko ime.

Ivice (Edges)- veze između čvorova.

Polja (Fields)- informacije o čvorovima (na primer rodjendan korisnika).

ID- identifikator čvora.

Link- Facebook URL čvora.

Entiteti:

- **Profil**- može biti Korisnik, Stranica, Grupa ili Događaj.
- **Korisnik**- osoba na Facebook-u
- **Lista prijatelja**- objekat koji se odnosi na grupu prijatelja koji je kreiran od strane nekoga ili je kreiran automatski
- **Grupa**- Facebook grupa
- **Stranica**- Facebook stranica
- **Događaj**- Facebook događaj
- **Objava**- Individualni unos na nečijem profilu
- **Postignuće** (milestone)
- **Status**
- **Link**- link koji je objvljen na zidu korisnika
- **Slika**- individualna slika na Facebook-u
- **Album**
- **Video**- indivudalni video na Facebook-u
- **Komentar**- komentari mogu biti postavljeni na različitim sadržajima u okviru Facebook-a
- **Poruka**- individualna poruka u Facebook sistemu slanja poruka
- **Ćaskanje**- Facebook poruke između osoba
- **Aplikacija**- Facebook aplikacija. Aplikacije se kreiraju, održavaju i brišu u App dashboard-u

6.2 Facebook Artefakti

Forenzički artefakti su forenzički objekti koji imaju neku forenzičku vrednost. Bilo koji objekat koji sadrži neke podatke ili dokaze nečega što se desilo, kao što su logovi, registri...

Generalno postoje 6 specifičnih kategorija artifakta koji se mogu pojedinačno identifikovati kada se ispituje hard disk računara:

1. **Facebook Chat -** Ovaj artefakt se najčešće nalazi u memoriji kao JavaScript tekst u JSON formatu na računaru koji radi i/ili u datoteci pagefile.sys i hiberfil.sys.

Slika 3 – Tekst u JSON formatu

2. **Facebook poruke -** Facebook chat i poruke su sada isti artefakt, ali u starijim verzijama Fejsbuka to su bile dva različita artefakta. Ovaj artefakt se najčešće nalazi u memoriji računara koji radi i/ili pagefile.sys i hiberfil.sys.

3. **Facebook objave na zidu/statusi komentari/updejti –** HTML koji je izvučen iz privremenih internet fajlova/web keševa i memorije

Slika 4- HTML Facebook objava

4. **Facebook fragment web stranice-** Fragment HTML izvučen iz privremenih internet fajlova/web keševa i memorije

5. **Facebook slike-** Facebook slike imaju specifičan obrazac naziva datoteka i nalaze se u privremenim internet datotekama/veb keš memoriji. Ime datoteke sadrži tri skupa brojeva poput sledećeg:
   „1221785571_1221785571_10150672801465915_n.jpg“
   Drugi skup brojeva može ukazivati na Facebook korisnički ID kojem fotografija pripada i može se tražiti preko Facebook-ovog Graph API-ja.

6. **Facebook URLs –** URL u bilo kojem artefaktu web pretraživača koji referencira Facebook URL. Ovi artefakti uglavnom upućuju na druge Facebook korisnike ili određene Facebook aktivnosti.

7.Postojeći softveri za analizu socijalnih mreža

Ne postoji specifični softver koji se koristi za analizu Facebook socijalne mreže. U zavisnoti od toga šta je potrebno analizirati i koje informacije su potrebne, moguće je koristiti neke od trenutno dostupnih softvera za analizu i vizuelizaciju socijalniih mreža.

Do pre nekoliko godina bio je dostupan softver Facebook Forensics Toolkit (FFT) razvijen od strane kompanije Afentis Forensic koji je bio namenjen baš analizi Facebook socijalne mreže, ali on nije više u upotrebi.

Softver za analizu društvenih mreža (SNA) uključuje dva paketa zasnovana na grafičkom korisničkom interfejsu (GUI) ili na paketima napravljenim za programiranje/skriptovanje. GUI paketi su generalno lakše naučiti dok su programski alati moćni i proširivi.

Karakteristike softvera za analizu društvenih mreža su proračun mrežnih standarda i statistike, kreiranje matrice susednosti, ivica liste, ili ivice, vizuelizacija i još mnogo toga. Vizuelna prezentacija ili vizuelizacija društvenih mreža koje ustvari predstavljaju razumevanje mrežnih podataka i rezultat analize su veoma važni. Vizuelizacija je često objektat kvalitativne mreže podataka koja uključuje grafikone, tabele, vremenske linije, karte i druge izolovani slučajeve. Takođe se može koristiti za izolovanje podataka.

Neki od softvera su:

Software SocNet

Multi-platformski softver prilagođen korisniku za analizu i vizualizaciju društvenih mreža. Ovaj softver omogućava kreiranje društvene mreže u nekoliko koraka na virtuelnom platnu ili učitavanje podataka društvenih mreža u različitim formatima. Izračunavanje statističkih pokazatelja, kreiranje nasumična mreža automatski, uključujući veb pretraživač, jednostavan korisnički interfejs, podršku za učitavanje i uređivanje višestrukih odnosa. Algoritam rasporeda za grafikone, koeficijent grupisanja, klikova, koji automatski obnavlja nepoznati SN skup podataka je proširiv.

NodeXL

Ova aplikacija ima spreman i fleksibilan okvir u Excel okruženju za Microsoft u 2007, 2010 i 2013, što olakšava otkrivanje obrazaca i lako prikazivanje grafičke mreže kao izlaz. Neke karakteristike ovog softvera su: kreiranje novih ivica na osnovu sličnosti, izračunavanje statističkih kriterijuma, vektor centralnosti, koeficijent grupisanja, rangiranje stranica, fleksibilan raspored, zumiranje, dinamičko filtriranje, otkrivanje zajednica, pristup dodacima, direktna veza sa socijalnim mrežama kao što su Facebook, e-pošta, tviter i druge društvene mreže.

Graph-tool

Ova aplikacija je efikasan modul za statističku analizu grafikona i vizuelizaciju društvene mreže. Softver ima višejezgarnu arhitekturu. Neke od njegovih karakteristika su: pogodan interfejs za Graphviz pakete, podržava ivice, čvorove i svojstva grafova, izračunava statističke kriterijume, implementira topološke standardne algoritme, detektuje module i zajednice putem statističkog zaključivanja, mnogi algoritmi se implementiraju korišćenjem biblioteka paralelno, koristi graf ML, u stanju je da filtrira čvorove i ivice.

Pajek

Ovaj softver je dizajniran da transformiše mrežu u manje mreže i da ih analizira i vizuelizuje. Neke karakteristike ovog softvera su: koristi 6 struktura za implementaciju algoritma: mrežu, vektor, grupisanje, particionisanje, hijerarhijski, permutacija, izračunava statistički kriterijum, izdvaja podmreže, eliminiše petlje u mreži, implementira splc-kn-cpm metode, izbegava grupisanja u mreži, skalabilno, 3D vizuelizacija , implementira algoritam rasporeda , identifikuje jake i slabe veze, identifikuje mrežni prag, menja redosled mreže, podržava različite jezike za datoteke sa podacima.

Meerkat

Softver za analizu teksta, koji automatski sumira velike količine teksta i povezuje njegovo društveno umrežavanje. Koristi onlajn razgovore na sajtovima kao što su Facebook, Youtube i tako dalje. Softver se prventveno pojavio kao pomoć lekarima da analiziraju podatke u vidu društvenih mreža. Neke karakteristike ovog softvera su: može se razvijati i pruža informacije o najuticajnijem centralnom čvoru, vizuelizira mrežu, uređuje interaktivne mreže, podržava dinamičku mrežu, izračunava statističke metrike, identifikuje populacije, podržava biblioteke C ++.

Takodje mogu se koristiti i softveri koji služe za ekstrakciju dokaza, koji nisu specijalno dizajnirani za socijalne mreže, već imaju sposobnost da oporave, pregledaju ili analiziraju podatke iz drugih tehnologija koje su prisutne i u forenzici socijalnih mreža. Neki od njih su: **CacheBack**, **Internet Evidence Finder (IEF)** i **EnCase Forensic**.

U sledećoj tabeli se nalazi prikaz nekih Internet artifakta koji se specifično odnose na dokaze socijalnih mreža, pristuna je i kolona koja daje detalje o lokaciji određenog artefakta. Ovi artefakti se mogu obrađivati nekim od već postojećih softvera za ekstrakciju dokaza.

Artefakt	Opis dokaza	Primarna lokacija podataka
Internet istorija	Lista posećenih URL-ova	Baza podataka pretraživača
Web stranice	Web sajt podaci i fajlovi (html)	Keš pretraživača pagefile.sys, hiberfil.sys

Sesija	Kolaćići i drugi podaci sesije	Fajlovi profila pretraživača Keš pretraživača
Slike	Slike, npr jpeg slike	Keš pretraživača pagefile.sys, hiberfil.sys
Video	Video fajlovi	Keš pretraživača pagefile.sys, hiberfil.sys
Email	Email koji obezbeđuje socijalna mreža	Podaci email klijenta
Preuzimanja (Downloads)	Materijal koji je preuzet	Keš pretraživača Privremeni fajlovi

Tabela 1- Artefakti

Prema istraživanju koje je sprovedeno nad ovim artefaktima koristeći alate za ektrakciju dokaza, došlo se do zaključka da je veliku broj dokaza socijalnih mreža moguće ispitati na ovaj način.

8. Zaključak

Socijalne mreže su bitan deo našeg svakodnevnog života, predstavljaju jedan od glavnih načina komunikacije.

Grana forenzike koja se bavi socijalnim mrežama je još uvek u razvoju. Postoje razni limiti kada je u pitanju pribavljanje i analiza informacija, koji variraju u zavisnoti od socijalne mreže, što dodatno otežava proces digitialne forenzike. Takođe pristup socijalnim mrežama je dostupan ne samo preko web pretraživača nego i preko mobilnnog telefona, što povlači još problema prlikom korišćenja konvencijalnih alata digitalne forenzike za prikupljanje i analizu podataka.

Trenutno na tržištu ne postoji softveri namenji specifičnim socijalnim mrežama, taj problem se donekle prevazilzi korišćenjem kombinacija nekih od postojećih alata.

Dokazi sa socijalnih mreža imaju potencijal da budu jako bitni u istragama koje obavlja digitalna forenzika. Neophodno je razvijati inovativne i bolje načine predstavljanja informacija istražiteljima. Heterogenost na socijalnim mrežama predstavlja značajan problem koji je potrebno prevazići i razviti konzistentne i efektivne alate za forenziku socijalnih mreža.

Prvi deo seminarskog rada govori o socijalnim mrežama, podacima i načinima vizuelizacije. Zatim je predstavljen formalni model znanja sa socijalne mreže. U poslednjem delu ovog rada se govori o Graph API-ju i Facebook Artefaktima, kao i o postojećim softverskim rešenjima.

9. Literatura

[1] H. Arshad, A. Jantan and G.K. Hoon, Computers & Security, 2020

[2] https://developers.facebook.com/docs/graph-api/

[3]Brian Brian Cusack1 and Jung Son AUT University, Auckland, New Zealand, Evidence examination tools for social networks

[4] Miroslav Baca1 ,Jasmin Cosic,Zoran Cosic, Centre for biometrics, Faculty of Organization and Informatics, Varazdin, Croatia, Forensic Analysis of Social Networks (Case Study)

[5] Markus Huber, Martin Mulazzani, Manuel Leithner, Sebastian Schrittwieser, Gilbert Wondracek, Edgar Weippl, Vienna PhD school of informatics, Social Snapshots: Digital Forensics for Online Social Networks

[6] Muhammad Firdaus,(Department of Information Security, Graduate School Pukyong National University, Forensic Analysis of Social Media Data

[7] https://www.w3.org/wiki/Socialwg/Social_API/Facebook_API

[8] https://www.magnetforensics.com/resources/how-important-are-facebook-artifacts-2/

[9]Nasrin Jokar, Ali Reza Honarvar, KhadijehEsfandiari, Shima Aghamirzadeh, Department of Electrical and Computer Engineering, Safashahr Branch, Islamic Azad University, Safashahr, Iran, The review of social networks analysis tools