UNIVERZITET U NIŠU

ELEKTRONSKI FAKULTET

Danica Đorđević

Forenzika mrežnog saobraćaja

Digitalna forenzika

Student: Danica Đorđević 1121

Niš, 2021. god.

Sadržaj

1. UVOD

Internet je mreža koja je zauvek promenila način života ljudi, komunikacije i poslovanja. Velika ekspanzija interneta je dovela i do zloupotrebe informacija koje se prenose putem globalne mreže. Iako nam Internet nudi mnoge pogodnosti i olakšava komunikaciju, poslovanje i razmenu podataka, on ima i svoje mane u polju bezbednosti. Mnoge informacije na Internetu su osetljive i kao takve, neophodno je osigurati njihov bezbedan prenos od jedne mašine na drugu. Zbog slabe bezbednosti je danas sve veći broj hakerskih napada, krađe podataka, zloupotrebe poverljivih podataka, slanje malicioznih programa, itd. Sve ovo spada u kompjuterski kriminal. Otkivanjem dokaza za ovu vrstu kriminala bavi se digitalna forenzika. Njen glavni zadatak jeste da prikupi digitalne dokaze kojima će da ospori ili potvrdi neku tvrdnju na prekršajnom sudu. To znači da se digitalna forenzika bavi rekronstrukcijom oštećenih i pronalaženjem skrivenih ili šifrovanih podataka. Postoji dosta grana digitalne forenzike, a neke od njih su:

- forenzika računarskog sistema,
- forenzika mrežnog saobraćaja,
- forenzika mobilnih uređaja,
- forenzika za analizu podataka,
- forenzika baza podataka.

Kriminalom na mreži bavi se posebna grana digitalne forenzike, a to je forenzika mrežnog saobraćaja, koja će biti obrađena u ovom radu.

Mrežni forenzičari se bave bezbednošću mreža, otkrivanjem napada, neovlašćenih pristupa i zloupotrebe mreža. Njihov zadatak je da detektuju bilo kakve anomalije i preuzmu adekvatne mere. Detekcija anomalija se vrši praćenjem i analizom mrežnog saobraćaja, kako lokalnog (LAN), tako i spoljašnjeg (WAN/Internet). Sadržaj se obično prikuplja u vidu paketa i

skladišti za kasniju analizu ili se analizira i filtrira u realnom vremenu. Može se, prema tome, izvršiti podela sistema mrežne forenzike na:

- "Uhvati kako možeš" sistemi - u kojima se svi paketi koji prolaze kroz određeni saobraćajni deo beleže, zapisuju i skladište, a analiza se vrši naknadno. Ovaj pristup zahteva veliki kapacitet za skladištenje, koji obično uključuje RAID sisteme.
- "Stani, gledaj i slušaj" sistemi - u kojima se svaki paket analizira, a samo neki se beleže i skladište za buduću analizu. Ovaj pristup zahteva manji kapacitet za skladištenje, ali zato zahteva brži procesor kako bi pratio dolazni mrežni saobraćaj.

Mrežna forenzika, pored analize mrežnih paketa, uključuje i analizu mrežne opreme: rutera, svičeva, habova, mrežnih kartica, optičkih kablova, itd.

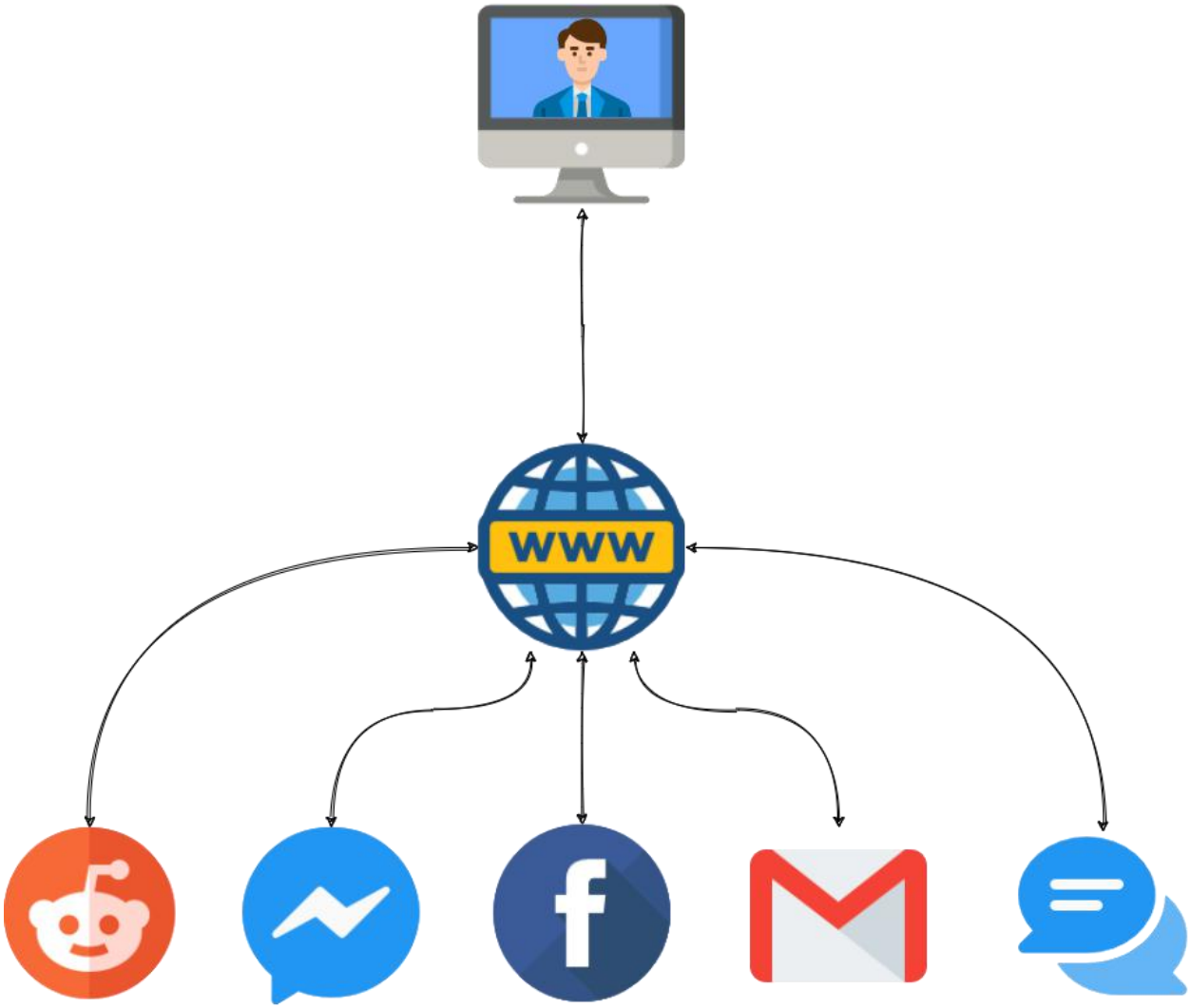
2. IMPLEMENTIRANI MREŽNI ALAT

Implementirani mrežni alat ima za cilj da uoči, filtrira i vizuelizuje unapred prikupljene mrežne podatke. Ovaj alat se koristi za prikupljanje informacija koje govore o tome sa kojim serverima se najviše komuniciralo, razmenjivalo paketa. Takođe se može videti i sa kojim tipom servera se komuniciralo. Klasifikacija servera je izvršena po reklamama, CDN servisima i samim sajtovima.

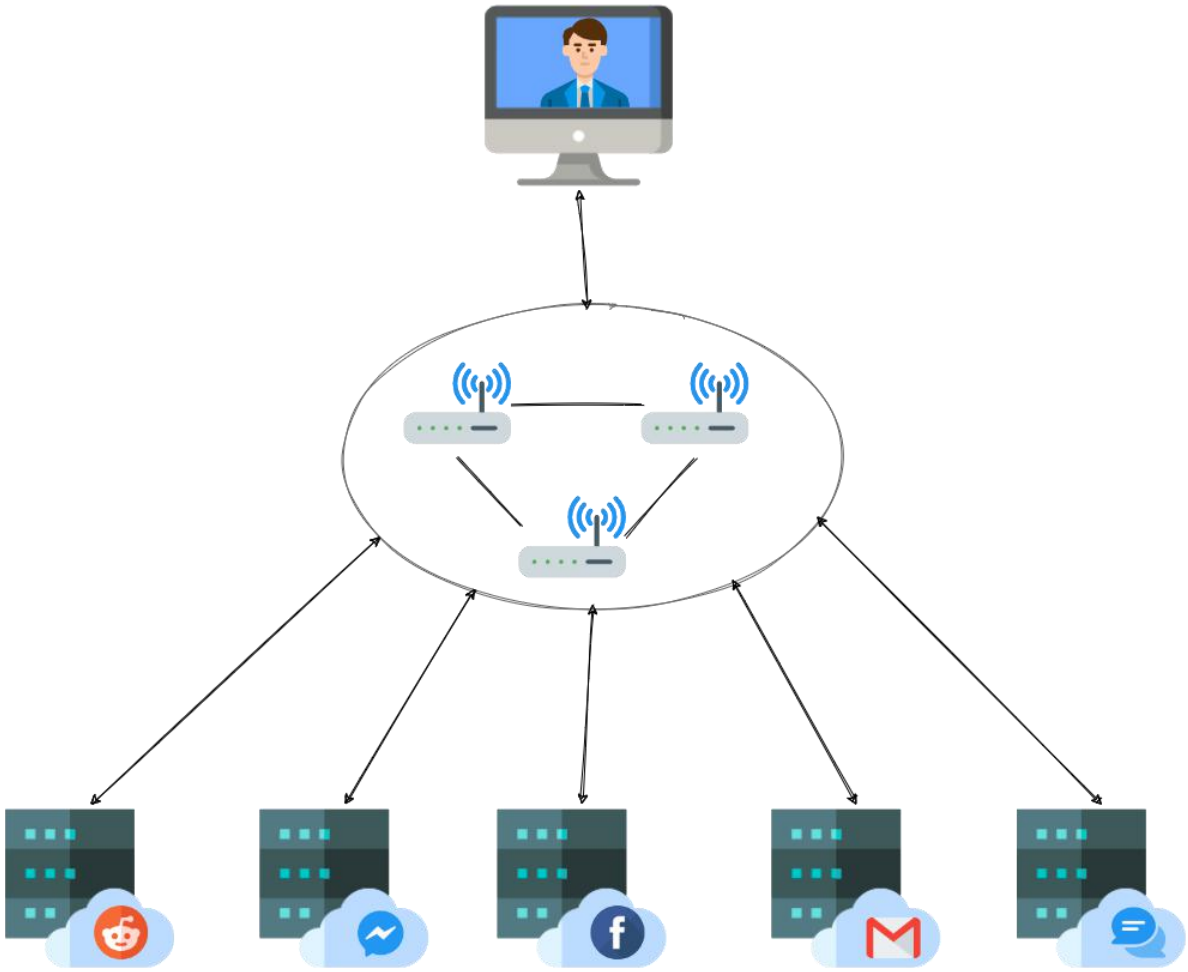
2.1. Prikupljanje podataka

Alat analizira prikupljene mrežne pakete sa korisničkog računara. Tu je moguće ujedno pratiti i lokalni i spoljašnji saobraćaj. Podaci se prikupljaju i skladište u fajl formatu *.pcapng* korišćenjem mrežnog alata Wireshark. Zatim se tako prethodno sačuvani podaci propuštaju kroz implementirani alat, koji ih filtrira i analizira.

Proces prikupljanja mrežnih podataka počinje posetom različitih sajtova od strane korisnika. U procesu prikupljanja mrežnih podataka, korisnik zapravo komunicira sa različitim udaljenim serverima. Oni služe da korisniku dostave različite delove posećene web strane. Serveri mogu biti zaduženi za dostavljanje reklama, resursa, html strana, itd. Komunikacija između korisnika i udaljenih servera se obavlja preko različitih mrežnih protokola. U ovom radu su posmatrani paketi na transportnom nivou: TCP, UDP. Analizu paketa na aplikativnom nivou je teže realizovati, jer većina protokola koristi bezbednosne mehanizme kao što je enkripcija podataka, pa je obavljanje analize otežano. Komunikacija korisnika sa udaljenim serverima je data na slikama 1 i 2.



Slika 1. Komunikacija korisnika sa servisima na Internetu



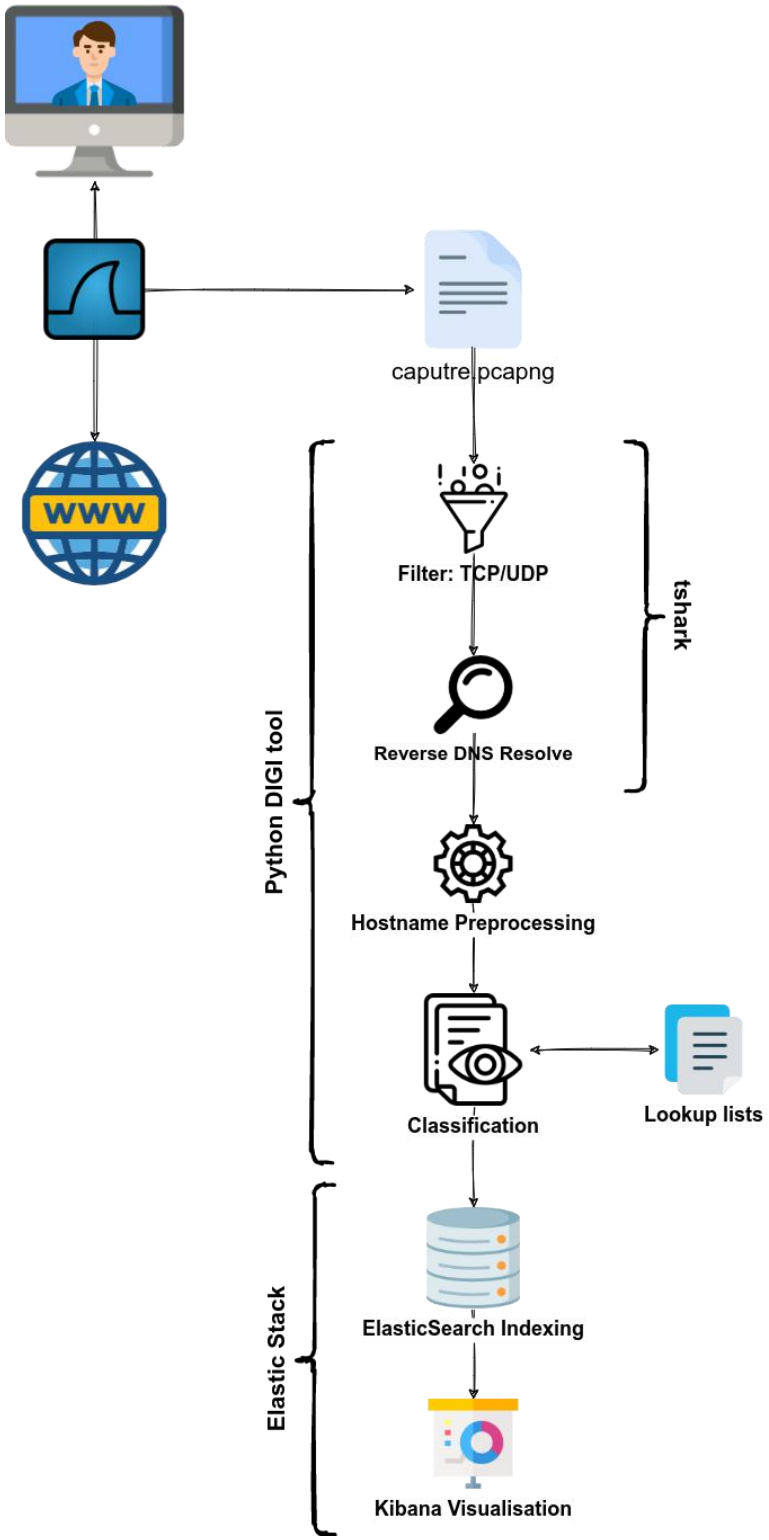
Slika 2. Prikaz komunikacije korisničkog računara sa udaljenim serverima

2.2. Analiza paketa

Implementirani mrežni alat analizira pakete na transportnom nivou. Analiza paketa se izvršava u nekoliko etapa:

1. Filtriranje paketa
2. Propuštanje paketa kroz obrnutu DNS pretragu
3. Procesiranje hostname-a
4. Klasifikacija hostname-a po tipu
5. Indeksiranje podataka u Elasticsearch-u
6. Vizuelizacija podataka u Kibana alatu

Svih šest etapa su prikazane na slici 3.



Slika 3. Proces analize paketa

Prva faza analize podataka jeste filtriranje paketa. Među snimljenim mrežnim podacima, mogu se naći različite vrste paketa, kao što su:

- **HTTP** paketi (Hyper Text Transfer Protocol) - protokol aplikativnog nivoa , koji prenosi neenkriptovane podatke kao što su internet stranice sa jednog host računara na drugi,
- **HTTPS** paketi (Hyper Text Transfer Protocol Secure) - protokol aplikativnog nivoa , koji prenosi enkriptovane podatke kao što su internet stranice sa jednog host računara na drugi,,
- **DNS** paketi (Domain Name System) - protokol na aplikativnom nivou, koji prevodi IP adrese u čitljiva imena,
- **SSH** paketi (Secure SHell) - protokol na aplikativnom nivou, koji stvara siguran kanal između host računara na mreži,
- **ARP** paketi (Addres Resolution protocol) - protokol sloja veze, koji pronalazi MAC adresu na osnovu poznate IP adrese hosta,
- **TCP** paketi (Transmission Control Protocol) - protokol na transportnom nivou, koji obezbeđuje pouzdan prenos paketa,
- **UDP** paketi (User Datagram Protocol) - protokol na transportnom nivou, koji se koristi u slučajevima kada ne mora biti zagarantovan pouzdan prenos svih paketa, kao što je video striming,
- **POP3** (Post Office Protocol version 3) - protokol na aplikativnom nivou, koji pribavlja elektronske poruke sa mreže,
- **SMTP** (Simple Mail Transfer Protocol) - protokol na aplikativnom nivou, koji se koristi za slanje elektronske pošte preko mreže,
- **FTP** (File Transfer Protocol) - protokol na aplikativnom nivou, koji pomaže u prenosu podataka sa jednog host računara na drugi, preko mreže,
- **GQUIC** paketi - protokol na transportnom nivou, koji poboljšava performanse connection-oriented web aplikacijama uspostavljanjem određenog broja multipleksiranih veza između dve krajnje tačke koristeći UDP,
- Ostali paketi.

Neki od prethodno spomenutih paketa nisu od značaja za analizu na transportnom nivou, s toga ih je neophodno eliminisati, a propustiti kroz dalju analizu pakete koji su od značaja. Iz skupa mnogobrojnih protokola, implementirani alat izdvaja TCP i UDP protokole kao relevantne. Takođe je neophodno eliminisati sve DNS pakete, s obzirom da je komunikacija sa DNS serverima neizbežna, oni su nerelavtni za dalju analizu i statistiku. Iz postojećih paketa su, takođe, izdvojeni samo oni koji nose podatke o komunikaciji korisnikovog računara sa udaljenim serverom. Za analizu se koriste paketi koji su razmenjeni u komunikaciji između jednog specificiranog računara (u ovom slučaju korisnikov računar) i ostatka mreže. Ostali paketi, kao što su broadcast paketi i paketi između drugih hostova u mreži, nisu razmatrani. Iskorišćeni filteri su prikazani na slici 4.

```
f"ip.addr == {target_address} && (tcp || udp) && !dns"
```

Slika 4. Iskorišćeni filteri

U drugoj fazi analize je obavljena obrnuta DNS pretraga. U ovoj pretrazi se vrši preslikavanje IP adrese servera na njegovo simboličko ime. Sistem Internet domena (DNS - Domain Name System) je bazni Internet servis, koji omogućava prevođenje Internet domena u IP adrese i obrnuto. Može se desiti da je više različitih domena vezano za istu IP adresu, kao što je to slučaj sa deljenim serverima. Snimljeni paketi u *.pcapng* formatu sadrže samo IP adrese odredišta i izvora. Za analizu su mnogo pogodnija simbolička imena odredišta i izvora, stoga je urađena obrnuta DNS pretraga. Za implementaciju obrnute DNS pretrage je iskorišćena funkcionalnost *tshark* alata (terminalski alat Wireshark-a), koja na osnovu sačuvanih DNS paketa u *.pcapng* fajlu mapira IP adrese na njihovo simboličko ime. Flegovi koji aktiviraju ovu funkcionalnost tshark-a su prikazani na slici 5.

```
f"-NmnNtdv",
```

Slika 5. Aktivirani flegovi za omogućavanje obrnute DNS pretrage u tsharku.

Treća faza analize predstavlja procesiranje host imena. U ovoj fazi se iz imena hosta izvlače:

- TLD (Top Level Domain),
- FLD (Free Level Domain),
- domen,
- poddomen.

Domen najvišeg nivoa (eng. Top Level Domain) predstavlja najviši domen u hijararhijskom sistemu domena na Internetu. Na primer, u adresi *mail.yahoo.co.uk* domen najvišeg nivoa predstavlja *co.uk*. Odgovornost za upravljanje većinom domena najvišeg nivoa je dodeljena određenim organizacijama od strane Internet korporacije za dodeljena imena i brojeve (ICANN - Internet Corporation for Assigned names and Numbers).

Domen predstavlja tekstualnu oznaku koja identifikuje skup uređaja ili Internet servisa, povezujući ih u jedinstvenu administrativno-tehničku celinu. Domen se najčešće sastoji od niza alfanumeričkih simbola. Dužina imena ne sme biti kraća od dva, niti duža od šezdeset tri. Takođe, ime domena ne sme da sadrži crticu na kraju ili početku naziva. Na primer, u adresi *mail.yahoo.co.uk*, domen predstavlja *yahoo*.

FLD predstavlja spoj domena i domena najvišeg nivoa. Na primer, u adresi *mail.yahoo.co.uk*, *yahoo.co.uk* predstavlja FLD.

Poddomen je dodatni deo FLD-a. Poddomeni su kreirani za organizovanje i navigaciju do različitih sekcija sajta. Na primer, u adresi *mail.yahoo.co.uk*, poddomen predstavlja *mail*.

Za izvlačenje ovih podataka iz host imena, iskorišćena je *tld* python biblioteka. Ova biblioteka koristi *publicsuffix.org* listu domena za razbijanje na delove imena hostova.

Četvrta faza analize predstavlja klasifikaciju servera po tipu sadržaja koji dostavljaju. Podela je izvršena u 3 klase:

- ads,
- assets,
- site.

Host ime se upoređivalo sa listom poznatih host imena. Postoje liste poznatih *ads* servera i poznatih *assets* servera. Upoređivanje se vršilo sa tim listama. Ukoliko se host ime ili deo host imena nalazi u listi hostova koji dostavljaju reklame, to host ime bi se klasifikovalo kao dostavljač reklama tj. kao *ads*. Ukoliko bi se host ime nalazilo u listi poznatih dostavljača resursa, to host ime bi se klasifikovalo kao *assets*. Ako se host ime ne nalazi ni u jednoj listi, onda je to host ime klasifikovano kao *site*.

Lista poznatih dostavljača reklama i resursa je sastavljena na osnovu istih lista koje koriste AdBlock alati i browser ekstenzije:

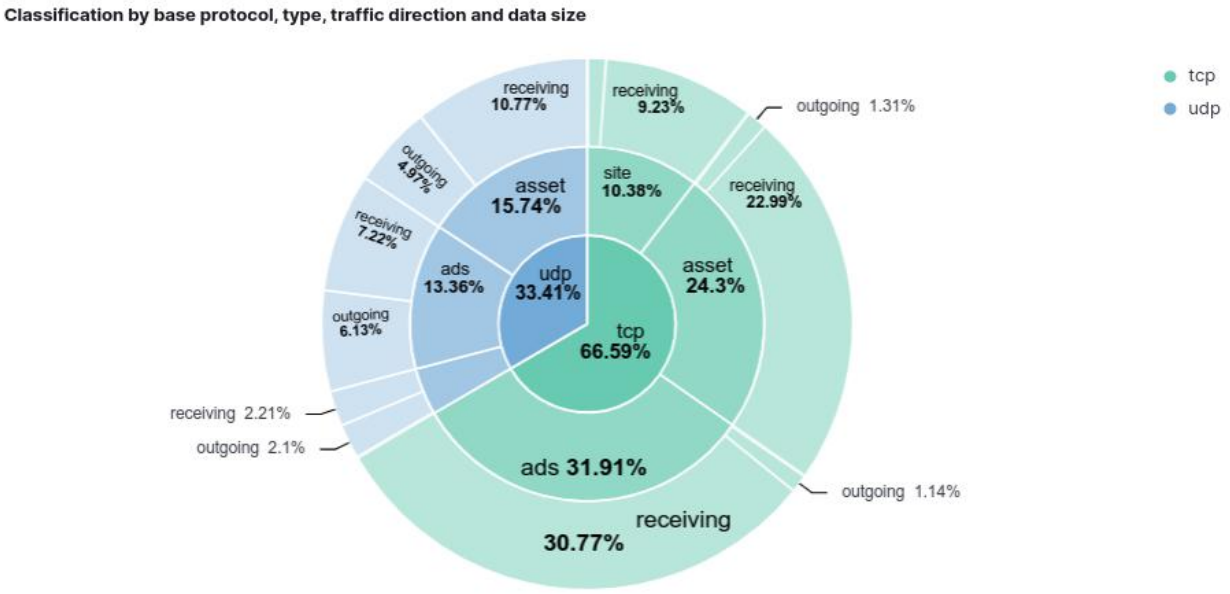
- AdAway
- AdGuardDNS
- AnuDeep
- Disconnect
- EasyList

Lista poznatih dostavljača resursa je generisana na osnovu najpopularnijih CDN provajdera i njihovih poznatih domena.

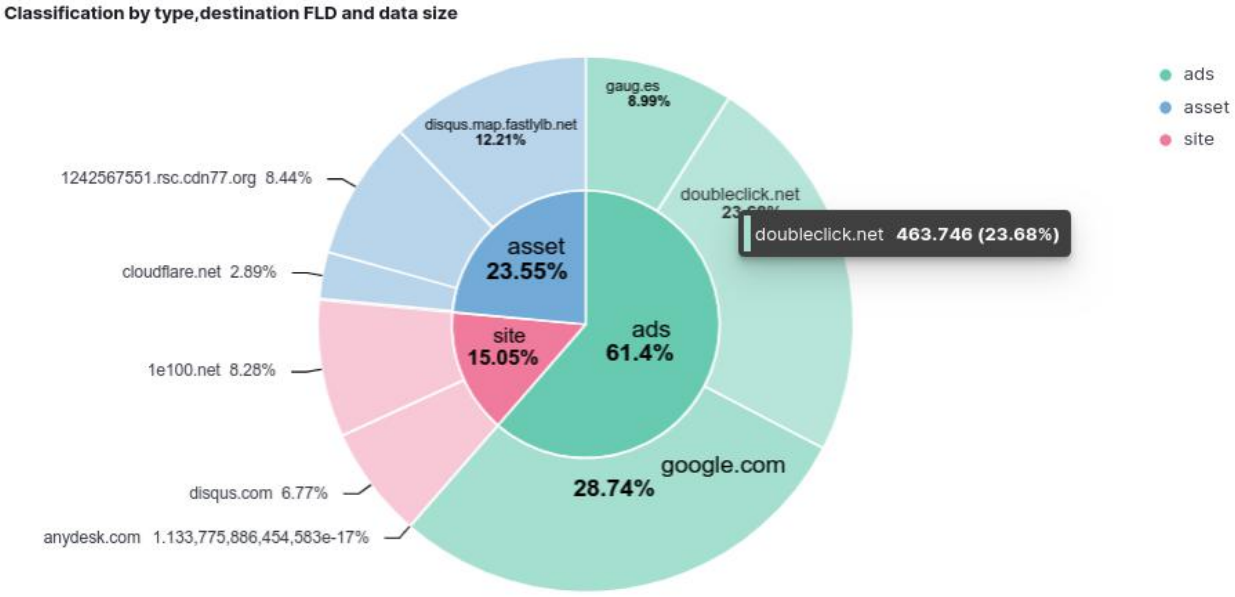
Peta faza je indeksiranje podataka u Elasticsearch bazi. Elasticsearch baza je izabrana zbog brzine pretrage podataka i zbog mogućnosti odabira određenog perioda za koji se statistika prikazuje. Ova baza ima kompatabilnu komponentu za vizuelizaciju - Kibana komponenta.

U završnoj fazi je izvršena vizuelizacija analiziranih podataka. Napravljeni su grafovi za vizuelizaciju:

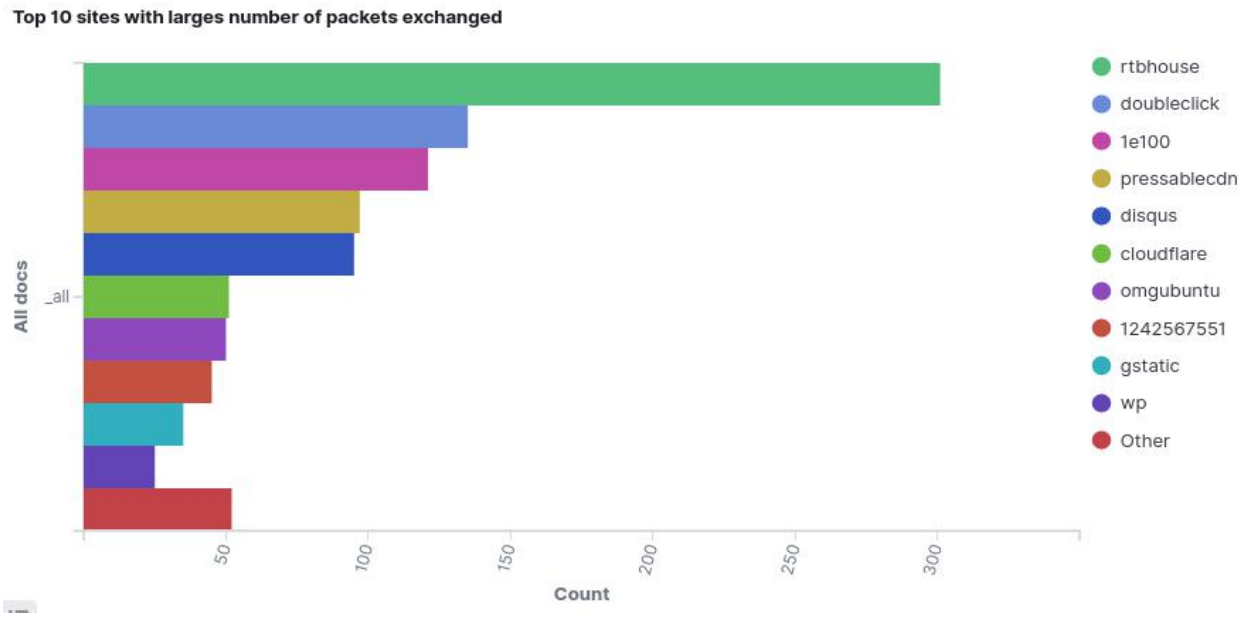
- Klasifikacija po protokolu, tipu servera, smeru saobraćaja i količini razmenjenih paketa (slika 6)
- Klasifikacija prema tipu, odredišnoj FLD adresi i količini razmenjenih paketa (slika 7)
- Prvih 10 sajtova sa kojima je korisnički računar razmenio najveću količinu paketa u bajtovima (slika 8)
- Klasifikacija prema tipu, smeru saobraćaja i količini razmenjenih paketa (slika 9)
- Klasifikacija prema tipu i smeru saobraćaja (slika 10)
- Klasifikacija po tipu, prema količini razmenjenih podataka (slika 11)
- Klasifikacija po tipu, prema broju razmenjenih paketa (slika 12)
- Prvih 20 sajtova po tipu sadržaja koji dostavljaju i količini razmenjenih paketa sa tim sajtovima (slika 13)
- Klasifikacija prema tipu, izvorišnoj FLD adresi i količini razmenjenih paketa (slika 14)
- Broj paketa koji ucestvuje u statistici (slika 15)



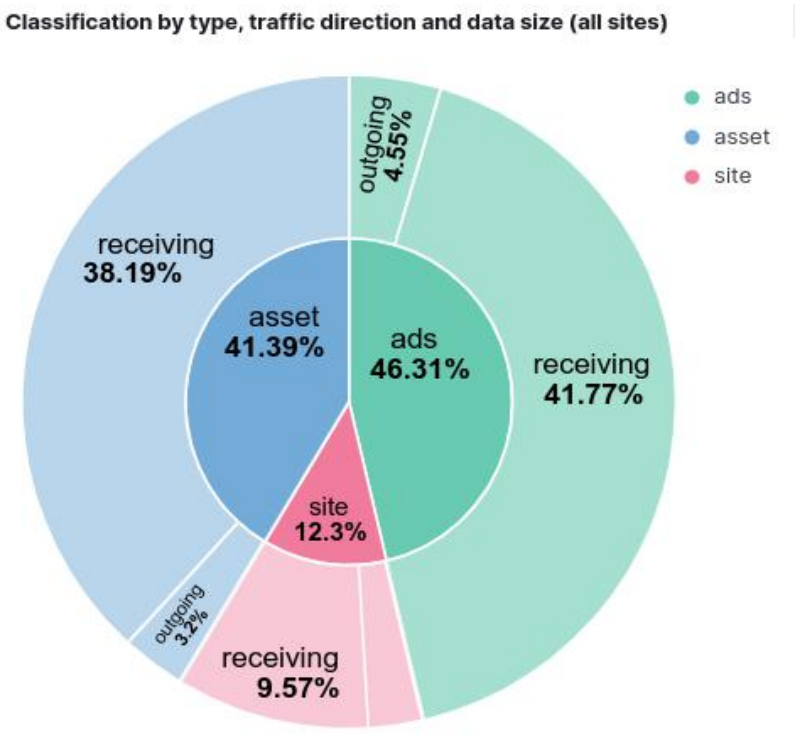
Slika 6. Vizuelni prikaz klasifikacije podataka prema protokolu, tipu servera, smeru saobraćaja i količini razmenjenih paketa



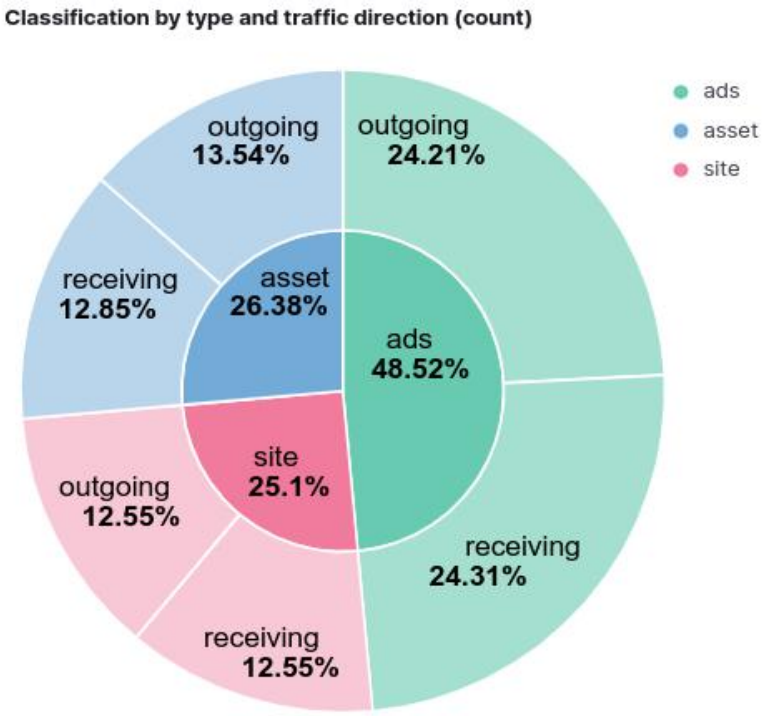
Slika 7. Vizuelni prikaz klasifikacije podataka prema tipu, odredišnoj fld adresi i količini razmenjenih paketa



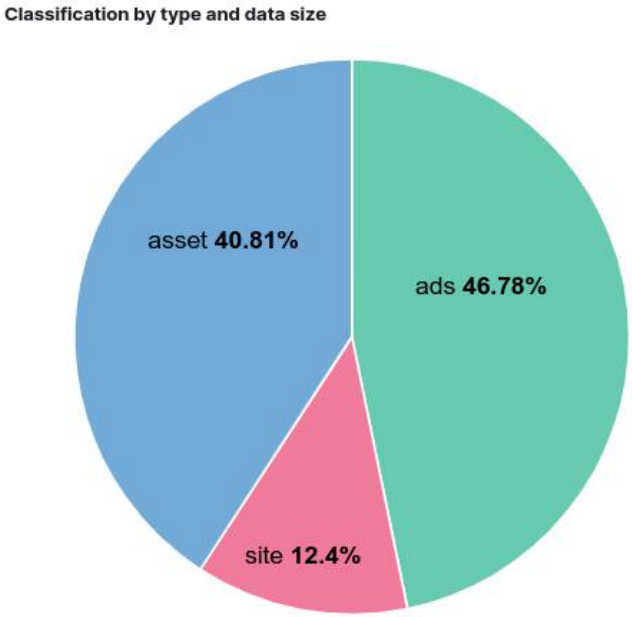
Slika 8. Vizuelni prikaz prvih 10 sajtova sa kojima je korisnički računar razmenio najveću količinu paketa u bajtovima



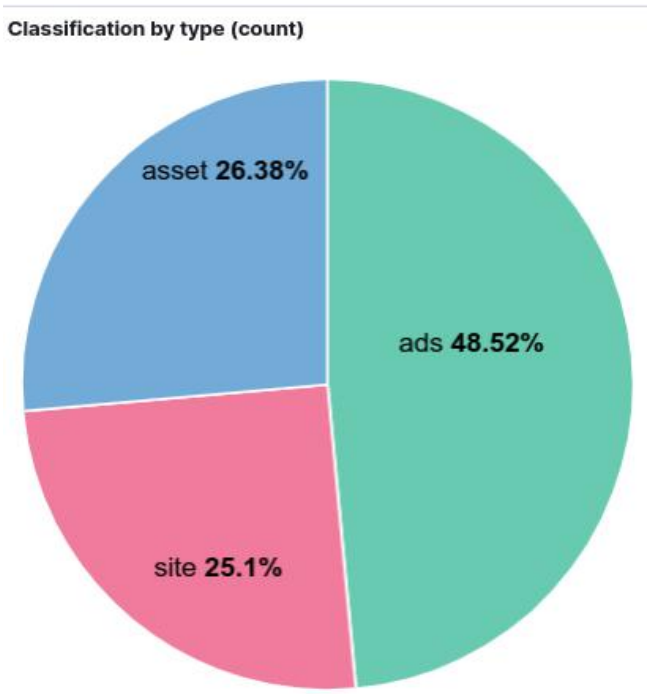
Slika 9. Vizuelni prikaz klasifikacije podataka prema tipu, smeru saobraćaja i količini razmenjenih paketa



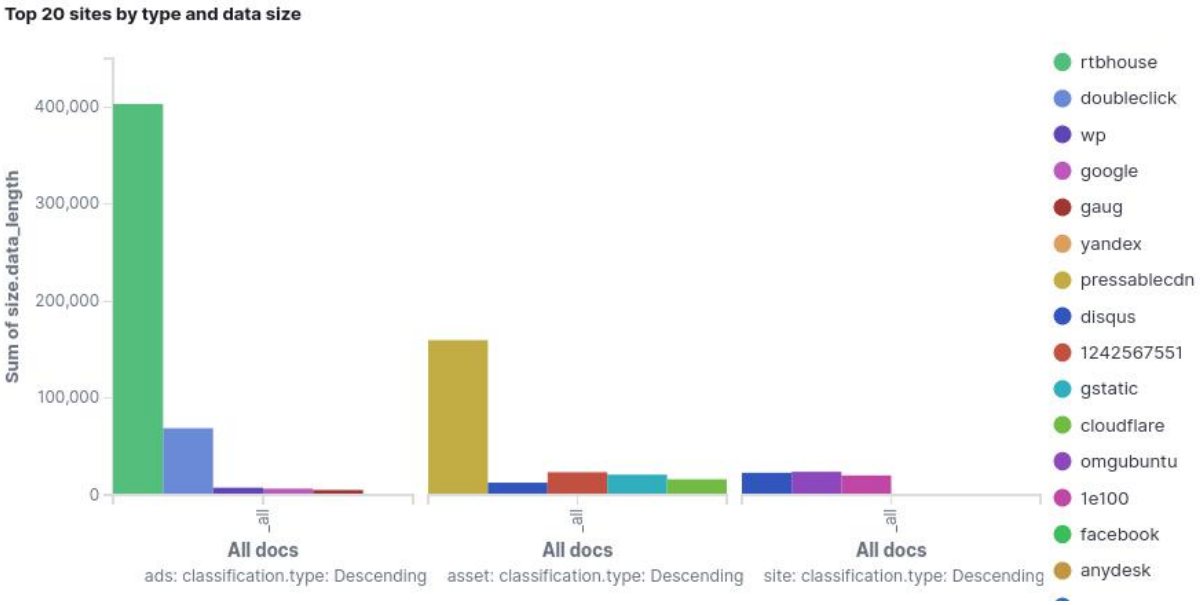
Slika 10. Vizuelni prikaz klasifikacije podataka prema tipu i smeru saobraćaja



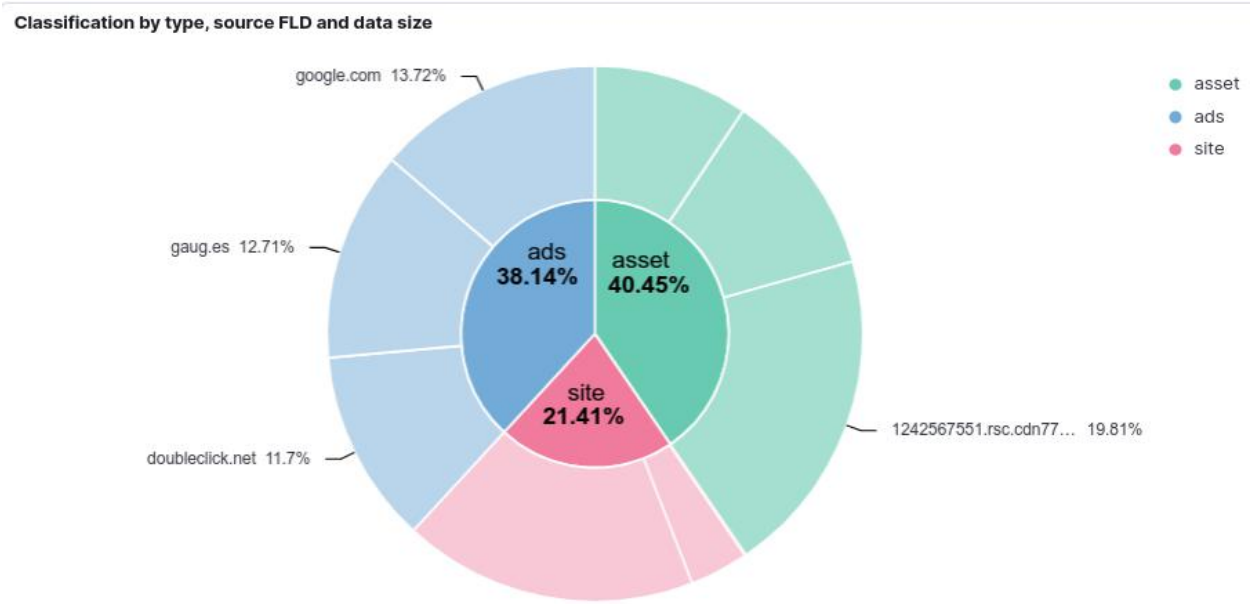
Slika 11. Vizuelni prikaz klasifikacije podataka po tipu, prema količini razmenjenih paketa



Slika 12. Vizuelni prikaz klasifikacije podataka po tipu, prema broju razmenjenih paketa

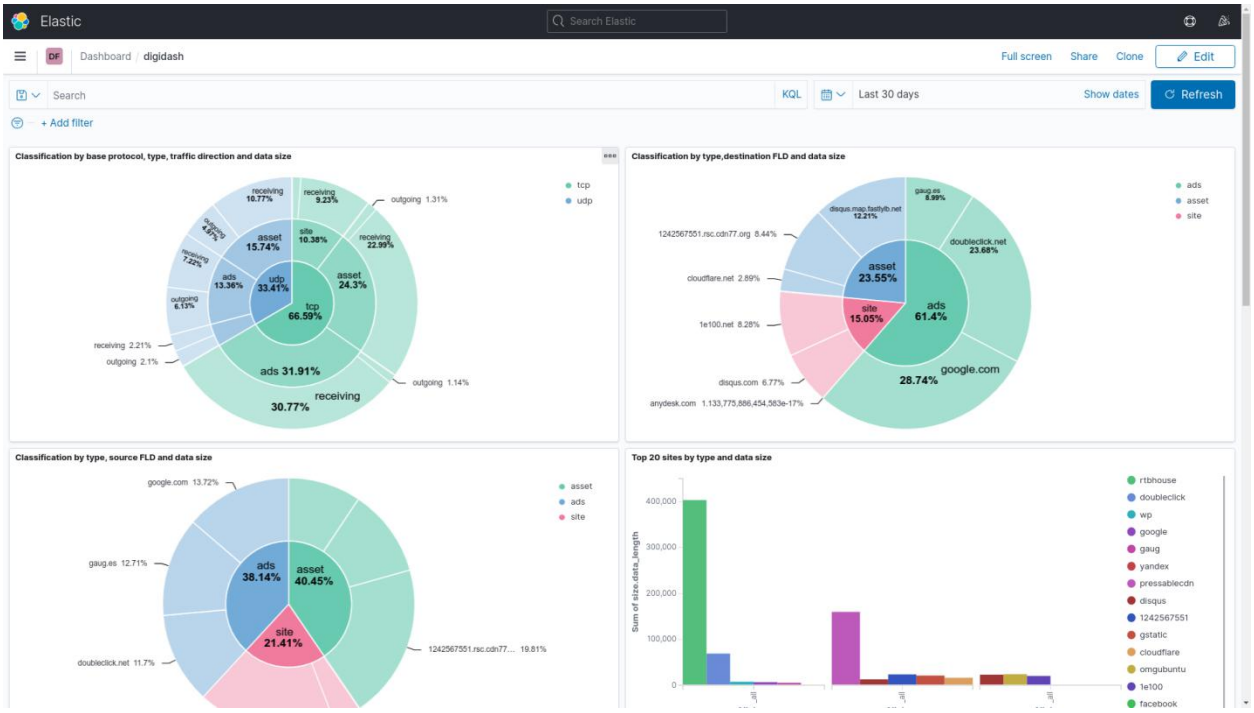


Slika 13. Vizuelni prikaz prvih 20 sajtova po tipu sadržaja koji dostavljaju i količini razmenjenih paketa sa tim sajtovima



Slika 14. Vizuelni prikaz klasifikacije podataka prema tipu, izvorišnoj fld adresi i količini razmenjenih paketa

Slika 15. Vizualni prikaz broja paketa koji ucestvuje u statistici



Slika 16. Kibana panel sa graficima

3. ZAKLJUČAK

Računarska tehnologija se iz godine u godinu sve više razvija i biva dostupnija sve većem broju ljudi. Sve više podataka se kreću mrežom, a neki od njih su poverljivi i osetljivi podaci. Velike korporacije i organizacije su zbog povećanog kriminala na mreži, promenile politiku čuvanja podataka. Zbog toga je neophodno posvetiti posebnu pažnju bezbednosti na internetu, ali i edukaciji ljudi o tome kako da štite svoje podatke na mreži. Danas je sve veći broj napada, krađe digitalnih podataka, kao što su nalozi na društvenim mrežama, Paypal računi i brojevi kartica za plaćanje. Takođe se ostavlja i veliki broj digitalnih dokaza preko mobilnih uređaja, kao što su trenutna lokacija, lista kontakata, tekstualne poruke, logovi poziva, slike, video zapisi, itd. Neophodno je preduzeti određene mere kako bi pojedinac koji koristi usluge na Internetu bio zaštićen. Baš zbog bezbednosti na internetu, mrežna forenzika ima veliki značaj.

4. LITERATURA

[1] https://en.wikipedia.org/wiki/Digital_forensics

[2] https://en.wikipedia.org/wiki/Network_forensics

[3] https://pypi.org/project/tld/

[4] https://github.com/rsalmei/alive-progress

[5] https://en.wikipedia.org/wiki/QUIC

[6] Ratomir Đ. Đokić, Milorad S. Markagić, Forenzika računarskih mreža, pp. 136-145, https://scindeks-clanci.ceon.rs/data/pdf/0042-8469/2013/0042-84691301136D.pdf

[7] Master rad - Razvoj modela i forenzika alternativnih uređaja, Pegor Dumonjić, https://singipedia.singidunum.ac.rs/izdanje/41400-razvoj-modela-i-forenzika-alternativnih-racunarskih-uredjaja

[8] Master rad - Značaj proaktivne forenzike za bezbednost informacionih sistema, Andrijana Đoković, https://singipedia.singidunum.ac.rs/preuzmi/41429-znacaj-proaktivne-forenzike-za-bezbednost-informacionih-sistema/1508