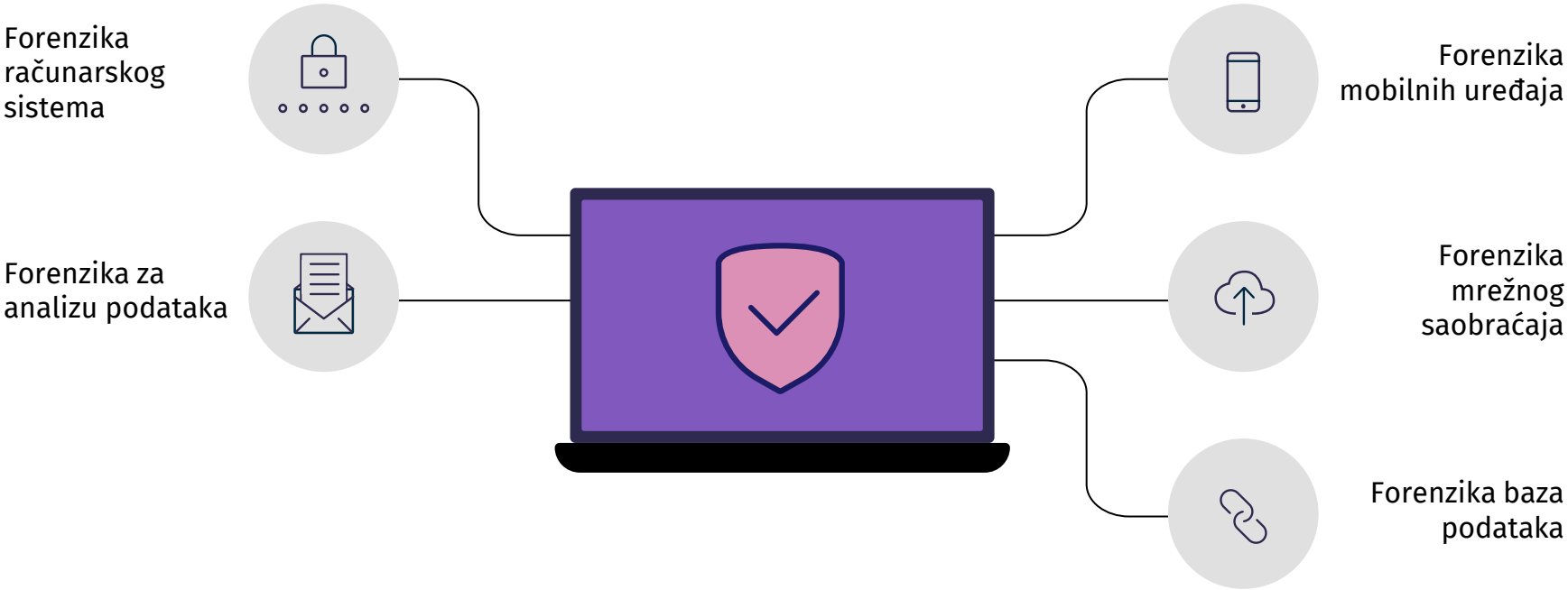
Forenzika mrežnog saobraćaja

Danica Đorđević 1121

Digitalna forenzika

Digitalna forenzika se bavi otkrivanjem dokaza kompjuterskog kriminala. 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 rekonstrukcijom oštećenih i pronalaženjem skrivenih ili šifrovanih podataka.

Grane digitalne forenzike



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,
- samim sajtovima.

Prikupljanje podataka

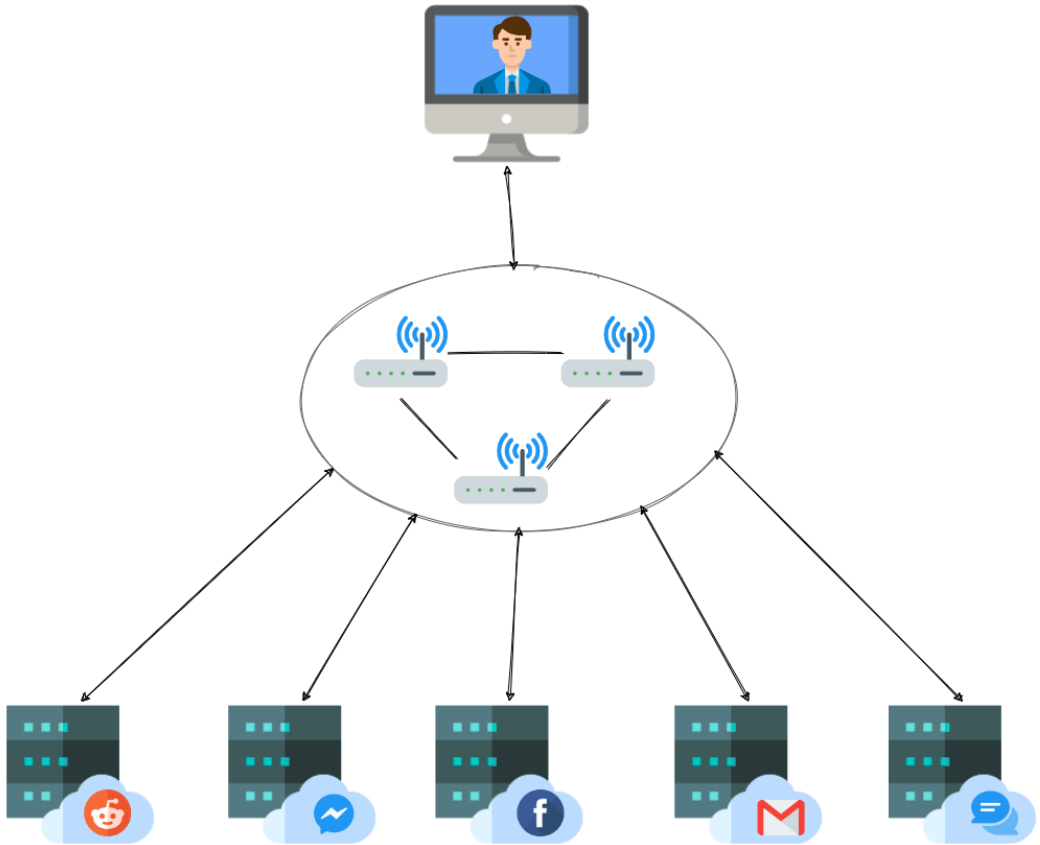
Cshat

Facebook

Mail

Reddit

Komunikacija sa udaljenim serverima

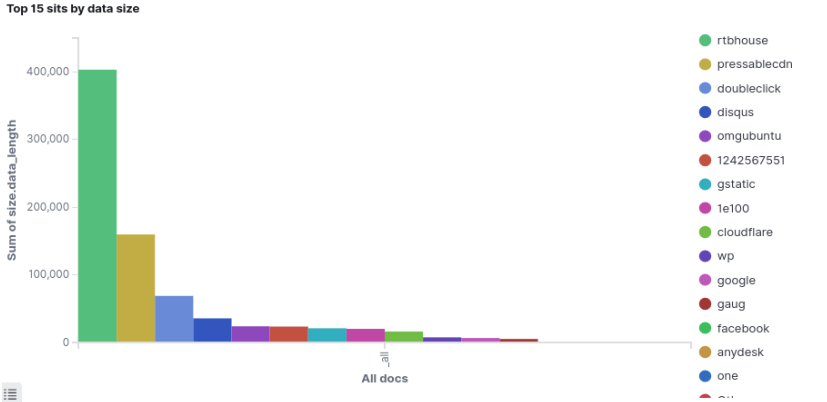


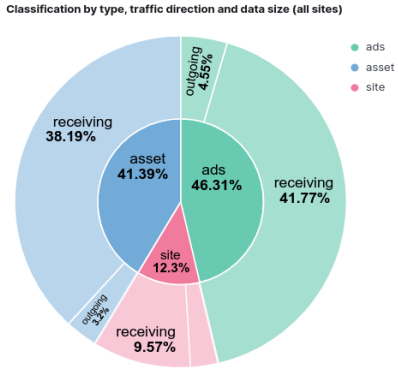
Analiza paketa

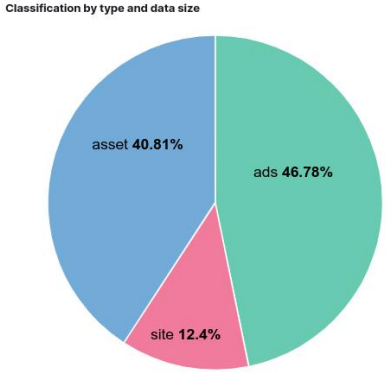
Implementirani mrežni alat analizira pakete na transportnom nivou. Analiza paketa se izvršava u nekoliko etapa:

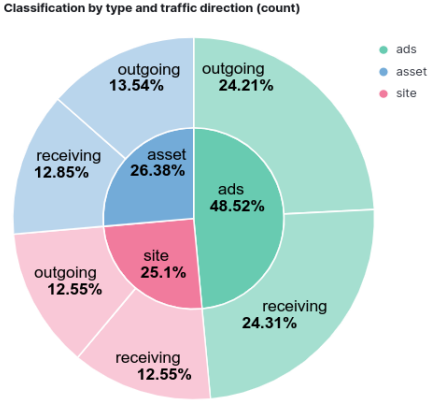
1. Filtriranje paketa
2. Propuštanje paketa kroz obrnutu DNS pretragu
3. Procesiranje hostname-a
4. Klasifikacija hostname-a po tipu
5. Indeksiranje podataka u Elasticsearch-u
6. Vizuelizacija podataka u Kibana alatu

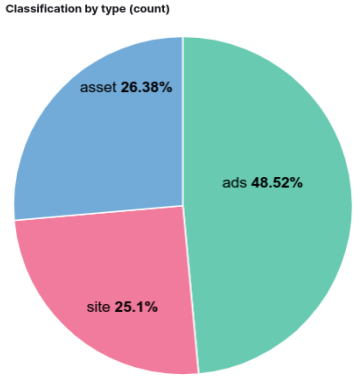
Vizuelizacija podataka

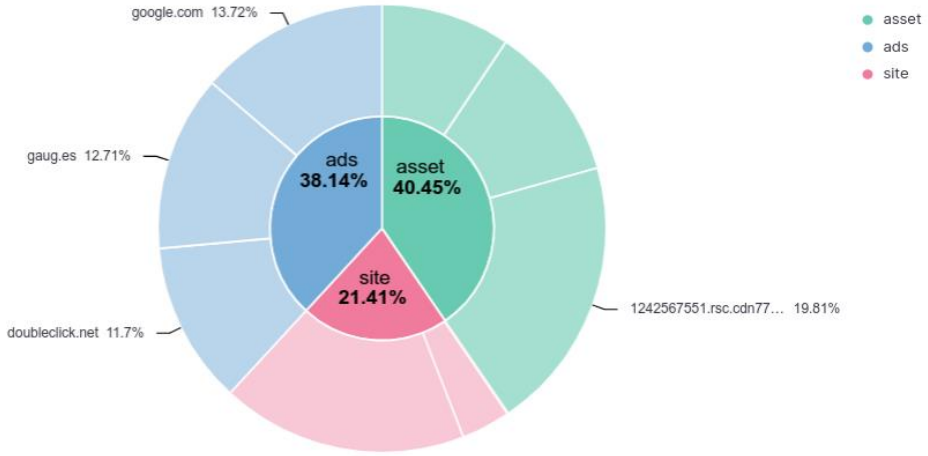












Hvala na pažnji.