Centar Informacijske Sigurnosti

Programski alat Maltego

lipanj 2011.

CIS-DOC-2012-05-048

Upozorenje

Podaci, informacije, tvrdnje i stavovi navedeni u ovom dokumentu nastali su dobrom namjerom i dobrom voljom te profesionalnim radom CIS-ovih stručnjaka, a temelje se na njihovom znanju i petnaestak godina iskustva u radu u informacijskoj sigurnosti. Namjera je da budu točni, precizni, aktualni, potpuni i nepristrani.

Ipak, oni su dani samo kao izvor informacija i CIS ne snosi nikakvu izravnu ili posrednu odgovornost za bilo kakve posljedice nastale korištenjem podataka iz ovog dokumenta.

Ukoliko primijetite bilo kakve netočnosti, krive podatke ili pogreške u ovom dokumentu, ili imate potrebu komentirati sadržaj molimo Vas da to javite elektroničkom poštom na adresu info@CIS.hr.

O CIS-u

CIS izrađuje pregledne dokumente (eng. white paper) na teme iz područja informacijske sigurnosti koji će biti korisni zainteresiranoj javnosti, a u svrhu **podizanje njezine svijesti o informacijskoj sigurnosti** i **sposobnosti za čuvanje i zaštitu informacija i informacijskih sustava**. Pored toga, CIS razvija i održava mrežni portal www.CIS.hr kao referalnu točku za informacijsku sigurnost za cjelokupnu javnost; izrađuje obrazovne materijale namijenjene javnosti; organizira događaje za podizanje svijesti o informacijskoj sigurnosti u javnosti i pojedinim skupinama te djeluje u suradnji sa svim medijima.

CIS **okuplja mlade** zainteresirane za informacijsku sigurnost i radi na njihovom pravilnom odgoju i obrazovanju u području informacijske sigurnosti te pripremu za **profesionalno bavljenje informacijskom sigurnošću**.

Centar informacijske sigurnosti [CIS] nastao je 2010. godine na poticaj Laboratorija za sustave i signale[LSS] Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu, a kao posljedica 15togodišnjeg rada na istraživanju, razvoju i primjeni informacijske sigurnosti. LSS je među ostalim potaknuo osnivanje CARNetovog CERTa i sudjelovao u izradi Nacionalnog programa informacijske sigurnosti RH.

Smisao CISa je da bude **referentno mjesto za informacijsku sigurnost** za javnost, informatičare i posebno za mlade te da sustavno podiže njihovu svijest i sposobnosti u području informacijske sigurnosti.

Rad CISa podržava Ministarstvo znanosti, obrazovanja i sporta Republike Hrvatske, a omogućuju sponzori.

Prava korištenja

Sadržaj

1. Uvod

Programski alat Maltego služi za inteligentnu analizu podataka (eng. Data Mining) i prikupljanje informacija. Od ostalih alata razlikuje se po tome što može identificirati odnose među informacijama te pronalaziti do sad nepoznate odnose među njima. Dostupnost takvih informacija igra veliku ulogu u informacijskoj sigurnosti i od ključne je važnosti za ispitivanje sigurnosti te obranu pojedinog sustava od napada. Kako bi se određena meta napala potrebno je saznati gdje je ona locirana, s kojim je sustavima povezana, koje su joj najslabije točke, koje su najslabije točke sa sustavima s kojima je povezana, itd. Sve te informacije su korisne i sigurnosnim stručnjacima i zlonamjernim korisnicima te je od velike važnosti tko će te informacije saznati odnosno prikupiti prvi.[1]

Problem koji se javlja je što je dostupna velika količina takvih podataka te je ljudskom umu često vrlo teško uočiti povezanosti između naočigled nepovezanih podataka. Tvrtka Paterva, čiji je logo vidljiv na slici 1, je doskočila tom problemu stvorivši alat za grafički prikaz povezanosti među informacijama, koje njegovim korištenjem postaju očite i jednostavne za interpretirati. Povezanosti koje program Maltego može interpretirati mogu biti među:

- korisnicima (npr. društvene mreže),
- tvrtkama,
- orgranizacijama,
- web stranicama,
- internetskim infrastrukturama kao što su na primjerdomene, DNS (eng.*domain name system) zapisi*, Netblokovi, IP (eng. *internet protocol)* adrese, i dr.,
- izrazima,
- dokumentima i datotekama.

Rad alata Maltego temelji se na otvorenom obavještavanju (eng. *Open-source inteligence*)[1] odnosno sakupljanju i analizi informacija koje su javno dostupne na Internetu. Program nije otvorenog koda te postoje komercijalne i besplatne inačice koje se razlikuju u svojim mogućnostima. Neke od mogućih primjena alata Maltego su praćenje neželjenih objava i poruka elektroničke pošte na listama (eng. *mailing lists)*, verifikacija i testiranje sigurnosti IT (eng. *Information Technology*) rješenja, prikupljanje informacija s javnih izvora u svrhu provjere pozadina pojedinaca pri zapošljavanju, i dr.

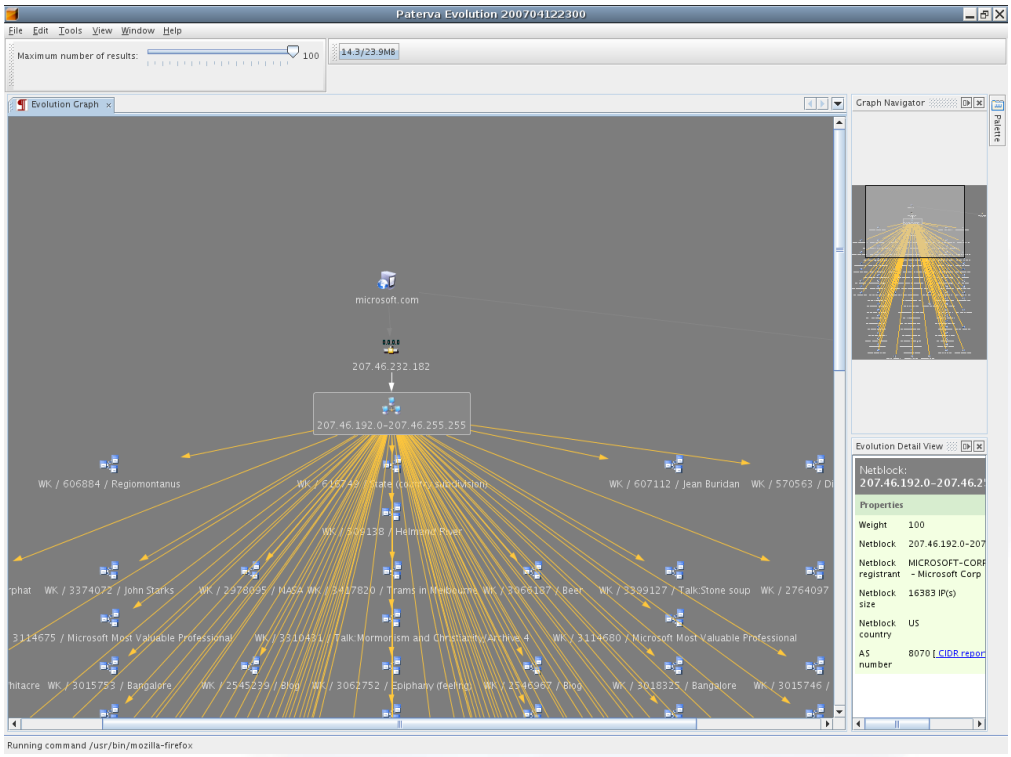
Slika 1. Logo tvrtke Paterva i alata Maltego
Izvor:paterva.com

U drugom će se poglavlju opisati povjesni razvoj alata Maltego, a u trećem način rada i sama arhitektura. Poglavlje 4 opisuje mogućnosti spomenutog programa, a poglavlje 5 njegove primjene. Na samom kraju dan je opis razvoja vlastitih dodataka za program te budućnost programa.

[1] Pojam „open-source intellgence“ koji se odnosi na otvorene informacije ne smije se zamijeniti s pojmom „open-source code“ (besplatni programi otvorenog koda), što je čest slučaj.

2. Općenito o alatu Maltego

Alat Maltego razvila je mala privatna tvrtka Paterva, osnovana 2007. godine, a locirana u gradu Irene u Južnoj Africi. Tvrtku, čiji je glavni posao razvoj alata za prikupljanje informacija, osnovao je Roelof Temmingh, također jedan od osnivača tvrtke za informacijsku sigurnost SensePost, koja se od 1995. godine bavi sličnim projektima. Predhodnik Maltega, kojeg je također razvio Temmingh, zvao se Evolution, a objavljen je krajem 2005. godine. Evolution je bio u beta inačici nekoliko mjeseci prije nego je cijeli projekt, zbog kršenja uvijeta korištenja (eng. *terms of use)* tvrtki koje se bave pretraživanjem Interneta te kršenja autorskih prava istoimenog proizvoda tvrtke Novell, ugašen. Evolution je, kao i Maltego, bio multiplatformski jer je pisan u programskom jeziku Java, a imao je slične mogućnosti i svrhu kao i Maltego - prikupljanje javno dostupnih podataka. Uz korištenje alata bila je potrebna instalacija internetskog preglednika kao što su Opera ili Mozilla. Evolution je, uz sučelje slično alatu Maltego prikazano na slici 2, nudio do 24 različite operacije obrade podataka.



Slika 2. Izgled sučelja alata Evolution
Izvor: Linux.com

U rujnu 2007. godine izdana je prva inačica programa Maltego, a ime je dobila skraćivanjem engleske rečenice „My Alter Ego“. S novim redizajniranim sučeljem nova inačica prednjačila je prethodniku, s jednostavnošću i preglednošću, a i dodane su nove mogućnosti analize podataka (eng. *Data Mining*) koje se nazivaju **transformacijama**. U prvotnom izdanju alata bile su kodirane kao dio aplikacije (Maltego 1.0), no u novijim inačicama implementirane su na udaljenom poslužitelju te je tako uveden način rada klijent-poslužitelj[2]. Poslužitelj se naziva TAS (eng. *Transform Application Poslužitelj*) koji sakuplja sve informacije proizašle iz transformacija, a na njega se mogu učitati i transformacije koje je napravio korisnik. Arhitektura prvi put objavljena u Maltegu, omogućavala je korisnicima da ograniče svoje pretrage kroz jedinstvena API (eng. *Application Programming Interface*) sučelja, koja se ne kose s uvijetima korištenja tvrtki koje se bave pretraživanjem i društvenih mreža. Nažalost pretraživanje korištenjem legalnih transformacija je ograničenije nego

[2] Klijent-psolužitelj model jedna je od značajki distribuiranih aplikacija gdje se na udaljenom poslužitelju obavlja glavnina zadataka aplikacije, dok korisnik samo pregledava rezultate zadataka.

što je bilo u Evolutionu. Nakon prvog izdanja program Maltego je doživio nekoliko preinaka, a one su sljedeće:

inačica 2.0.0

- učitavanje/spremanje cijelog grafa,
- ispis grafova,
- izvoz entiteta[3]u CSV formatu,
- optimizirana navigacija.

inačica 2.0.1

- olakšano kopiranjeizmeđu grafova i teksta,
- automatsko prepoznavanje tipa entiteta pri kopiranju iz teksta,
- pokretanje svih transformacija[4] od jednom (eng. *Run all transforms*),
- prikaz do 10 000 rezultata,
- inverzna pretraga,
- zumiranje na pokazivač miša za lakše pronalaženje čvorova na grafu,
- proizvoljno otkazivanje transformacija,
- podrška za NTLM (eng. *NT Local area network Manager*) posrednički poslužitelj (eng. proxy).

inačica 2.0.2

- mogućnost pisanja lokalnih transformacija,
- ispravljeno otkrivanje entiteta,
- poboljšano automatsko otkrivanje mreže.

inačica 3.0.4

- uvoz CSV/XLS/XLSX datoteka,
- odabir poveznica,

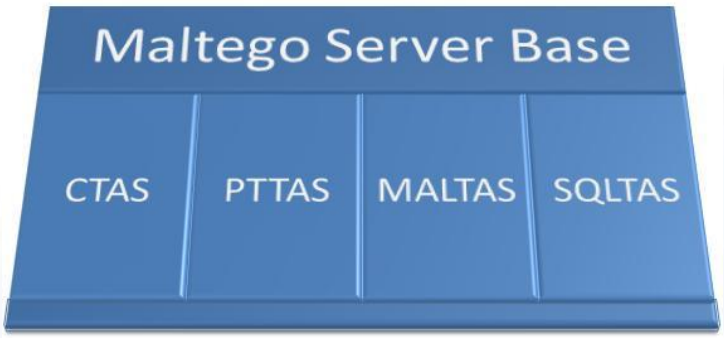
[3] Entitet je objekt grafa nad kojim se izvršava pretraga

[4] Transformacija je naziv za pretraživanje koje se izvšava nad entitetima

3. Opis rada alata

3.1. Arhitektura klijent-poslužitelj

Alat Maltego temelji se na na klijent-poslužitelj modelu programske arhitekture. Većina programa, ondosno računalno zahtjevniji dio, odvija se na namjenskom poslužitelju (eng. *dedicated server*). Poslužitelj može posluživati servisima i funkcijama više klijenata odnosno računala odjednom. Funkcije koje poslužitelji opće namjerne obično imaju su razmjena poruka elektroničke pošte, pristup bazi podataka, pristup Internetu i dr. Maltego poslužtelj ima namjenu izvođenja transformacija, a sastoji se od poslužiteljske baze koja sadrži operacijski sustav i dodatne programe za podržavanje izvođenja transformacijskih modula, što je prikazano slikom 3.

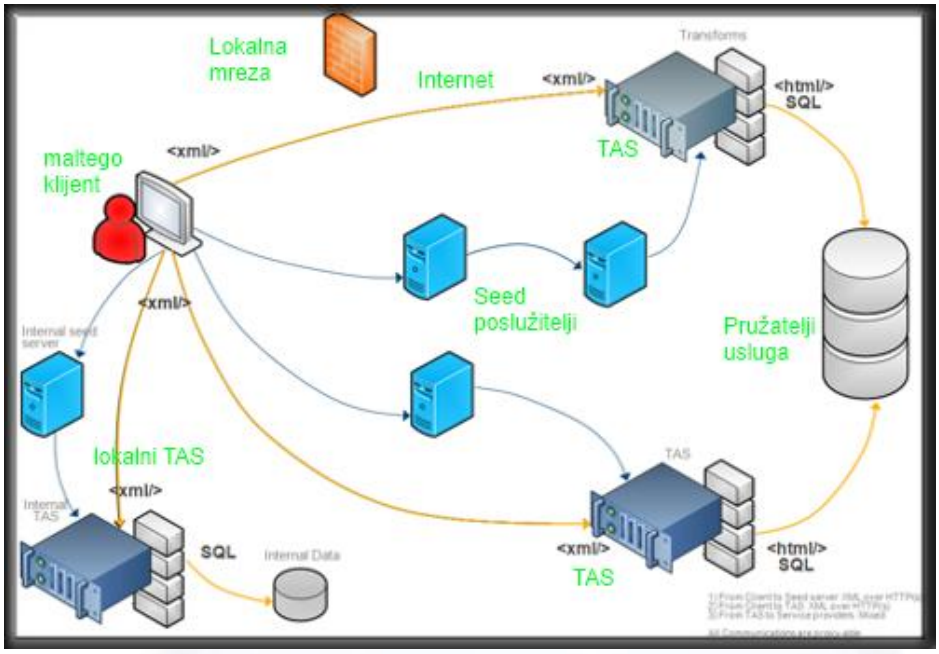


Slika 3.Arhitektura Maltego poslužitelja
Izvor: PATERVA

Poslužitelj TAS (eng. *Transform Application Server*) je naziv za poslužitelj transformacija, kojim upravlja klijent. Tvrtka Paterva poslužitelje pokreće na vlastitoj infrastrukturi lociranoj u različitim dijelovima svijeta, ali također nudi korisnicima kupovanje slike poslužitelja kao VMWare slike. Korisnik tada može pokrenuti poslužitelj na svom računalu ili vlastitoj mreži računala.

Maltego klijent šalje zahtjeve za transformacijama na *seed* poslužitelj[5] u XML (eng. *Extensible Markup Language*) formatu putem HTTPS (eng. *Hypertext Transfer Protocol Secure*) komunikacije. *Seed* poslužitelj prosljeđuje zahtjeve prema TAS poslužiteljima te ima mogućnost dijeljenja transformacija s drugim korisnicima za ubrzavanje rada. Poslužitelji TAS prosljeđuju zahtjeve pružateljima usluga kao što su tražilice (Google, Yahoo,...) društvene mreže (Faebook, Twitter,...) te baze podataka. Rezultat upita se vraća na Maltego klijent. Maltego podržava dvije vrste poslužiteljskih modula; profesionalni i osnovni. Glavna razlika među dvije vrste poslužitelja je broj modula koji su dostupni za uporabu. Profesionalni poslužitelj dolazi s CTAS, SQLTAS i PTTAS modulima dok osnovni poslužitelj dolazi s CTAS modulom, koji su opisani u nastavku. Model komunikacije u potpunosti je prikazan slikom 4.

[5] *Seed* poslužitelj je posebna vrsta poslužitelja koja služi za tzv. *peer to peer* komunikaciju koristeći protokol PNRP (eng. *Peer Name Resolution Protocol*).



Slika 4. Arhitektura komunikacije Maltego poslužitelja i klijenta
Izvor: Paterva.com

U vrijeme pisanja ovog teksta, postojalo je pet modula za transformacije:

- C-TAS (eng. *Comercial Transform Application Server)* – komercijalni TAS modul,
- PT-TAS (eng. *Penetration Testing Transform Application Server)* – TAS modul za ispitivanje sigurnosti,
- MALTAS (eng.*Malware domain List Transform Application Server)* – modul za pristup listi zlođudnih domena,
- SQ-LTAS, (eng. *SQL database Transform Application Server)* – modul za interakciju sa SQL bazama podataka,
- SO-TAS (eng. *Social Network Transform Application Server)* – modul za izvršavanje transformacija nad društvenim mrežama.

C-TAS - komercijalni TAS modul sadrži iste transformacije kao i trenutni poslužitelj koji je spojen s komercijalnom inačicom programa Maltego.

SQL-TAS - ovaj modul omogućuje interakciju s SQL (eng. Structured Query Language) bazama podataka koje TAS ne može obrađivati te omogućuje pokretanje raznih SQL upita nad tablicama i povratak rezultata u obliku entiteta. Trenutno podržane SQL baze podataka su: MySQL, MSSQL, DB2, Oracle i Postgre, dok se druge baze mogu pretraživati po dogovoru s tvrtkom Paterva uz određenu naknadu.

PT-TAS - modul koji omogućuje izvođenje raznovrsnih zadataka vezanih uz penetracijsko testiranje kao što su skeniranje priključaka (eng. *port scanning*), pronalaženje IP (eng. *Internet Protocol*) adresa, pregled DNS zapisa, ispitivanje na ranjivosti, itd.

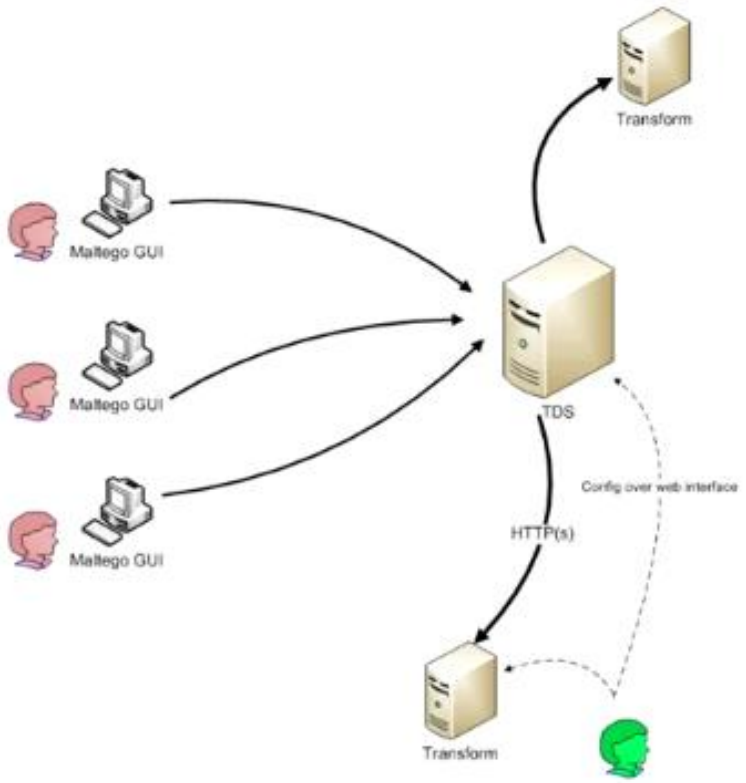
MAL-TAS - modul koji omogućuje transformacije koje izvršavaju pregled baze podataka zlonamjernih domena (MalwareDomainsList.com[6]) s pregledom povezanosti osoba, poruka elektroničke pošte i sličnih informacija sa zlonamjernim domenama.

SO-TAS - pregled različitih transformacija povezanih s društvenim mrežama. Ovaj modul u vrijeme pisanja ovog teksta nije bio dostupan zbog kršenja uvijeta korištenja za većinu društvenih mreža.

[6] Web stranica zajednice koja pronalazi zlonamjerne web stranice i prati njihov rad

3.2. TDS poslužitelj

Kao proširenje mogućnosti programskog alata Maltego dodan je poslužitelj distribucija transformacije (eng. *transform distrbution server, TDS*). Mnogo korisnika alata Maltego radi u timu te je potrebno koristiti iste (većinom lokalne) transformacije na više različitih računala. Mnoge lokalne transformacije ne rade uvijek i na svakom računalu zbog zahtjeva za različitim programskim bibliotekama. Na različitim računalima postoje različite inačice transformacija te se nemogu udaljeno nadograditi. Neke transformacije sadržavaju privatne podatke poput korisničkog imena i lozinke pa ih je potrebno zaštititi. Iz tog razloga je razvijen poslužitelj TDS, sa pripadajućim web sučeljem koji omogućuje distribuciju transformacija među korisnicima, kao i njihovu nadogradnju te upravljanje njihovim postavkama. TDS također omogućuje postavljanje dozvola kome će koje transformacije biti vidljive i na kojem će se „seed“ poslužitelju pokretati. Model komunikacije korisnika i poslužitelja TDS dan je slikom 5.



Slika 5. Arhitektura TDS
Izvor: Paterva.com

Korisnici mogu pronaći transformacije na TDS poslužitelju te ih izvršiti nad entitetima, preko već opisane komunikacijske arhitekture alata Malego, bez puno podešavanja i problema s instalacijom i inicijalizacijom.

3.3. Način korištenja alata[3]

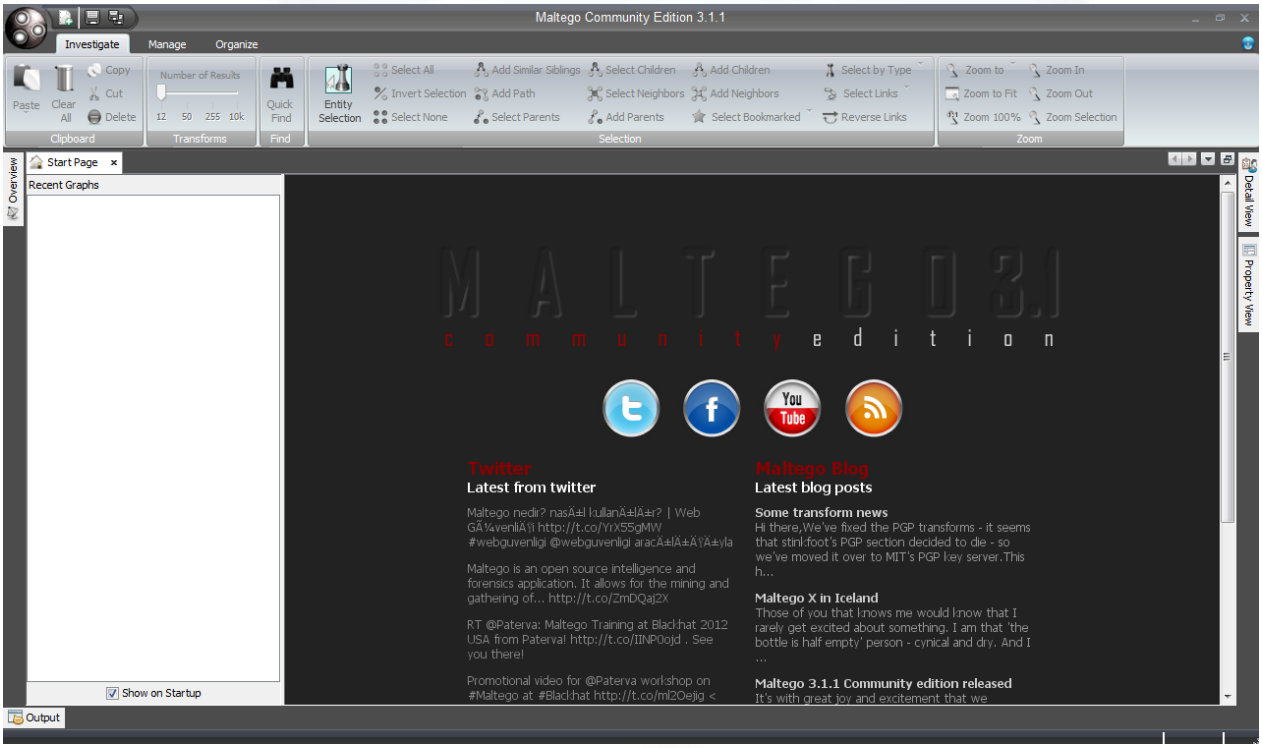
Iz razloga što je cijeli izvorni kod alata Maltego pisan u programskom jeziku Java, alat radi na svim poznatim operacijskim sustavima koji podržavaju JDK (eng. *Java Development Kit)* 1.5 i više inačice. Instalacija alata moguća je preuzimanjem paketa za instalaciju programa sa sljedeće poveznice:

http://www.paterva.com/web5/client/download.php

ili preuzimanjem operacijskog sustava Backtrack[7] na kojem dolazi predinstalirana.

Na stranici je moguće preuzeti različite arhive ovisno o preferenciji operacijskog sustava te odabiru komercijalne ili inačice za zajednicu (eng. *Community edition).* Komercijalna inačica sadrži više mogućnosti i ima povlašteni pristup poslužitelju i brojne druge prednosti koje će biti opisane u nekom od narednih poglavlja. U vrijeme pisanja ovog teksta najnovija inačica bila je 3.1.1.

Nakon preuzimanja datoteke i korištenja čarobnjaka za instalaciju paketa (za operacijske sustave Microsoft Windows) Maltego će zatražiti registraciju za pokretanje, pošto mu je za rad potrebna veza s poslužiteljom. Ovisno o tipu licence, biti će potrebna aktivacija da bi se Maltego mogao koristiti. Kada je paket aktiviran i pokrenut pojavljuje se početna stranica koja je prikazana slikom 6.



Slika 6. Sučelje programa Maltego 3.1.1
Izvor:CIS

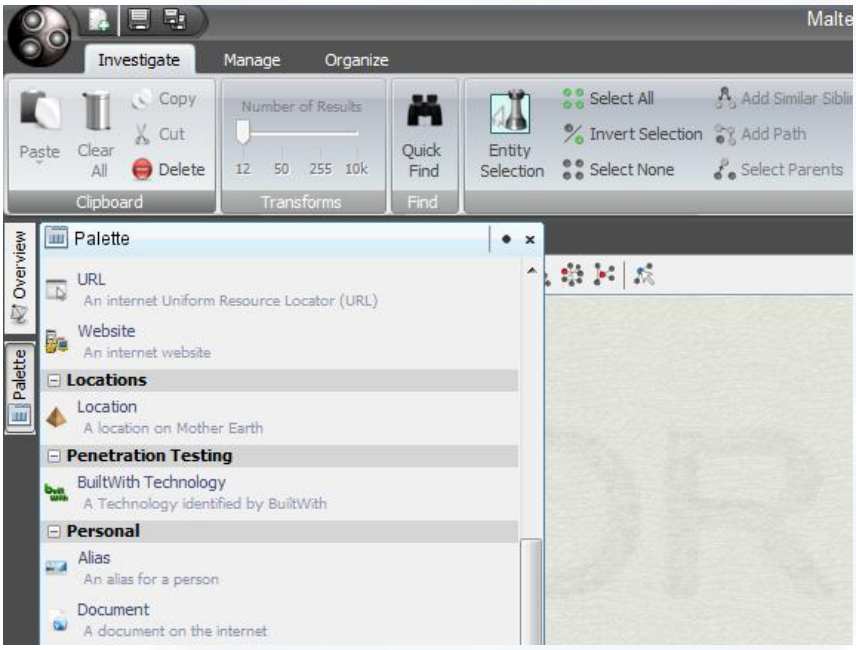
Kako bi počeli s korištenjem alata potrebno je napraviti novi graf i zatim se spojiti na poslužitelj i potražiti koje su sve transformacije dostupne. To se izvodi odabirom kartice Manage i klikanjem na „Discover transformations“ kao što je to prikazano na slici 7.

[7] Operacijski sustav Backtrack sadrži brojne alate za probijanje i ispitivanje sigurnosti sustava i mreža, a može se preuzeti na poveznici http://www.backtrack-linux.org/

Slika 7. Otkrivanje dostupnih transformacija
Izvor: CIS

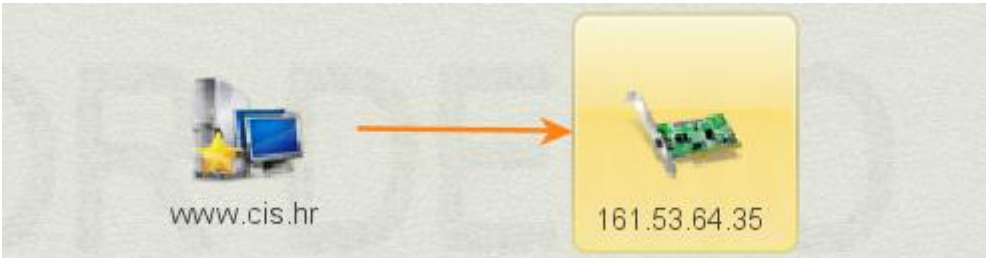
Nakon učitavanja svih transformacija potrebno ih je postaviti prema potrebi korištenja te prihvatiti uvijete korištenja ukoliko je pojedina transformacija sadrži. Transformacije se postavljaju klikom na „Manage Transforms“ (izbornik prikazana na slici 7 krajnje desno).

Alat Maltego je sada potpuno postavljen i spreman za pokretanje transformacija. Nova pretraga podataka započinje se odabirom Maltego loga (crna kružnica s tri manje kružnice), prikazane na slici 7 te odabirom na „New“. Otvorit će se novi graf te će se s lijeve strane prikazati paleta, prikazana na slici 8, koja sadrži entitete koje pretražujemo. Entiteti su informacije koje pretražujemo, a mogu biti osobe, adrese elektroničke pošte, uređaji, lokacije, brojevi telefona i sl.



Slika 8. Paleta entiteta programa Maltego
Izvor:CIS

Sustav pretraživanja je jednostavan, tzv. klikni-i-povuci (eng. *Drag-and-drop*) metodom postavlja se ikona entiteta na površinu grafa. Kad je entitet postavljen može se namiještati lijevim klikom, desnim klikom, preimenovanjem i sl. Kada smo entitet postavili desnim klikom namiještamo koje transformacije nad objektom želimo napraviti. Pretpostavimo da je postavljen entitet Web sjedišta te smo kliknuli transformaciju „to IP adress“, rezultat transformacije je prikazan slikom 9.



Slika 9. Rezutlat transformacije „To IP address“
Izvor:CIS

Rezultat ove transformacije daje nam IP adresu web sjedišta. Ovo je osnovni primjer kako se koristi alat Maltego, za širu sliku o primjenama savjetuje se pregled poglavlja 5.

4. Mogućnosti

4.1. Transformacije

Transformacije su operacije koje se izvršavaju nad informacijama koje pretražujemo odnosno entitetima (adrese elektroničke pošte, poslužitelji, web stranice, osobe, itd) preslikavajući ih u nove entitete koji su korisniji za dobivanje nekih ključnih informacija (IP adrese, DNS zapisi, lokacije, brojevi telefona i sl.). Primjerice moguće je postaviti entitet web stranice te izvršiti transformaciju „toWebsite [Replace with Thumbnail]“ koja će nam ikonu entiteta web stranice zamijeniti slikom sadržaja web stranice. Transformacija je prikazana slikom 10.

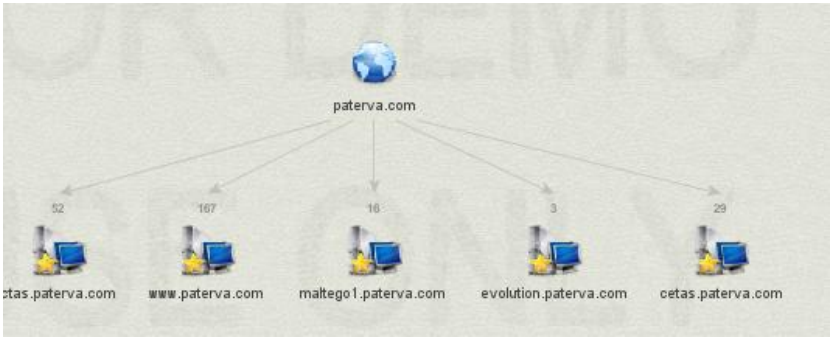
Slika 10.transformacija toWebsite [Replace with Thumbnail]
Izvor: CIS

Svaki entitet koji se nalazi u alatu Maltego posjeduje vlasititi set transformacija koji se izvršavaju na poslužitelju. Slijedi popis entiteta i bitnijih transformacija i njihov opis:

- Internet Autonomous System (AS)
  - **ASNumberToNetblocks_Robtex** - transformacija pokazuje koje su rute locirane unutar AS broja pregledavanja poslužitelja RobTex.
- Domain Name System ime poslužitelja
  - **DNSNameToDomain_DNS -** izvlačenje svih imena domena iz DNS imena isključuje TLDs i SLD,
  - **DNSNameTOIPAddress_DNS -** pretvara DNS ime na IP adresu pomoću DNS protokola,
  - **DNSNameTOWebsite_QueryPorts** - transformacija određuje je li DNS ime web sjedišta te ukoliko se radi o web sjedištu provjerava ima li aktivne HTTP(S) priključke.
- Internet Domene
  - **DomainToMXrecord_DNS** - pronalazi MX (eng. *mail exchange*) zapise za domenu,
  - **DomainToNSrecord_DNS** - pronalazi NS (eng. *name server*) zapise za domenu,
  - **DomainToDNSName_DNSBrute** - pokušava otkriti različita zajednička DNS imena unutar domene
  - **DomainToEmailAddress PGP** - transformacija kontaktira javni PGP (eng. *Pretty Good Privacy*) poslužitelj i vraća adresu elektroničke pošte koja sadrži danu domenu,
  - **DomainToEntities Whois NER** - transformacija koja dohvaća infromacije tko je prisutan na domeni te potom obrađuje entitete koristeći NER (eng. *Named Entity Recognition*).
  - **Search Engine** - transformacija pretražuje lokaciju za zanimljivim dokumentima kao što su dokumenti Microsoft Word i Excel na web stranicama unutar domene.
  - **DomainToPerson PGP** - kontaktira javni PGP poslužitelj i vraća entitet osobe koja je locirana na danoj domeni.

- **DomainToPhone Whois** - pretražuje domenu i nalazi telefonske brojeve korisnika na domeni.
- **DomainToWebsite DNS** - provjerava postoji li web stranica na domeni.

Transformacija je prikazana slikom 11.



Slika 11. transformacija DomainToWebsite
Izvor: CIS

- IPv4 (eng. *Internet Protocol version 4)* adrese
  - **IPAddressToDNSName** [SharedIP, SharedMX, SharedNS] - skupina transformacija koja provjerava nasuprotnu provjeru nad IP adresama tako da pregledava ServerSniff, Robtex, DNS, MX i NS zapise.
  - **IPAddressToEmailAddress Whois, NER, API** - transformacija nalazi informacije o IP adresi, zatim pretražuje adresu elektroničke pošte.
  - **IPAddressToNetblock NS4block** - transformacija kontaktira Robtex usluge i određuje ima li ikakvih DNS blokova koji su mu priključeni preko određene IP adrese.
  - **IPAddressToPhone Whois** - dohvaća telefonski broj povezan s IP adresom.
  - **Search Engine** - pretražuje Internet i prikazuje gdje se sve nalazi tražena IP adresa.

- Fizička lokacija
  - Za sad nije implementirana transformacija za entitet lokacije no neke transformacije mogu dati lokaciju kao rezultat.

- DNS zapis imena poslužitelja
  - **NSrecordToDomain DNS** - dohvaća sve domene s DNS liste,
  - **NSrecordToDomain SharedNS** - dohvaća NS zapise pregledavajući ServerSniff i RobTex usluge. Kao nusproizvod dobivaju se netblokovi[8] za koje je NS primarni poslužitelj,
  - **NSrecordToIPAddress_DNS -** NS zapis pretvara u IP adresu koristeći DNS protokol,

[8] Netblok je naziv za skupinu računala u istoj podmreži

- Netblock[9]
    - **NetblockToAS SS** - određuje broj AS pregledavanjem usluge ServerSniff,
    - **NetblockToDNSName SS** - pretražuje DNS imena koja postoje unutar Netblocka,
    - **NetblockToEntities NER Whois** - pretražuje imena unutar netbloka te ih prebacuje u entitete koristeći NER uslugu,
    - **NetblockToLocation SS** - određuje zemlju u kojoj je određeni blok,

- URL (eng. *Uniform Resource Locator)*
    - **URLToEmail Parse** - prebacuje adrese elektroničke pošte na danom URL-u,
    - **URLToPerson NLP** - pomoću procesiranja prirodnog jezika (eng. *Natural Language* Procesing) izvlači entitete,
    - **URLToURL IncomingLinks** - pretražuje nadolazeće poveznice,

- 5.1.10 Website
    - **WebsiteToEmailAddress Mirror** - transformacija koristi „Gary's Ruby website mirror“ skriptu za izvlačenje adresa elektroničke pošte.

- 5.2.2 Email
    - **EmailAddressToDomain DNS** - uklanja dio ispred znaka „@“ za danu adresu,
    - **EmailAddressToEmailAddress SignedPGP** - kontaktira javni PGP poslužitelj i vraća adrese elektroničke pošte potpisnika za danu adresu,
    - **EmailAddressToPerson Same PGP** - pretražuje javni PGP poslužitelj i vraća ime osobe za danu adresu,
    - **Search Engine** - pretražuje gdje se na Internetu pojavljuje tražena adresa elektroničke pošte,
    - **EmailAddressToEmailAddress** - provjerava postojanje adrese elektroničke pošte.

- 5.2.3 Person
    - **PersonToEmailAddress SamePGP** - vraća adresu elektroničke pošte povezanu s osobom ukoliko postoji.

- Phone Number
    - **Search Engine** – pretražuje telefonski broj i vraća adresu elektroničke pošte povezanu s tim brojem.

- Twitter
    - **TwitToPerson Parse** - pretvara Twitt u entitet povezan s Twitterom,
    - **TwitToURL Expand** - pokušava doznati URL-ove iz Twittova.

- Povezanost s korisničkim računom socijalne mreže Facebook - za sad ne postoje transformacije ovog tipa, no neke će transformacije dati ovaj entitet kao rezultat.

[9]Blok od više računala odnosno objekata u jednoj mreži, pojam je specifičan za alat Maltego

- Povezanost s korisničkim računom mreže Twitter

  - **AffTwitterToAffTwitter GetDetail** - pronalazi detalje o Twitter entitetu.
  - **AffTwitterToAffTwitter RecFrom** - pronalazi sve korisnike koji su napisali Twittove traženoj osobi,
  - **AffTwitterToAffTwitter WritesTo** - pronalazi korisnike kojima je tražena osoba napisala Twitt,
  - **AffTwitterToPerson** - transformacija koja konvertira povezanost s korisničkim računom mreže Twitter u entitet osobe,
  - **AffTwitterToTwit OtherAuthors** - nalazi sve Twittove ostalim osobama od odabranog autora,
  - **AffTwitterToAffTwitter Followers** - pronalazi sve sljedbenike ciljanog Twitter računa,
  - **AffTwitterToAffTwitter Friends** - pronalazi sve Twitter prijatelje.

4.2. Lokalne transformacije

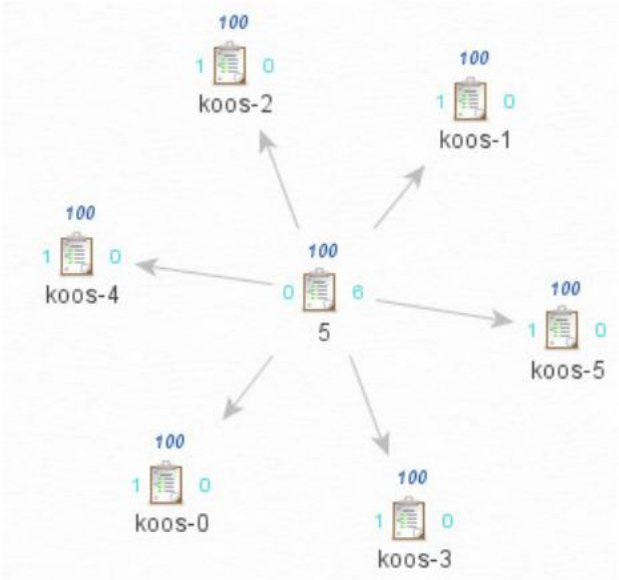
Lokalne transformacije su upiti koji se izvšavaju lokalno, na istom računalu na kojem se izvršava i Maltego, a prisutne su tek od inačice 2.0.2. Transformacije, jednom kad se pozovu, produciraju izlaz koji se prikazuje u obliku entiteta na grafu. Mogu se kodirati u praktički bilo kojem jeziku sve dok se drže specifikacija koje izdaje tvrtka Paterva. Lokalne transformacije omogućuju integraciju s proizvoljnim informacijama koje osobno računalo može dohvatiti preko Interneta bez potrebe za spajanjem na poslužitelje tvrtke Paterva. Lokalne transformacije uglavnom razvijaju korisnici, a podržane su u više programskih jezika iako se preferiraju Perl i Python.

4.2.1. Razvoj vlastitih transformacija

Vlastite transformacije razvijaju se većinom u skriptnim jezicima Perl i Python. Slijedi primjer takve transformacije koja vraća listu entiteta za zadanu vrijednost:

```
#!/usr/bin/perl
my $entityValue = $ARGV[0];
 #XML header
my $header=<<EOT;
<MaltegoMessage><MaltegoTransformResponseMessage> <Entities>
EOT ;
 #XML footer
my $footer=<<EOT;
</Entities> </MaltegoTransformResponseMessage> </MaltegoMessage>
EOT;
 print $header;
for (0..$entityValue){
      print "<Entity Type='Phrase'><Value>koos-
$_</Value></Entity>\n";
}
print $footer;
```

Prvi redak skripte je direktorij u kojem se nalazi perl skripta, zatim deklaracija varijable $entityValue koja se zadaje putem komandne linije. Nakon deklaracije varijable slijedi deklaracija XML zaglavlja koje je potrebno da bi transformacija bila kompatibilna s alatom Maltego. U 11. retku nalazi se ključan dio programskog koda. Takozvana for petlja koja ispisuje sve entitete sa zadanim izrazom. Nakon provođenja skripte dobivamo rješenje prikazano na slici 12.



Slika 12. Rezultat prevođenja lokalne transformacije
Izvor: Paterva.com

Rješenje prikazuje sve entitete sa upitom broja 100 i njihovom povezanosti.

Transformacije primaju ulaz preko parametara komandne linije. Prvi (obvezni) parametar sadržava vrijednost entiteta, dok je drugi opcionalan i sadržava vrijednost polja. Kako bi se rezultat transformacije mogao prikazati potrebno je programski izlaz namjestiti tako da se rezultati zapisuju unutar XML (eng. *extensible markup language*) oznaka na primjer:

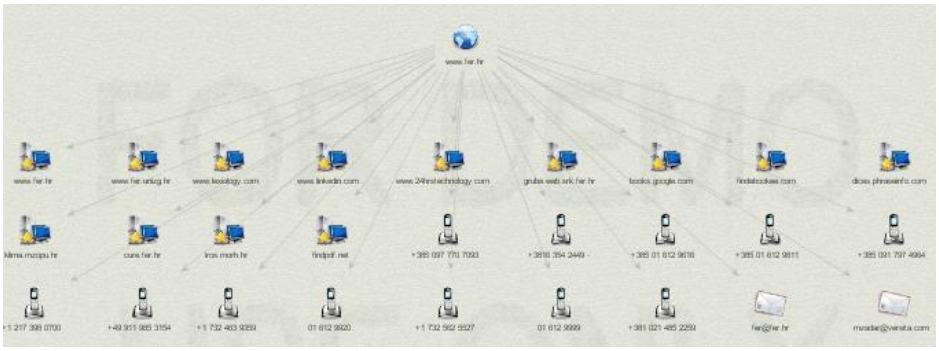
```
<MaltegoMessage>
<MaltegoTransformResponseMessage></MaltegoTransformResponseMessage>
</MaltegoMessage>
```

Pri izradi vlastitih transformacija moraju se poštovati još brojna pravila, primjerice o imenovanju atributa, dojavljivanju pogrešaka i drugi. Za više detalja korisnike se upućuje na dokument [2].

4.3. Prikaz rezultata transformacija[5]

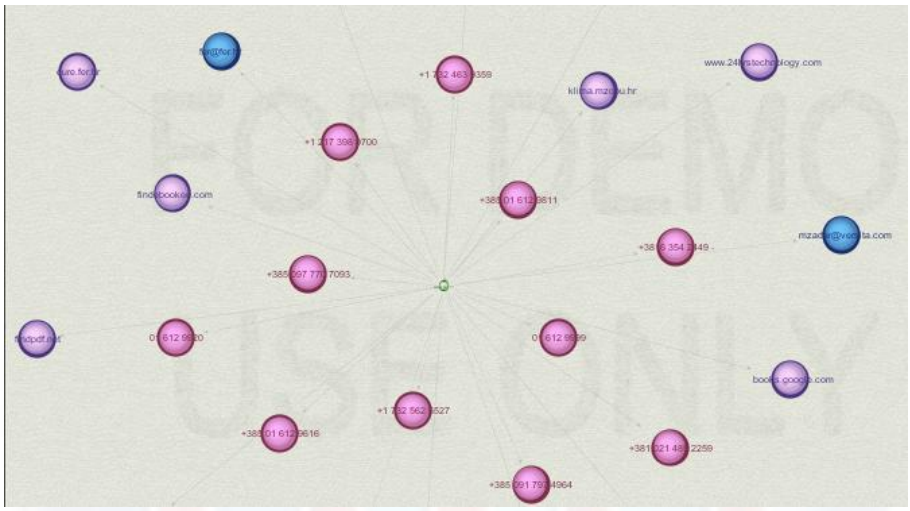
Samo provođenje transformacija odnosno „*data mining*“ operacija nad podacima nije toliko ključna stavka za alat Maltego kao prikaz rezultata (višestrukih) transformacija kako bi se iz njih mogli izvući zaključci o povezanosti podataka. Opcije za pregled transformacija odabiremo iz kartice pogledi (eng. *views*):

- „Main view“ – osnovni način pregleda podataka, gdje se rezultati sortiraju kao stablo razgranato prema dolje (slika 13),



Slika 13. Main view
Izvor: CIS

- „Bubble view“ – omogućuje korisnicima sortiranje informacija na grafu prema važnosti dolaznih i odlaznih veza oko entiteta nad kojim se vrši transformacija (slika 14),



Slika 14. Bubble view
Izvor: CIS

- „Entity list“ - detaljan opis svih identiteta i njihovih poveznica (slika 15)

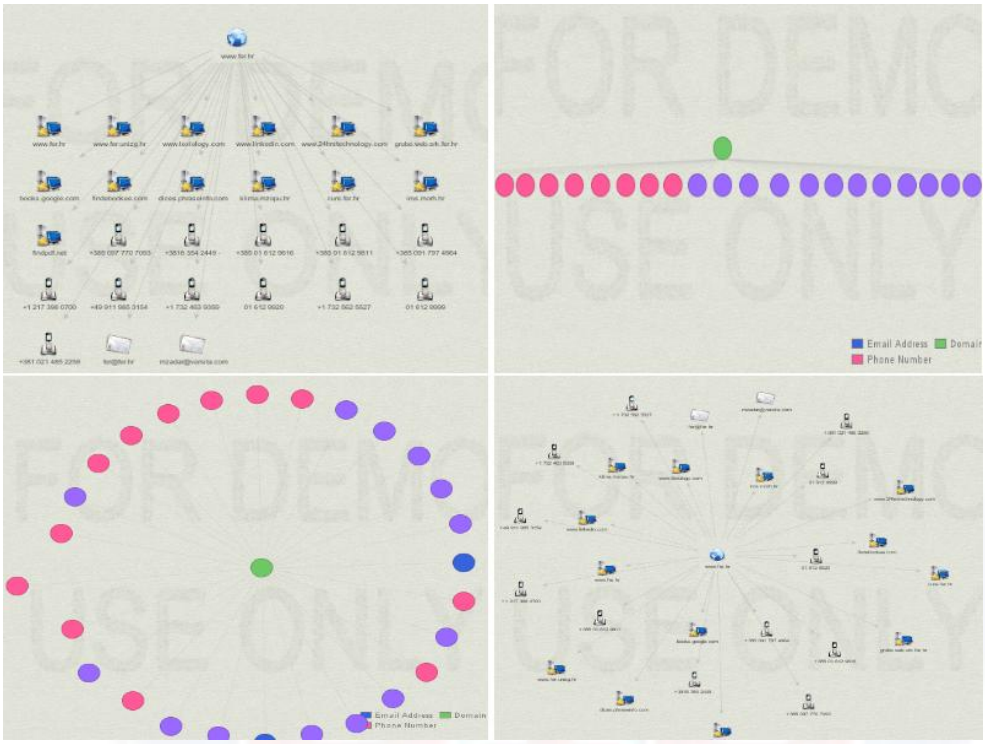
www.fer.hr	Domain	www.fer.hr	0	0	27
www.fer.hr	Website	www.fer.hr	161025	1	0
fer@fer.hr	Email Address	fer@fer.hr	35	1	0
mzadar@versit	Email Address	mzadar@versit...	16	1	0
www.fer.unizg	Website	www.fer.unizg...	40	1	0
www.linkedin.c	Website	www.linkedin.c...	32	1	0
www.lexiology.	Website	www.lexiology...	35	1	0
grube.web.srk.	Website	grube.web.srk...	30	1	0
www.24hrstech	Website	www.24hrstec...	31	1	0
findpdf.net	Website	findpdf.net	22	1	0
klima.mzopu.hr	Website	klima.mzopu.hr	25	1	0
iros.morh.hr	Website	iros.morh.hr	23	1	0
dices.phraseinf	Website	dices.phrasein...	26	1	0
cure.fer.hr	Website	cure.fer.hr	25	1	0
books.google.c	Website	books.google....	29	1	0
findebookee.co	Website	findebookee.com	28	1	0
+3816 354 244	Phone Number	+3816 354 24...	7	1	0

Slika 15. Entity list
Izvor: CIS

„Main view“ ima nekoliko dodatnih opcija prikazanih na slici 16:

- blokovski raspored - osnovni raspored za glavni pregled. Entiteti su grupirani po tipu i stablasto.

- hijerarhijski raspored - stablasta struktura. Svaki entitet je grupiran u roditeljsko-dječjem odnosu,
- centralni raspored - entiteti koji su najbliži centru grafa imaju najviše dolaznih veza dok su drugi raspoređeni u krug. Dobar raspored za uočavanje anomalija,
- organski raspored - čvorovi su raspoređeni tako da se minimalizira udaljenost među njima.



Slika 36. Opcije Main pregleda 1 redom s lijeva na desno:,block, hierachical, circular, organic
Izvor: CIS

4.4. Ograničenja besplatne inačice

Besplatna inačica (eng. *community* edition) ima sljedeća ograničenja na klijentu:

- zabranjena komercijalna upotreba,
- maksimalno 12 rezultata po transformaciji,
- potreba za registracijom na stranici tvrtke Paterva,
- API (eng. *application programming interface*) ključevi istječu svakih nekoliko dana,
- izvršavanje transformacija na sporijem poslužitelju,
- komunikacija između poslužitelja i klijenta nije šifrirana,
- ne nadograđuje se sve do izdavanja nove inačice
- nema podrške krajnjem korisniku,
- nema nadogradnji transformaicija na poslužitelju,
- moguće je otkrivanje transformacija isključivo s poslužitelja tvrtke Paterva,
- ograničenje transformacija na 75 dnevno,
- moguće je izvođenje samo jednog entiteta u isto vrijeme.

5. Primjena

5.1. Penetracijsko testiranje [6]

Penetracijsko testiranje ili skraćeno pentesting je postupak identifikacije ranjivosti u sustavu ili mreži, a služi za potvrdu funkcionalnosti sigurnosnih kontrola, pravovremeno uočavanje i uklanjanje sigurnosnih propusta te prevenciju mogućih sigurnosnih incidenata. Pentesting uključuje korištenje metoda napada koje provode provjereni profesionalci na sličan način kako to čine i zlonamjerni korisnici. Ovisno o tipu testa koji se provodi, postupak može uključivati sve od jednostavnog skeniranja IP adresa za identifikaciju uređaja pa do dugotrajnog prikupljanja podataka, nadgledanja i provale u ciljani sustav.

Pentesting se sastoji od nekoliko koraka. Prvi je planiranje i priprema u kojem se odlučuje o opsegu i dubini pretrage, koordinirati se s naručiteljem u koje vrijeme se izvodi i koliko traje. Drugi korak je izvođenje koje se sastoji od prikupljanja i analize informacija, skeniranja pokušaja proboja, zadržavanje pristupa te čištćenja tragova nakon proboja. Završni korak se sastoji od izvještavanja o ranjivostima naručitelju, određivanja rizika i posljedica napada te predlaganja mjera zaštite i uklanjanja pronađenih ranjivosti.

Maltego je idealni alat za obavljanje dijela posla koji se odnosi na skupljanje i inteligentnu analizu podataka. S nekoliko osnovnih transformacija navedenih u poglavlju 3.2 može se obaviti dio posla penetracijskog testiranja, dobiti rezultate u obliku grafa i stvoriti osnovnu sliku o sustavu kojeg napadamo (testiramo). No, alat Maltego je nakon dogovorene suradnje s tvrtkom Offensive Security razvio zaseban modul poslužitelja za transformacije PTTAS (eng. *PenTesting Transform Application Server).*

Poslužitelj PTTAS sadrži sljedeće korisne transformacije:

_**To Website Title** - koristi se ukoliko je web poslužitelja iznimno puno, a potrebno je saznati koje se sve stranice na njima pokreću. Ulaz je WebsiteEntity, a izlaz WebtitleEntity,

- _**To Website – SSL info** - kao i prethodna transformacija, ali se koristi zajedno sa skenerom priključaka. Ulaz je IPAddressEntity, a izlaz WebsiteEntity.
- _**To Webdir** - daje popis svih direktorija pronađenih na web stranici tako da pregledava podatke dostupne na Internetu. Izlaz je WebdirEntity.
- _**To Vuln -** Koristeći Nessuzs 3.2 dozvoljava se pokretanje liste NASL (eng. *Nessus Attack Scripting Langugage*) na ciljanom sustavu. Nakon popunjenja NASL ID (eng. Identification) liste dobivamo popis ranjivosti sustava u obliku VulnEntity entiteta.
- _**Do Portscan -** izvršava skeniranje priključaka konfiguriranih u transformaicji. Transformacija korsiti Nmap za skeniranje, a može se iskoristiti na Netblock ili IPadress entitetu.
- _**To Service** - nakon skeniranja priključaka mogu se naći servisi koji su pokrenuti na poslužitelju.

Na sajmu BlackHat u Amsterdamu 2009 predstavljen je set transformacija koje oponašaju alat Nmap, poznati alat koji se koristi pri pentestingu. Ovo je set (lokalnih) transformacija koje se koriste:

- **nmapPorts.py** - transformacija izvršava osnovno skeniranje sljedećih priključaka: 22, 2, 215, 80, 443, 3306. Skeniranje će se izvršiti na IP adresi i vratit će istu IP adresu s dodatnim poljem „otvoreni priključci“,

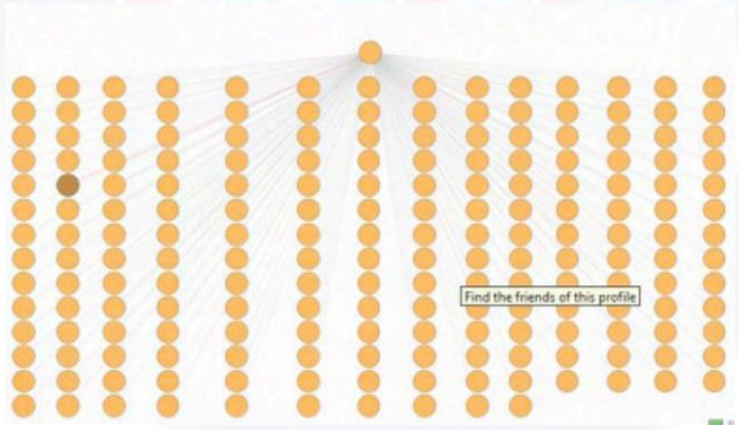
- **nmapPorts-ask.py** - radi isto kao i prethodna transfomacija, ali skenira proizvoljne priključke.
- **nmapPortsNetblock.py** - također radi kao i prethodna transformacija, ali vraća IP adresu iz netbloka s otvorenim priključcima.

5.2. Socijalni inženjering[7]

Socijalni inženjering se definira kao proces u kojem, prjevarom, korisnici otkivaju svoje povjerljive podatke ili daju pristup resursima kojima svojevoljno ne bi htjeli dati pristup. Socijalni inženjering i oni koji ga koriste mogu se podijeliti u više kategorija. Kategorije sežu od profesionalnih špijuna i hakera sve do prodavača i svakodnevnih ljudi. Sakupljanje informacija kao jedan od ključnih činova u socijalnom inženjerstvu domena je alata Maltego. Alat Maltego izvodi puno automatiziranih radnji socijalnog inženjeringa poput korelacije podataka i njihovog prikupljanja. Prikupljanje podataka najlakše je izvesti ako je tražena osobameta član neke od društvenih mreža [5]. Potrebni koraci za izvođenje prikupljanja podataka su sljedeći:

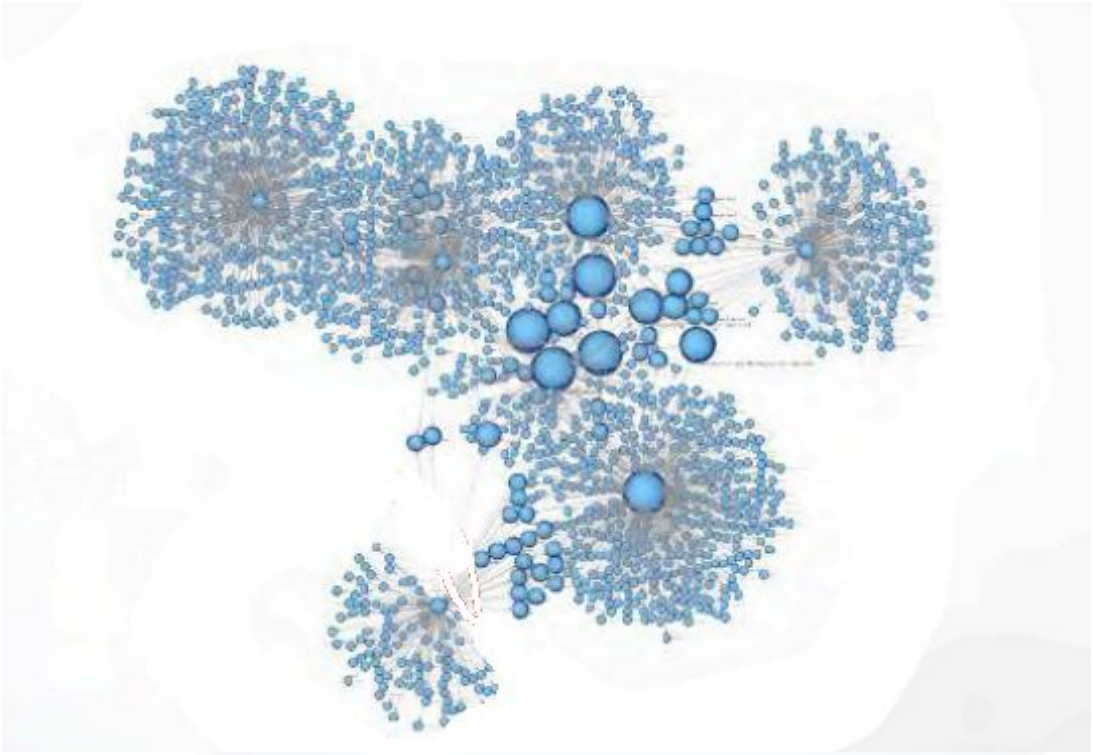
- kreiranje vjerodostojnog korisničkog računa,
- izrgradnja identiteta na korisničkom računu,
- indirektno približavanje meti (učlanjenje na iste društvene grupe, povezivanje s prijateljima mete,..)
- prikupljanje podataka.

Nakon što je društvena mreža dobro pripremljena, sve što je potrebno je prikupiti podatke pomoću nekih od transformacija unutar alata Maltego. Primjerice transformacija za Twitter koje mogu prikupljati zapise korisnika, njegove vijesti i slike. Na slici 17 prikazana je mreža prijatelja na socijalnoj mreži Facebook prema meti (tamno smeđa) i lažnom korisničkom računu (vrh grafa).



Slika 4. Mreža Facebook prijatelja pri socijalnom inženjeringu
Izvor: Defcon18

„Bubble“ pogled, nakon nekoliko transformacija („EmailAddressToDomain DNS“, „DNSNameTOIPAddress_DNS“ i još nekoliko koje su za sad nelegalne zbog kršenja ugovora o korištenju) daje rezultat na slici 18, koji prikazuje povezanost s metom, broj interakcija, mjesta na Internetu koje meta posjećuje, odnosno njezine navike i sl.



Slika 5. Povezanost mete, ljudi i mjesta na Internetu;
što je veći krug to je veća povezanost
Izvor:Defcon 18

Sakupljanje informacija u ovakvom vidu, iznimno je dobro plaćeno [5]. Neke od korisnih transformacija razvila je tvrtka Packetninjas pod nazivom **SocialNet**[10]**.**

[10] http://www.packetninjas.net/socialnet/- stranica tvrtke koja sadrži više informacija o transformacijama

6. Zaključak

Maltego je najbolji dostupni komercijalni alat za prikupljanje i analizu podataka. Prednosti su mu jednostavnost korištenja, primjenjivost i proširivost. Maltego je platforma koja može dati vrlo dobru sliku o okolini objekta istraživanja kao i povezanosti s drugim entitetima. Jedinstvena perspektiva koju Maltego pruža nad mrežama i mrežnim resursima pojednostavljuje posao stvaranja poveznica među naočigled nespojivim podacima. Prava moć alata Maltego dolazi pri razvoju vlastitih transformacija te njihovog pokretanja na TDS poslužitelju. Alat nažalost nije otvorenog koda odnosno besplatan, kako bi možda naziv open-source intellgence mogao krivo navesti korisnike. Za potpuno iskorištavanje snage alata Maltego bilo potrebno kupiti komercijalnu inačicu, koja osim velike brzine i efikasnosti donosi i podršku zajednice Maltego te promptnije nadogradnje od strane tvrtke Paterva.

7. Leksikon pojmova

Race condition - Race condition - Race condition (hrv. Istovremeni pristup) je sigurnosni problem do kojeg dolazi kada dva procesa istovremeno i nesinkronizirano pristupaju određenom resursu sustava (memorijskom prostoru, datoteci, itd.)

http://www.tech-faq.com/race-condition.html

Priključnica (Krajnje točke u komunikaciji transportnih protokola)

- Brojčane vrijednosti temeljem kojih računalo po prihvatu podataka zna koju uslužnu programsku potporu (servise) mora aktivirati te na koji način razmjenjivati podatke na transportnom sloju. http://searchnetworking.techtarget.com/definition/port-number

IP

- Internet Protocol - IP je jedan od glavnih protokola u Internetu, a koristi se za usmjeravanja paketa kroz Internet. U tu namjenu, dodjeljuje IP adrese izvora paketa i njegovog odredišta na temelju kojih će se paketi usmjeravati kroz nekoliko računalnih mreža. http://compnetworking.about.com/od/networkprotocolsip/g/ip_protocol.htm

URL

- URL (eng. Uniform Resource Locator) predstavlja adresu određenog resursa na Internetu. Resurs na koji pokazuje URL adresa može biti HTML dokument, slika, datoteka ili bilo koja datoteka koja se nalazi na određenom web poslužitelju.

http://searchnetworking.techtarget.com/definition/URL

HTTP

- HTTP (eng. HyperText Transfer Protocol) - Osnovna i najčešća metoda prijenosa informacija na Webu. Predstavlja protokol na aplikacijskom sloju OSI modela, a osnovna namjena je prijenos HTML dokumenata (tj. web stranica). HTTP je request/response protokol za komunikaciju između poslužitelja i klijenta. HTTP klijent, kao što je web preglednik najčešće inicira prijenos podataka nakon što uspostavi TCP vezu s udaljenim web poslužiteljem na određenom priključku. Poslužitelj konstantno osluškuje zahtjeve na određenom mrežnom komunikacijskom priključku (tipično priljučak 80), čekajući da klijent inicira komunikaciju. - Osnovna i najčešća metoda prijenosa informacija na Webu. Predstavlja protokol na aplikacijskom sloju OSI modela, a osnovna namjena je prijenos HTML dokumenata (tj. web stranica). HTTP je request/response protokol za komunikaciju između poslužitelja i klijenta. HTTP klijent, kao što je web preglednik najčešće inicira prijenos podataka nakon što uspostavi TCP vezu s udaljenim web poslužiteljem na određenom priključku. Poslužitelj konstantno osluškuje zahtjeve na određenom mrežnom komunikacijskom priključku (tipično priključak 80), čekajući da klijent inicira komunikaciju.

http://hr.wikipedia.org/wiki/HTTP

PHP (PHP: Hypertext Preprocessor)

- PHP (eng. PHP: Hypertext Preprocessor) **-** Objektno-orijentiran programski jezik namijenjen prvenstveno za izradu dinamičnih web sjedišta. PHP je besplatan proizvod, objavljen pod PHP License licencom. Sintaksom je vrlo sličan popularnim jezicima poput C/C++, Java i Perl, a u potpunosti je implementiran u programskom jeziku C. Zbog jednostavnosti uporabe i visoke popularnosti postao je jednim od najpopularnijih jezika za izradu web sjedišta i usluga. Za razliku od jezika C/C++ i Jave koji su strogo tipizirani, PHP nema tipove podataka. - Objektno-orijentiran programski jezik namijenjen prvenstveno za izradu dinamičnih web sjedišta. PHP je besplatan proizvod, objavljen pod licencom PHP License. Sintaksom je vrlo sličan popularnim jezicima poput C/C++, Java i Perl, a u potpunosti je implementiran u programskom jeziku C. Zbog jednostavnosti uporabe i visoke popularnosti postao je jednim od najpopularnijih jezika za izradu web sjedišta i usluga. Za razliku od jezika C/C++ i Jave koji su strogo tipizirani, PHP nema tipove podataka. Reference: http://www.techrepublic.com/article/what-is-php/5074693

E-mail

- Predstavlja način prijenosa tekstualnih poruka putem komunikacijskih mreža, najčešće Interneta. Usluga omogućava umetanje dodatnih datoteka kao privitke (engl. attachment), a ovisno o poslužitelju usluge može postojati ograničenje na količinu, veličinu i tip datoteka. Elektronička pošta je postala standard za poslovnu komunikaciju, te je zamijenilo standardne dopise (dopisi se i dalje šalju ali putem elektroničke pošte). Nedugo nakon popularizacije elektronička pošta je postala medij za prijenos raznih zlonamjernih, štetnih programa kao što su crvi i virusi. Uporabom raznih heurističkih metoda prepoznavanja ovo se većinom spriječilo, no i dalje se dnevno razmjenjuju razne (bezopasne) spam ili junk poruke kojima je cilj reklamirati neki proizvod ili uslugu. - Predstavlja način prijenosa tekstualnih poruka putem komunikacijskih mreža, najčešće Interneta. Usluga omogućuje umetanje dodatnih datoteka kao privitke (engl. attachment), a ovisno o poslužitelju usluge može postojati ograničenje na količinu, veličinu i tip datoteka. Elektronička pošta je postala standard za poslovnu komunikaciju, te je zamijenilo standardne dopise (dopisi se i dalje šalju ali putem elektroničke pošte). Nedugo nakon popularizacije elektronička pošta je postala medij za prijenos raznih zlonamjernih, štetnih programa kao što su crvi i virusi. Uporabom raznih heurističkih metoda prepoznavanja ovo se većinom spriječilo, no i dalje se dnevno razmjenjuju razne (bezopasne) spam ili junk poruke kojima je cilj reklamirati neki proizvod ili uslugu.
Reference: http://www.webopedia.com/TERM/E/e_mail.html

MAC protokol (Komunikacijski protokol za pristup mediju)

- Media Access Control (MAC) je protokol za komunikaciju podacima, također poznat kao Medium Access Control protokol (protokol upravljanja pristupom mediju). On omogućuje mehanizme adresiranja i kontrole pristupa kanalima koji služe za komunikaciju terminala, odnosno čvorišta, s mrežom koja ima više pristupnih točaka.
Reference: http://ahyco.ffri.hr/ritehmreze/teme/mac.htm

IV(Inicijalizacijski vektor)

- Broj koji se koristi zajedno sa tajnim ključem prilikom šifriranja podataka. Stalno se mijenja kako bi osigurao nasumičnost što je vrlo važno svojstvo u svim kriptografskim algoritmima.
Reference: http://whatis.techtarget.com/definition/initialization-vector.html

Društveni inženjering

- Oblik zavaravanja osoba, umjesto računala. - Društveni inženjering je oblik zavaravanja ljudi (a ne računala) kako bi obavili određene radnje ili izdali povjerljive informacije. Glavni cilj društvenog inženjeringa je prikupljanje informacija pomoću kojih će napadač lakše napasti informacijskih sustav ili ostvariti neovlašten pristup.
Reference: http://searchsecurity.techtarget.com/definition/social-engineering

DNS

- DNS (eng. Domain Name System) je hijerarhijski sustav imenovanja izgrađen na distribuiranim bazama podataka za računala, usluge ili bilo koji resurs spojen na Internet ili privatnu mrežu.
Reference: http://www.kb.iu.edu/data/adns.html

XML – XML (eng. EXtensible Markup Language) je jezik za označavanje podataka. Ideja je bila stvoriti jedan jezik koji će biti jednostavno čitljiv i ljudima i računalnim programima. U XML-u se sadržaj uokviruje odgovarajućim oznakama koje ga opisuju i imaju poznato, ili lako shvatljivo značenje.
Reference: http://webdesign.about.com/od/xml/a/aa091500a.htm

Brute-force napad (Napad grubom silom)

- U kriptografiji napad grubom silom podrazumijeva strategiju pronalaska tajnog ključa ili lozinke koja se, u teoriji, može iskoristiti protiv svakog kriptografskog algoritma. Podrazumijeva sistematično isprobavanje svih mogućih ključeva ili lozinki dok se ne otkrije ispravan. U najgorem slučaju mora se proći kroz cijeli prostor ključeva.
Reference: http://www.computerhope.com/jargon/b/brutforc.htm

API

-API (eng. Application Programming Interface) predstavlja skup dobro definiranih pravila i koraka koji omogućuju interakciju dvaju ili više sustava. Služi kao sučelje između različitih programskih proizvoda i omogućuje njihovu interakciju.
Reference: http://www.webopedia.com/TERM/A/API.html

WWW

- WWW (eng. World Wide Web) je jedna od najkorištenijih usluga Interneta koja omogućava dohvaćanje dokumenata. Dokumenti mogu sadržavati tekst, slike i multimedijalne sadržaje, a međusobno su povezani poveznicama (eng. hiperlink).
Reference: http://www.webopedia.com/TERM/W/World_Wide_Web.html

SQL - SQL (Structured Query Language)) je programski jezik za pohranu, upravljanje i dohvat podataka pohranjenih u relacijskoj bazi podataka. SQL je najraširenij programskih jezik za upravljanje bazama podataka.
Reference: http://www.1keydata.com/sql/sql.html

DNS lažiranje

- Kod napada lažiranjem DNS priručne memorije, napadač šalje posebno oblikovani DNS odgovor DNS poslužitelju s namjerom da lažna informacija u DNS odgovoru bude pohranjena u priručnu memoriju DNS poslužitelja. Ovisno o informaciji u lažnom DNS odgovoru, moguć je DoS (eng. Denial of Service) ili MITM (eng. man-in-the-middle) napad.
Reference: http://www.networkworld.com/news/tech/2008/102008-tech-update.html

8. Reference

[1] Paterva
http://www.paterva.com, 15.5.2012

[2] Paterva,
http://www.paterva.com/web5/documentation/localTransforms-SpecIII.pdf 15.5.2012

[3] Youtube,
https://www.youtube.com/playlist?list=PLC9DB3E7C258CD215, 16.5.2012

[4] Net security
http://www.net-security.org/secworld.php?id=12737, 20.5.2012

[5] Social Networking Special Ops: Extending Data Visualization Tools for Faster Pwnage

[6] Ethical hacker,
http://www.ethicalhacker.net/content/view/202/24, 20.5.2012

[7] Maltego blog,
http://maltego.blogspot.com/, 12.5.2012

[8] Slide Share,
http://www.slideshare.net/thrashor/hacker-tool-talk-maltego, 19.5.2012

[9] Holistic info section
http://holisticinfosec.org/toolsmith/pdf/december2009.pdf, 20.5.2012

[10] Threat thoughts
http://threatthoughts.com/tag/maltego/, 17.5.2012