
# VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

## FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

## ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS


# IDENTIFIKACE AGRESORA KYBERŠIKANY
IDENTIFICATION OF CYBERBULLY

**BAKALÁŘSKÁ PRÁCE**
BACHELOR'S THESIS


**AUTOR PRÁCE** — **Daniel Paučo**
AUTHOR

**VEDOUCÍ PRÁCE** — **doc. Ing. Dan Komosný, Ph.D.**
SUPERVISOR


**BRNO 2018**

## ABSTRAKT

Predložená bakalárska práca sa zaoberá možnosťami určenia identity agresora kyberšikany a je zameraná na analýzu sieťových informácií o zariadeniach agresora (počítač, mobilný telefón). Podľa zadania som v programovacom jazyku Python vytvoril aplikáciu, ktorá dokáže naklonovať ľubovoľnú webstránku a následne ju spustí na servery planetlabu. Za pomoci tejto "'phishingovej"' webstránky, aplikácia dokáže zachytávať sieťové informácie o všetkých svojich návštevníkoch, ktoré si ukladá na neskoršie využitie. Najväčším prínosom aplikácie je že funguje aj v tzv. realtime móde kedy aktívne ukazuje IP adresy, ktoré sú momentálne pripojené na spustenom webe. Okrem toho ukazuje aj informácie ako kde sa daná IP adresa nachádza: štát, región, mesto a geolokačné údaje. Ďalej je z týchto informácií možné vyčítať taktiež operačný systém, použitý prehliadač, rozlíšenie prehliadača a počet návštev webu.



## KĽÚČOVÉ SLOVÁ

Kyberšikana, Zákon o elektronických komunikáciách, IP adresa



## ABSTRACT

This bachelor thesis deals with the options of determining the identity of the aggressor of the cyberbullying and it is focused at the analysis of the network information of the aggressor's devices (computer, smartphone). Regarding the layout of the thesis was created application which is able to clone any website and consequently run it on the server of planetlab. Thanks to this "'phishing"' website, the application is able to get network information about all visitors and saves it for later usage. Most important part of the application is that it is working in realtime mode where shows the IP addresses which are currently connected to the website. Besides that it also shows information like location of the IP address: country, region, city and geolocation. The application also shows operating system, user agent, resolution of the browser a the number of visits of the website.



## KEYWORDS

Cyberbullying, the Electronic Communications Act, IP address

PAUČO, Daniel. *Identifikace agresora kyberšikany*. Brno, 2018, 45 s. Bakalárska práca. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedúci práce: doc. Ing. Dan Komosný, CSc.

# VYHLÁSENIE

Vyhlasujem, že som svoju bakalársku prácu na tému „Identifikace agresora kyberšikany“ vypracoval(a) samostatne pod vedením vedúceho bakalárskej práce, využitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autor(ka) uvedenej bakalárskej práce ďalej vyhlasujem, že v súvislosti s vytvorením tejto bakalárskej práce som neporušil(a) autorské práva tretích osôb, najmä som nezasiahol(-la) nedovoleným spôsobom do cudzích autorských práv osobnostných a/alebo majetkových a som si plne vedomý(-á) následkov porušenia ustanovenia § 11 a nasledujúcich autorského zákona Českej republiky č. 121/2000 Sb., o práve autorskom, o právach súvisiacich s právom autorským a o zmene niektorých zákonov (autorský zákon), v znení neskorších predpisov, vrátane možných trestnoprávnych dôsledkov vyplývajúcich z ustanovenia časti druhej, hlavy VI. diel 4 Trestného zákoníka Českej republiky č. 40/2009 Sb.

Brno ..... .....

podpis autora(-ky)

## POĎAKOVANIE

Rád by som poďakoval vedúcemu bakalárskej práce pánovi doc. Ing. Danovi Komosnému, Ph.D. za odborné vedenie, konzultácie, trpezlivosť a podnetné návrhy k práci.


Brno ..... .....

podpis autora(-ky)


Faculty of Electrical Engineering
and Communication
Brno University of Technology
Purkynova 118, CZ-61200 Brno
Czech Republic
http://www.six.feec.vutbr.cz

## POĎAKOVANIE

Výzkum popsaný v tejto bakalárskej práci bol realizovaný v laboratóriách podporených projektom SIX; registračné číslo CZ.1.05/2.1.00/03.0072, operačný program Výzkum a vývoj pro inovace.

Brno ..... .....

podpis autora(-ky)


EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

# OBSAH

# ZOZNAM OBRÁZKOV

# ÚVOD

Rozmachom informačných technológií posledných niekoľko rokov narastá počet užívateľov internetu a tým aj hrozieb, ktoré na nich číhajú. Za týmto fenoménom stoja hlavne smartfóny, ktoré sa často predávajú až za pomerne nízku cenu a tak si ich môže ktokoľvek dovoliť. Počet užívateľov smartfónov od roku 2014 do roku 2017 stúpol až o 750 miliónov[1] a do budúcnosti sa predpokladá ďalší nárast.

Pre väčšinu mladých ľudí je už bežné, že podstatnú časť svojho času trávia na internete. Tento jav sa týka predovšetkým dnešných detí, ktoré neustále potrebujú byť online a v spojení so svojimi vrstovníkmi. Internet sa pre ne stáva čím ďalej populárnejší, pretože ak v reálnom živote nemajú kamarátov, majú problém sa niekomu prihovoriť, alebo sa cítia menejcenné, internet je pre ne miesto, kde si vedia vytvoriť celkom novú virtuálnu identitu. S potrebou byť stále online prichádzajú aj možné negatíva a riziká – kyberšikana.

Výstupným produktom tejto bakalárskej práce je nástroj, ktorý slúži na vystopovanie agresora kyberšikany. Nástroj sa volá *Tracer* a funguje na princípe zadania verejnej IP adresy agresora a jej následnom vystopovaní z dostupných online databáz. Taktiež obsahuje funkcie ako klonovanie zadanej webstránky, vloženie IP loggeru do zdrojového kódu webstránky, alebo spúštanie a vypínanie httpd servera.

Práca je členená na 6 kapitol, kde v prvej kapitole je popísaná kyberšikana, jej prejavy, druhy a média, ktorými sa najčastejšie šíri. Druhá kapitola popisuje stopovanie agresora kyberšikany tak z technického hľadiska, ako aj z právneho. Popisuje zákon o elektronických komunikáciách alebo ako prebieha postup stopovania podľa trestného rádu ČR. Tretia kapitola obsahuje popis už existujúcich nástrojov na zber informácií a popis, ako fungujú. Štvrtá kapitola popisuje vytvorený nástroj na zber informácií o agresorovi (kusy kódu, vývojový diagram). V piatej kapitole je popísané nasadenie aplikácie a zber informácií, ako som postupoval pri nastavovaní servera, ktorý slúži na zbieranie dát o agresorovi. V poslednej kapitole sú príklady využitia vytvorenej aplikácie ako v realtime móde, tak aj práce s už uloženými dátami.

[1] Zdroj: https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

# 1 KYBERŠIKANA

Kyberšikana má rovnaké rysy a prejavy ako tradičná šikana. Predpona *kyber* popisuje spojenie s internetom alebo počítačom, to znamená, že kyberšikana sa odohráva vo virtuálnom prostredí tzv. kyberpriestore. Pod pojmom kyberšikana sa rozumie zámerné urážanie, vyhrážky, obťažovanie, či zverejňovanie intímnych informácií za pomoci komunikačných prostriedkov.

Kyberšikana najčastejšie prebieha cez internet (e-maily, sociálne siete,...) alebo cez telefón (SMS, MMS). Pre označenie toho, kto kyberšikanu pácha sa používa termín **agresor**. Tento agresor často koná anonymne, aby obeť nevedela, kto je daný agresor. Pre jednoznačné definovanie agresie sa objavujú pomerne rôzne definície, toto je jedna z krátkych a výstižných: „Ľudská agresia je akékoľvek chovanie zamerané voči druhému, ktoré so sebou nesie priamy zámer ublížiť [...] náhodné ublíženie nie je klasifikované ako výsledok agresie, pretože nie je zámerné.“[1].

Podľa niektorých štúdií, aby sa jednalo o kyberšikanu, je potrebné, aby tento agresívny akt naplnil tieto základné prvky[3]:

- **Deje sa prostredníctvom elektronických médií.**
- **Opakovanosť.**
- **Zámernosť agresívneho aktu zo strany útočníka.**
- **Mocenská nerovnováha.**
- **Obeť vníma toto jednanie ako nepríjemné, ubližujúce.**

## 1.1 Prejavy kyberšikany

Kyberšikanu je možné rozdeliť do niekoľkých podskupín a každá z nich predstavuje vážny spoločenský problém. Tu sú najčastejšie typy a ich prejavy[3]:

- **Vydávanie sa za niekoho iného.**
- **Vylúčenie a ostrakizácia.**
- **Flaming.**
- **Kyberharašenie a kyberstalking.**
- **Odhalenie a podvádzanie.**
- **Happy slapping.**

***Vydávanie sa za niekoho iného***

V tomto prípade sa agresor vydáva za obeť kyberšikany. Môže to dosiahnuť tým, že si vytvorí falošný profil obete, kde pridá jej fotky, vyplní profil a vystupuje pod identitou obete, spravidla nevhodným a ubližujúcim spôsobom[6].

***Vylúčenie a ostrakizácia***

V tomto prípade je obeť kyberšikany vylúčená z nejakej skupiny, do ktorej by chcela alebo mala patriť. Nejedná sa tu ani tak o žiadny prvok agresie, ale skôr o frustráciu danej obete, že nepatrí tam, kam by chcela. Pre príklad môže byť uvedné aj vylúčenie z týmu v počítačových hrách.

***Flaming***

V tomto prípade sa jedná o hádku medzi dvomi, alebo viacerými účastníkmi komunikácie. Názov *flaming* pochádza z anglického flame - oheň, čiže ohnivá výmena názorov. Tieto výmeny názorov končia často nadávkami, až výhražkami. Niekedy môže byť ťažké posúdiť takúto situáciu, pretože niektorí ľudia tieto hádky zámerne vyvolávajú.

***Kyberharašenie a kyberstalking***

Kyberharašenie sa dá opísať ako využitie komunikačných technológií na nevyžiadanú komunikáciu s inou osobou. Kyberharašenie nemá presnú definíciu, pretože môže mať veľa foriem. Jeho typickou formou je, že agresor obeti zámerne posiela množstvo nechcených správ. Množstvo mladých ľudí si na internete hľadá rôzne známosti s neznámymi, ktoré môžu vyústiť až v nechcenú komunikáciu, ktorej sa nevedia zbaviť.

Kyberstalking môže zahŕňať falošné obvinenia, ohováranie, zasielanie správ obsahujúcich vyhrážky, zastrašujúce zdelenia a jeho súčasťou môže byť aj vydieranie[9]. Často môže byť sprevádzaný aj stalkingom v realite, kde sa obeť môže obávať aj o svoje bezpečie.

***Odhalenie a podvádzanie***

Jedná sa o odhalenie a zverejnenie informácií o obeti ľuďom, ktorým tieto informácie neboli určené[6]. Najčastejšie sa jedná o informácie osobného, či intímneho charakteru ako sú napríklad fotky, alebo útržky z konverzácie.

***Happy slapping***

Fenomén, ktorý sa dostáva do popredia v posledných rokoch. V minulosti sa jednalo o to, že agresor si vybral neznámu okoloidúcu obeť, ktorú "sfackoval", niekto to nahrával na telefón a video potom zverejnil na internet. V dnešnej dobe často tieto

videá prekračujú medze zákona a fyzický útok môže spôsobiť aj vážne zranenia.

## 1.2 Médiá šírenia kyberšikany

V závislosti od toho, aké médium si agresor zvolí na šírenie kyberšikany, sa líši aj ich podoba. V tejto sekcií je popísaných zopár najčastejších médií, ktoré sú používané na šírenie kyberšikany.

***Sociálne siete***
Jedná sa o webové služby fungujúce pomocou webovej stránky, ktoré slúžia na nadväzovanie a udržiavanie kontaktov medzi ľuďmi. Ich hlavnou ideou je vytvorenie si vlastného profilu, ktorý môže byť verejný alebo čiastočne verejný a upraviť si ho podľa svojích predstáv. Najpodstatnejšou časťou sociálnych sietí je možnosť zdieľania statusov, fotografií atď. Prejavy kyberšikany na sociálnych sieťach môžu zahŕňať napríklad ubližujúce komentáre, zverejňovanie fotiek alebo osobných informácií obete a taktiež môže dôjsť k *ostrakizácií* – obeť bude vylúčená zo skupiny, alebo zoznamu priateľov.

***Online hry***
Môže sa jednať o akúkoľvek platformu, na ktorej sa dané hry hrajú, či už PlayStation alebo PC, hráči majú možnosť komunikovať medzi sebou, či už prostredníctvom textových správ alebo audiokomunikácie. Najčastejšie v tomto prostredí dochádza k *flamingu*, kde ostatní hráči osočujú iného, nadávajú mu a môže dôjsť taktiež k *ostrakizácií* – vylúčeniu hráča z hry alebo zo skupiny hráčov. Taktiež môže dochádzať k neustálemu ubližovaniu virtuálnej postavy v rámci jednej hry, kedy dochádza k frustrácií obete.

***Instant messaging a správy***
K tejto forme kyberšikany môže dojsť tak, že agresor odosiela obeti v reálom čase nechcené správy, môže si vytvoriť profil, ktorý má podobnú prezývku ako profil samotnej obete, a vystupovať pod jej menom. Pri SMS a MMS môže agresor neustále obťažovať obeť správami s ubližujúcim obsahom, alebo dokonca aj s nevhodnými obrázkami.

***E-mail***
E-mail patrí medzi najpoužívanejší prostriedok komunikácie na internete. Práve pre toto sa využíva veľmi často na šírenie kyberšikany. Jeho veľkou výhodou je, že odosielateľ môže ostať v anonymite – buď nie je možné e-mailovú adresu priradiť k člo-

veku, alebo si agresor zmení zdrojovú adresu. E-mailová komunikácia sa často stáva aj kanálom pre šírenie *spamu*, ktorý však nie je formou kyberšikany, ale online obťažovania.

***Chatovacie miestnosti***
Jedná sa o miesta v online svete, kde je možné komunikovať s inými ľuďmi buď v reálnom čase (chat), alebo asynchrónne (diskusné fórum). Najčastejšie sa chatovacie miestnosti a fóra tvoria s určitou tematikou, ktorej sa venujú a ľudia tak môžu zdieľať informácie, ktoré ich zaujímajú. V tomto prostredí často dochádza k prejavom kyberšikany ako napríklad ohováranie, ostrakizácia, alebo najčastejšie flaming. V chatovacích miestnostiach a na fórach je jednoduché vydávať sa za niekoho iného, chovať sa nevhodne a tým uviesť obeť do problémov. Častým javom je aj vydávanie sa za známeho obete a snažiť sa dostať z nej intímne informácie. Toto médium často využívajú kyberstalkeri.

## 1.3 Prečo vlastne ku kyberšikane dochádza?

Aj keď sú známe charakteristiky online prostredia, ktoré kyberšikane celkom nahrávajú a pomáhú jej vznikať, o konkrétnych motívoch detí a dospievajúcich, ktorí sa zapájajú do kyberšikany sa veľa nevie – v tejto oblasti je zatiaľ vykonaných pomerne málo štúdií.

Pri tradičnej šikane sa pri agresoroch na otázku, prečo šikanujú, najčastejšie stretneme s odpoveďou v zmysle, že obeť agresiu vyvolala, zaslúžila si ju atď[7]. Veľmi často je však zmienený aj fyzický vzhľad[4].

Jedným z najčastejších dôvodov pre kyberšikanu je odplata. Obete tradičnej šikany môžu hľadať spôsob, ako sa agresorovi z offline reality pomstiť spôsobom, ktorý zaistí anonymitu, čím znemožní ďalšiu odplatu zo strany agresora[5]. Práve z tohto výskumu Hinduji a Patchina hneď za odplatou nasledovala možnosť, že si to obeť vlastne zaslúžila a presvedčenie, že kyberšikana je iba žart. Oboje by mohlo poukazovať na jednoduchosť s akou je možné si kyberšikanu sám pred sebou obhájiť[5].

Najnovšie výsledky v tejto oblasti prináša štúdia zameraná priamo na motiváciu dospievajúcich k tradičnej šikane a kyberšikane[10]. Pri oboch typoch chovania boli najčastejšie uvedné dôvody agresie získanie si pozornosti druhých, cítiť sa sám lepšie, presadiť sa a zasadnúť si na niekoho, kto je iný ako ostatní.

Zhrnutím súčasných poznatkov vzniku šikany a kyberšikany by sa dalo povedať, že mnoho javov, kvôli ktorým šikana vzniká sa prekrýva a kyberšikanu je potrebné skúmať, chápať a taktiež riešiť v kontexte tradičnej šikany. Podľa preskúmaných

študií vzniká pomerne málo prípadov kyberšikany bez toho, aby sa niečo udialo v offline svete. Preto by mala prevencia v tejto oblasti pochádzať z offline sveta.

# 2 PRÁVNE PODKLADY

V Českej republike sa ani šikana ani kyberšikana nepovažujú za trestný čin. Nastáva tu však možnosť, že v určitých prípadoch by mohlo jednanie agresora prekročiť hranicu. Ako je opísané vyššie v sekcii Prejavy kyberšikany, ak by sa jednalo napríklad o ukradnutie identity, obťažovanie, vydieranie, alebo iné, môže sa jednať o naplnenie skutkovej podstaty trestného činu. Popis týchto jednotlivých činov je uvedný v Trestnom zákoníku[1].

„K tomu, aby bol páchateľ postihnutý musí byť starší 15 rokov (15–18 rokov mladistvý). K trestnej zodpovednosti mladších 15 rokov nedochádza, neznamená to však, že nemôžu byť postihnutí inak, prípadne môžu byť postihnutí rodičia. Neplnoletý páchateľ môže byť postihnutý nariadením ústavnej výchovy, môže nad ním byť stanovený dohľad. Pokiaľ ide o trestné sadzby, je v prípade šikany možný aj jednočinný skutok, tzn. že jedno jednanie môže byť kvalifikované ako viac trestných činov.“[8].

## 2.1 Zákon o elektronických komunikáciách

Od dňa 22. februára 2005 platí v Českej republike zákon o elektronických komunikáciách ZEK[2], ktorý sa vzťahuje aj na poskytovateľov internetových služieb. Podnikateľ zaisťujúci verejnú komunikačnú sieť, alebo verejne dostupnú službu elektronických komunikácií je povinný na náklady žiadateľa zriadiť a zabezpečiť v určených bodoch svojej siete rozhranie pre pripojenie koncového telekomunikačného zariadenia pre odposluch a záznam správ. Kompetentné orgány prekazujú svoje oprávnenie k odposluchu a záznamu správ predaním písomnej žiadosti, ktorá obsahuje jednacie číslo, a ktoré je podpísané zodpovednou osobou. Podnikateľ zaisťujúci verejnú komunikačnú sieť, alebo verejne dostupnú službu elektronických komunikácií je povinný uchovávať po dobu 6 mesiacov prevádzkové a lokalizačné údaje. Prevádzkové údaje sú ustanovením § 90 ods. 1 ZEK definované ako akékoľvek údaje spracované za účelom prenosu správy sieťou, alebo za účelom účtovania. Lokalizačné údaje sa podľa § 91 ods. 1 ZEK rozumejú akékoľvek spracované údaje určujúce zemepisnú polohu koncového zariadenia uživateľa verejne dostupnej služby elektronických komunikácií[2]. Po uplynutí tejto doby je subjekt povinný tieto údaje zlikvidovať, pokiaľ neboli

[1] https://www.zakonyprolidi.cz/cs/2009-40

[2] Zdroj: https://www.zakonyprolidi.cz/cs/2005-127

poskytnuté orgánom oprávneným k ich využitiu. Toto uchovávanie platí len pre subjekty podľa ZEK, mimo ZEK sa nevzťahuje a uchovávanie nie je nutné. Povinný subjekt je podnikateľom v elektronických komunikáciách, ktorý poskytuje verejnú sieť elektronických komunikácií, prípadne služby elektronických komunikácií.

## 2.2 Stopovanie agresora z právneho hľadiska

Ako bolo spomenuté vyššie v sekcii Zákon o elektronických komunikáciách, povinné subjekty majú uloženú povinnosť uchovávať prevádzkové a lokalizačné údaje a taktiež aj špecifický postup orgánov činných v trestnom riadení, ktorý je nutné využívať pri zaisťovaní legálnych dôkazov. Na získanie týchto údajov je potrebné mať vydaný písomný príkaz s odôvodnením od predsedu senátu podľa § 88a ods. 1 TŘ[3]. Vzhľadom k nepriamej povahe dôkazov môže nastať spochybnenie niektorých záverov v dokazovaní. Prevádzkové a lokalizačné údaje podľa českej judikatúry nevedú k identifikácii presnej osoby ako páchateľa, alebo osoby zúčastnenej na trestnom čine, pretože vedú vždy iba k identifikácii komunikačného prístroja. Najkomplikovanejšie je použitie IP adresy, kde je nutné rozlišovať medzi statickou a dynamickou adresou. Podľa WP29[4] sa v prípade dynamickej adresy jedná o osobný údaj, pretože poskytovateľ pripojenia je schopný na základe logov priradiť IP adresu ku danému stroju. Aj keď majú metadáta veľkú výpovednú hodnotu, nie je možné tvrdiť, že bez iných údajov jednoznačne identifikujú konkrétnu osobu agresora[2].

[3]Zdroj: https://www.zakonyprolidi.cz/cs/1961-141

[4]WP29 guidelines on the Data Protection Officer requirement in the GDPR

# 3 ANALÝZA MOŽNOSTÍ ZBERU INFORMÁCIÍ O AGRESOROVI

Najdôležitejšou časťou zachytených informácií je verejná IP adresa agresora, ktorá bude využitá na jeho stopovanie. Tu sa nachádza najväčši problém danej bakalárskej práce. Pokiaľ užívateľ nemá u providera zaplatenú alebo inak danú verejnú IP adresu, tak zachytená verejná IP adresa ukazuje na poskytovateľa internetového pripojenia. V tomto prípade sú dve možnosti:

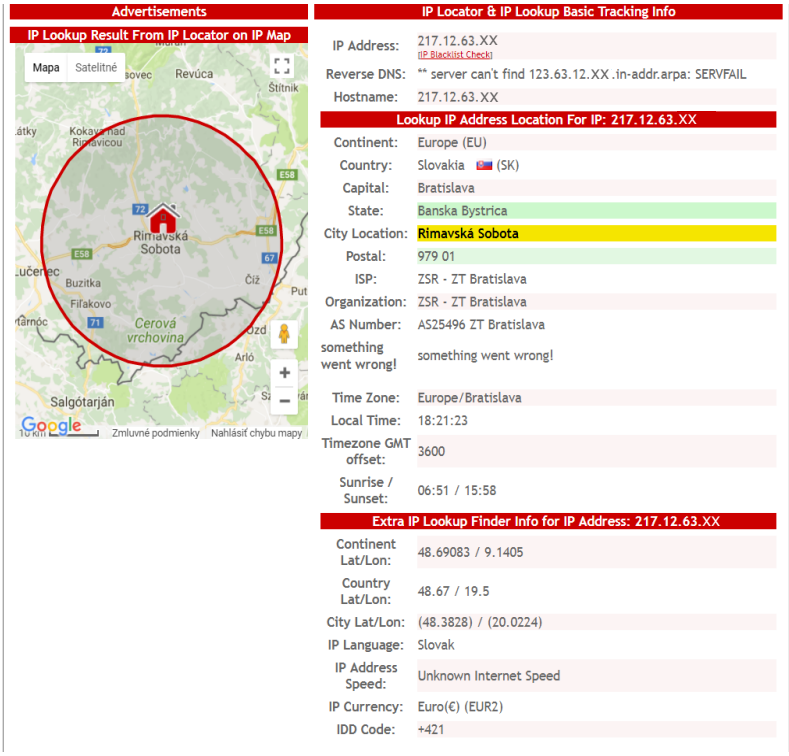
1. Jedná sa o lokálneho ISP,
2. Jedná sa o globálneho ISP.

## 3.1 Geolokácia

Po získaní IP adresy agresora je možné využiť tzv. službu IP geolocation, ktorá slúži na vykreslenie polohy agresora do mapy. Touto službou je možné zistiť informácie o počítači, routri, alebo vlastníkovi daného zariadenia.

***Lokálny ISP***

Ak sa jedná o lokálneho internetového providera, ktorý poskytuje služby v menšom meste a okolitých dedinách, vystopovanie agresora je tak ľahšie, pretože lokálny ISP nemá tak veľký počet zákazníkov ako globálny provider a sledovanie dátového toku užívateľov je tak jednoduchšie. Pokiaľ sa obeť sama rozhodne stopovať IP adresu, tak vidí názov providera. Podľa tejto informácie sa okruh potencionálnych agresorov výrazne zmenšuje oproti globálnemu ISP. Príkladom lokálneho poskytovateľa služieb môže byť napríklad *DjNet*.




Obr. 3.1: Služba *IP-Tracker*[1]– lokálny ISP.

***Globálny ISP***

Ak sa jedná o globálneho internetového poskytovateľa, ktorý poskytuje služby vo väčších mestách, alebo aj po celej republike, vystopovanie agresora je celkom zložitý proces a trvá od niekoľkých dní až po mesiace, v tých lepších prípadoch. Príkladom globálneho ISP je napríklad $O_2$, alebo *UPC*.

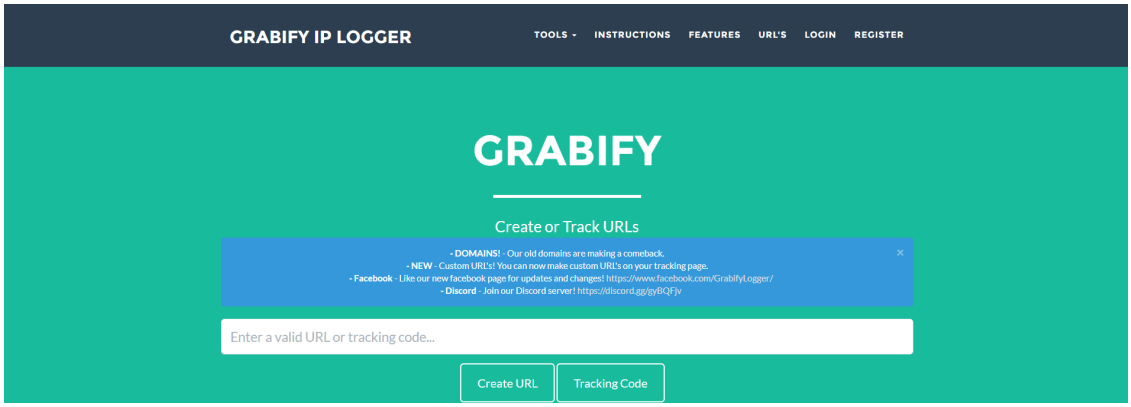
Najlepšia možná cesta na vystopovanie agresora je podať oznámenie na Políciu ČR, ktorá spolupracuje s poskytovateľmi internetového pripojenia čo je popísané vyššie v sekcii Zákon o elektronických komunikáciách.

## 3.2 Existujúce nástroje na zber informácií

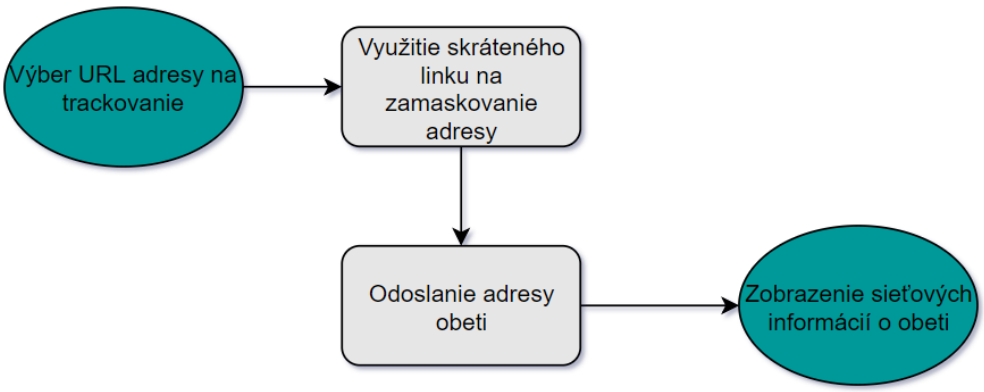
Na internete v dnešnej dobe už existuje väčší počet nástrojov, ktoré slúžia na zber informácií o danom užívateľov napr.: *IP logger, Grabify, Blasze,...* Tieto nástroje slúžia ako tzv. URL shortener – skracovač URL adries, ktorý po zakliknutí danej adresy zbiera štatistiky o užívateľovi a pomáha vo vystopovaní IP adresy, IP lokácie, zbiera dáta pre blog, fórum. Jednou z najväčších výhod tohto nástroja je možnosť vytvorenia si „neviditeľného“ IP logovacieho obrázku. Tento obrázok má rozmer

[1]Zdroj: http://www.ip-tracker.org/locator/ip-lookup.php

1×1px, preto je nazývaný „neviditeľným“. Obrázok sa môže vložiť buď na hostovaný web, alebo sa môže vložiť do e-mailu. Ak má agresor povolené načítanie obrázkov v e-mailovej schránke, po otvorení e-mailu je obrázok načítaný a ihneď odosiela žiadosť na server, kde sa daný obrázok nachádza, aby zachytil dáta o užívateľovi.




Obr. 3.2: Služba *grabify*[2].




Obr. 3.3: Vývojový diagram služby *grabify*.

Ďalším takýmto nástrojom je napríklad *iptrackeronline*, ktorý po zadaní IP adresy zobrazí údaje ako kontinent, štát, mesto, geolokačné údaje a iné, viď obrázok 3.4.

[2]Zdroj: https://grabify.link/


Obr. 3.4: Nástroj *www.iptrackeronline.com.*

## 3.3 WHOIS

WHOIS je protokol, ktorý funguje na báze žiadosti a odpovede. Zadaná žiadosť je smerovaná na databázy, ktoré uchovávajú registrovaných užívateľov alebo prevádzkovateľov internetových zdrojov ako sú doménové mená, IP adresy alebo autonómne systémy. Tento protokol odosiela databázový obsah v čitateľnej forme pre ľudí, tzn. že s odpoveďou už nie je potreba vykonávať napríklad žiadne dekódovanie.

WHOIS bol štandartizovaný v skorých 80. rokoch na vyhľadávanie domén, ľudí a iných zdrojov spojených s doménami. V tých časoch, ako boli všetky registrácie spracovávané jednou organizáciou, pre všetky whois žiadosti bol využívaný jeden centralizovaný server. Vďaka nemu bolo vyhľadávanie daných informácií veľmi jednoduché.

V modernom internete, služba WHOIS typicky komunikuje pomocou protokolu TCP. Servery zachytávajú žiadosti na známom porte 43. Klienti sú jednoduché aplikácie, ktoré založia pripojenie k serveru, prenesú textový záznam s menom zdroja, ktorý bol dotazovaný a očakávajú odpoveď vo forme sekvencie textu záznamov nájdených v databáze. Jednoduchosť tohto protokolu taktiež dovoľuje aplikácií, alebo príkazovej riadke dotazovať sa na WHOIS server pomocou protokolu Telnet.

V prípade, že registrantova identita je verejná, každý môže jednoducho pristúpiť

k dátam o doméne cez WHOIS. V prípade, že sa jedná o privátnu registráciu, zistenie registračných informácií môže byť obtiažne. Za túto službu, aby dáta ostali v anonymite, sa však pripláca. Ak už registrant mal niekedy zaregistrovanú doménu bez tejto služby, je možné dohľadať tieto informácie v cache pamäti WHOIS databázy.[3]

## 3.4 Phishing

Phishing pochádza z anglického slova password fishing, čo doslova znamená rybolov hesiel a zaraďuje sa medzi techniky sociálneho inžinierstva. Túto časť som do svojej bakalárksej práce zahrnul z dôvodu, že v dnešnej dobe sa phishing stále pokladá za najjednoduchší spôsob získania rôznych informácií o obeti. Útok najčastejšie prebieha tak, že podvodník si skopíruje obsah vybranej dôveryhodnej webstránky, tento obsah umiestni na svoj vlastný server a čaká kým sa mu niekto chytí do pasce a odošle mu svoje dôverné informácie ako napríklad prihlasovacie údaje, alebo cielene odošle obeti odkaz na daný web. Podľa štatistík z roku 2017[4], vznikne počas jedného mesiaca priemerne 1,4 milióna phishingových webstránok.

Tak ako každý kybernetický útok, aj phishing má rôzne vektory útoku:

*Spear phishing* – tento útok rozvíja phishingovú analógiu tak, že útočníci sa zameriavajú na špecifické obete alebo organizácie. Namiesto toho, aby sa pokúšali získať dôležité dáta tisícok ľudí, pre útočníkov príde lukratívnejšie zamerať sa na prosperujúce organizácie. Tento vektor útoku je jeden z najúspešnejších z phisingových útokov a je to tým, že útočníci strávia mnoho času vytváraním informácií, špecifických pre recipienta.

*Whaling* – phishingový útok zameraný priamo na vysoko postavených ľudí v organizáciách, z toho bol odvodený aj názov whaling. Ukradnuté dáta sú viac cenné ako tie bežných zamestnancov. Whaling si vyžaduje väčší prieskum pretože útočník potrebuje vedieť s kým cielená obeť komunikuje a o čom.

*Clone phishing* – na tento útok je potrebné vytvoriť repliku legitímnej webstránky na oklamanie obete, aby si myslela, že webstránka je reálna. Po pristúpení sa danú webstránku môžu byť o uživateľovi získavané dáta ako jeho IP adresa, poloha, rozlíšenie okna prehliadača, história prehliadania a iné informácie. Ak sa stránka tvári legitímne a nachádzajú sa na nej nejaké formuláre, je pravdepodobné, že sa na

[3] https://whois.icann.org/en/about-whois

[4] http://www.zdnet.com/article/1-4-million-phishing-websites-are-created-every-month-heres-who-the-scammers-are-pretending-to-be/

stránke nachádza aj keylogger, ktorý zachytáva všetky stlačené klávesy a odosiela ich útočníkovi na server.

## 3.5 Cookies

Komunikácia medzi webovým prehliadačom a serverom je definovaná HTTP protokolom. Tento protokol popisuje že každá URL žiadosť a jej odpoveď sú párové správy nezávislé na budúcnosti alebo minulosti. Najlepší spôsob pre zachovanie informácií medzi žiadosťami je využitie skriptovacieho jazyka Javascript. Cookies slúžia ako vylepšenie pre HTTP protokol, ktorý umožňuje tieto informácie ukladať.

Každá URL adresa alebo HTTP žiadosť vytvorená prehliadačom sa pretransformuje do riadkov textu nazývaných hlavičky, ktoré sa následne odošlú na server. Keď server odosiela odpoveď, deje sa to isté na strane servera. Cookies sú v podstate pridaný riadok v hlavičke, ktorý obsahuje cookie-style informácie. Tieto informácie sú v prehliadači pre užívateľa väčšinou neviditeľné. Ak užívateľ požiada server o načítanie obsahu stránky a server mu odpovie, môže sa tak stať že cookies informácie sú viditeľné v URL adrese, alebo sú prenášané na pozadí a tým pádom sú neviditeľné.

Kľúčovým bodom je, že cookies obsiahnuté v odpovedi servera sa ukladajú na strane klienta v prehliadači hneď po prijatí. Keď sa klient pripája na server, v žiadosti odosiela aj svoje uložené cookies, ktoré si však server iba načíta, ale neuloží si ich. Celé to funguje na tom princípe, že prehliadač nesie zodpovednosť za dáta, nie server. Server zase riadi to, čo sa má na stránke zmeniť.

### Telo cookies

Cookie sa dá považovať za premennú v jazyku Javascript, ktorá ukladá meno a hodnotu. Avšak oproti ostatným premenným je existencia cookie závislá na niekoľkých ďalších parametroch. Je to kvôli tomu, že cookies môžu byť v prehliadači načítané z akejkoľvek stránky, takže musia byť uložené osobitne.

Cookie obsahuje nasledujúce atribúty:

**meno (name)**
Tento parameter je reťazec znakov. Najčastejšie sa v ňom využívajú alfanumerické znaky a podtržníky.

**hodnota (value)**
Tento parameter je reťazec akýchkoľvek znakov. Tento reťazec musí spĺňať pravidlá

pre URL, čo znamená že funkcie escape() a unescape() by mali byť aplikované, ak sú cookies vytvorené. Meno a reťazec dokopy by mali obsahovať menej ako 4095 bytov. Akceptované sú taktiež reťazce s nulovou dĺžkou.

**doména (domain)**
Pokiaľ užívateľ prehliada rozličné stránky, tak ich cookies by sa nemali medzi sebou nijako ovplyvniť. Cookies obsahujú atribút doména, ktorý obmedzuje ich viditeľnosť pre jednu alebo viaceré stránky.

**cesta (path)**
Cesta je celkom podobná doméne, tento atribút obmedzuje viditeľnosť cookies pre niektoré časti serverovej štruktúry. Web stránka ako http://planetlab1.cesnet.cz:8080/index.php môže mať cookie s parametrom cesta '/index', ktorý je relevantný jedine pre Javascript danej stránky. Cesty reprezentujú zložky, nie samostatné súbory, takže '/usr/local/tmp' je správne, ale '/usr/local/tmp/index.php' nie.

Meno, doména a cesta spolu plne identifikujú individuálne cookie.

**dátum expirácie (expiry time)**
Dátum expirácie poskytuje jeden z dvoch čistiacich mechanizmov pre cookies. Bez tohto mechanizmu by sa cookies v prehliadači vytvárali donekonečna až kým by sa nezaplnila pamäť počítača.

Dátum expirácie je voliteľný parameter. Je to časový moment. Bez nastavenia tohto parametra sa cookie vymaže po vypnutí prehliadača. Po nastavení tohto údaju sa cookie uchová až do dátumu ktorý bol parametru zadaný. Pokiaľ bol časový údaj prekročený a prehliadač nebol spustený, cookie sa vymaže pri nasledujúcom spustení prehliadača.

**bezpečnostná značka (secure flag)**
Tento atribút môže mať hodnoty true/false. Ak je tento parameter nastavený na true, cookie je odosielané šifrovane pomocou SSL.[5]

[5]https://msdn.microsoft.com/en-us/library/ms970178.aspx

## 3.6 Ďalšie informácie o agresorovi

Metadáta sú v podstate dáta, ktoré popisujú iné dáta. Metadáta sumarizujú základné informácie o dátach, čo značne uľahčuje prácu s nimi. Bežne sú takýmito dátami autor, dátum vzniku, dátum úpravy, alebo veľkosť súboru. V prípade aplikácie *Tracer* sa jedná o metadáta ako rozlíšenie prehliadača, informácie o použitom prehliadači a operačný systém.

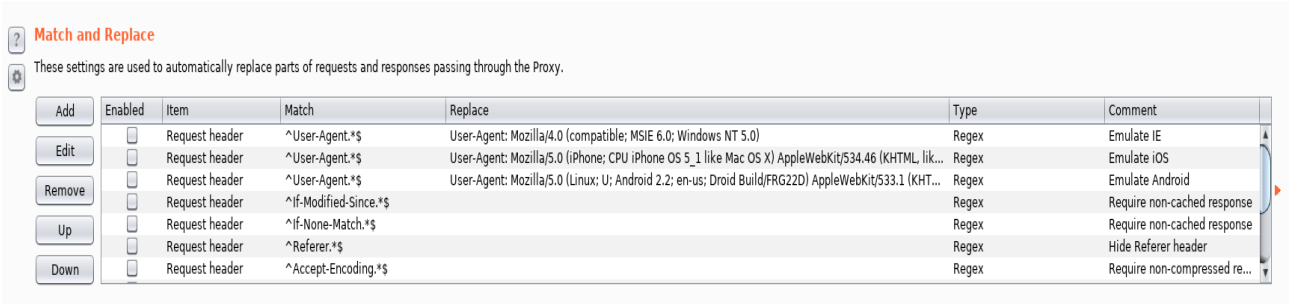
Rozlíšenie prehliadača som sa rozhodol zakomponovať medzi zachytávané dáta z toho dôvodu, že pomocou tejto informácie sa dá vo väčšine prípadov jednoznačne klasifikovať či sa jedná o počítač, alebo mobilný telefón.

Informácie o použitom prehliadači inak povedané aj User agent. Jedná sa o software, ktorý predáva webstránke informácie o použitom prehliadači a operačnom systéme. Webstránka je tak vďaka týmto informáciám schopná prispôsobiť svoj obsah príslušnému zariadeniu. Na jednu stranu je to výhoda, ale na druhú stranu sa jedná o predanie dôležitých údajov, ktoré môžu dopomôcť k identifikácií zariadenia. User agent prenáša informácie o použitom zariadení ako string, ktorý je možné vidieť na obrázku 3.5.

```
Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/66.0.3359.170 Safari/537.36
```

Obr. 3.5: Informácie predávané User agentom.

Niektoré webstránky sú však nakonfigurované tak, aby pracovali spoľahlivo iba s určitými prehliadačmi. Obsahujú v sebe kód, ktorý identifikuje použitého User agenta. Toto môže znamenať, že niektoré prehliadače nemusia dostať kompletný obsah webstránky, alebo ani nemusia byť vôbec načítané. Pre tento prípad existuje takzvaný User agent spoofing, kedy je užívateľ schopný kompletne zmeniť identifikačné informácie zariadenia. Tento spôsob sa dosť často využíva aj v penetračnom testovaní na oklamanie webstránky, že sa jedná o iné zariadenie.




Obr. 3.6: Zmena User agenta v nástroji Burp suite.

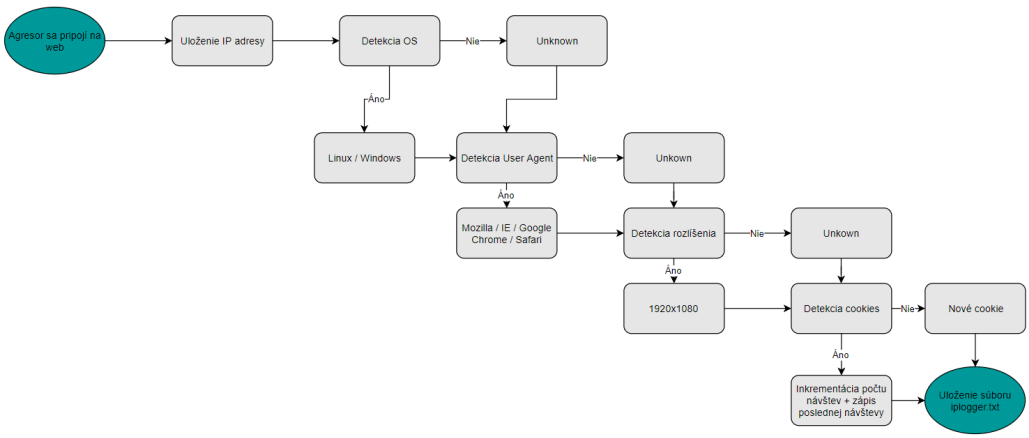
# 4 NÁSTROJ PRE ZBER INFORMÁCIÍ O AGRESOROVI

Cieľom bakalárskej práce bolo vytvoriť nástroj, ktorý bude schopný vystopovať IP adresu agresora po jej zadaní. Najťažšou časťou tejto práce je získanie verejnej IP adresy agresora. Pre tento účel bola do nástroja pridaná funkcia slúžiaca na naklonovanie zadanej webstránky. Po naklonovaní webstránky sa jej index vloží do zložky httpd servera a následne je potrebné spustiť server cez nástroj *Tracer*. Jednou z ďalších funkcií nástroja je vytvorenie tzv. skráteného linku. Vstupom do tejto funkcie je url adresa servera na ktorom beží vytvorený „phishingový“ web a jej výstupom je skrátená url adresa, z ktorej sa nedá rozpoznať o aký web sa jedná. Túto adresu je následne potrebné odoslať agresorovi a čakať kým na ňu klikne. Po navštívení stránky sa do súboru *iplogger.txt* zapíšú všetky potrebné údaje.

## 4.1 Módy aplikácie

Aplikácia *Tracer* funguje v dvoch hlavných módoch. Prvým módom je realtime mód, ktorý umožňuje sledovať aktívne pripojenia na stránke a taktiež zobrazuje všetky zistené informácie o pripojených adresách. Tento mód funguje tak, že do súboru *iplogger.txt* sa zapíšu všetky zistené sieťové informácie o agresorovi a čas, kedy sa na web pripojil. Tento čas sa následne porovnáva s aktuálnym časom a ak je rozdiel menší ako 5 minút, spojenie sa považuje za aktívne. Táto implementácia bola zvolená z dôvodu že aplikácia nebeží priamo na webovom serveri, takže nie je schopná s ním priamo interagovať.

Druhým módom je mód pasívny, kde sa v aplikácií dajú vylistovať všetky predchádzajúce pripojenia.




Obr. 4.1: Vývojový diagram aplikácie *Tracer*.

## 4.2 Implementované metódy zberu informácií

Najdôležitejšou súčasťou aplikácie je php kód, ktorý sa pomocou funkcie *generate()* vkladá do zdrojového kódu naklonovanej webstránky. Tento php kód je obsiahnutý v jednom stringu, keďže sa jedná o aplikáciu naprogramovanú v jazyku Python a inak by nebolo možné tento kód naimplementovať. Vo výpise 4.1 je možné vidieť zdrojový kód, ktorý slúži na identifikáciu operačného systému agresora.

```
$u_agent = $_SERVER['HTTP_USER_AGENT'];
$bname = 'Unknown';
$platform = 'Unknown';
$version= "";
if (preg_match('/linux/i', $u_agent)){
    $platform = 'Linux';
}
elseif (preg_match('/macintosh|mac␣os␣x/i', $u_agent)){
    $platform = 'Mac';
}
elseif (preg_match('/windows|win32/i', $u_agent)){
    $platform = 'Windows';
}
```

Výpis 4.1: PHP kód pre rozpoznanie operačného systému.

Druhou podstatnou časťou tohto kódu je funkcia na rozpoznanie použitého prehliadača, viď výpis 4.2.

```
if(preg_match('/MSIE/i',$u_agent) && !preg_match('/Opera/
   i',$u_agent)){
      $bname = 'Internet␣Explorer';
      $ub = 'MSIE';
}
elseif(preg_match('/Firefox/i',$u_agent)){
      $bname = 'Mozilla␣Firefox';
      $ub = 'Firefox';
}
elseif(preg_match('/Chrome/i',$u_agent)){
      $bname = 'Google␣Chrome';
      $ub = 'Chrome';
}
elseif(preg_match('/Safari/i',$u_agent)){
      $bname = 'Apple␣Safari';
      $ub = 'Safari';
}
elseif(preg_match('/Opera/i',$u_agent)){
      $bname = 'Opera';
      $ub = 'Opera';
```

Výpis 4.2: PHP kód pre rozpoznanie použitého prehliadača.

# 5 NASADENIE APLIKÁCIE A ZBER INFORMÁCIÍ

Vytvorená aplikácia bola nasadená na serveri Planetlabu. Planetlab je globálna výskumná sieť, ktorá podporuje vývoj nových sieťových služieb. Od začiatku roku 2003, viac ako 1000 výskumníkov z tých najlepších akademických inštitúcií používajú Planetlab na vývoj nových technológií pre distribuované úložisko, siete, mapovanie, peer-to-peer systémov, distribuovaných hashovacích tabuliek a spracovanie žiadostí. Planetlab sa momentálne skladá z 1353 uzlov a 717 webstránok.[1]

## 5.1 Nastavenie servera

Ako je spomenuté vyššie, hostingový server pre túto bakalársku prácu bol zvolený server od spoločnosti **planet-lab**, ktorý sa nachádza v Prahe, v Českej republike. Adresa webového servera je `http://planetlab1.cesnet.cz`. Jedná sa o Linuxový server, ktorý beží na distribúcií Fedora 8.6 z roku 2007. Server sa zo začiatku nachádzal v základnej verzií bez balíčkov ako je napríklad webový server. Na obrázku 5.1 je možné vidieť kroky, ktoré sú postupne potrebné na spustenie httpd servera a aplikácie *Tracer*.

[1] https://www.planet-lab.org/

```
 1. sudo yum --nogpgcheck install httpd
 2. sudo yum --nogpgcheck install php
 3. sudo yum --nogpgcheck install nano
 4. sudo nano /etc/httpd/conf/http.d
 [Nastaviť:
                -Listen 8080
                -ServerName 195.113.161.83
                -VirtualHost 8080]
 5. sudo wget https://www.python.org/ftp/python/3.5.2/Python-3.5.2.tgz
 6. tar xzf Python-3.5.2.tgz
 7. sudo yum --nogpgcheck install make
 8. sudo yum --nogpgcheck install gcc
 9. sudo yum --nogpgcheck install openssl-devel -y
10. ./configure
11. make altinstall
12.  sudo yum --nogpgcheck install python-setuptools
[Inštalácia balíčkov pre Python3.5]
14. sudo pip install pyshorteners
15. sudo pip install bs4
16. sudo pip install 'requests[security]'
[Vytvorenie textových dokumentov v zložke /var/www/html]
17. touch iplogger.txt
18. touch data.txt
```

Obr. 5.1: Príkazy potrebné na spustenie httpd servera a aplikácie *Tracer*.

Pre pripojenie sa na server je potrebné sa pripájať priamo na port *8080*, ktorý ako je vidieť bol zadaný do dokumentu *http.d*. Priamy link na stránku je:

`http://planetlab1.cesnet.cz:8080`.

## 5.2 Vytvorený nástroj na zber informácií

Pre tému tejto bakalárskej práce bol vytvorený web na zachytávanie sieťových informácií, ktorý je hostovaný na serveri **planet-lab**. Na serveri sa nachádza aplikácia **Tracer** vytvorená v pythone, ktorá dokáže naklonovať vzhľad akejkoľvek webovej stránky a zobraziť ju na hostovanom serveri. Tento web slúži ako phishingová stránka, ktorá bude odoslaná agresorovi a po následnom navštívení webu sú zachytené informácie o agresorových sieťových prvkoch.

V zdrojovom kóde webovej stránky sa nachádza PHP kód tzv. iplogger, ktorý zachytáva informácie ako dátum a čas navštívenia webu, verejnú IP adresu agresora, použitý prehliadač, operačný systém, rozlíšenie okna prehliadača a šírku pásma agresora. Všetky tieto zachytené informácie sa zapisujú do textového dokumentu s názvom *iplogger*, aby boli neskôr prístupné. Forma, akou sa informácie zapisujú je možné vidieť na obrázku 5.2.

```
D:04-04-2018 09:31:34 IP:185.48.23.x UA:Mozilla Firefox 52-Cookie:1
-LV:Wed Apr 4 2018 09:31:34-OS:Linux-S:781045.153Kb/s-R:1920x1080
D:04-04-2018 09:31:43 IP:185.48.23.x UA:Mozilla Firefox 52-Cookie:2
-LV:Wed Apr 4 2018 09:31:34-OS:Linux-S:555910.859Kb/s-R:1920x1080
D:04-04-2018 10:59:16 IP:185.48.23.x UA:Mozilla Firefox 52-Cookie:3
-LV:Wed Apr 4 2018 09:31:34-OS:Linux-S:508701.563Kb/s-R:1920x1080
D:06-04-2018 11:32:10 IP:78.27.139.x UA:Mozilla Firefox 9-Cookie:1
-LV:Fri Apr 6 2018 11:32:10-OS:Windows-S:778638.016Kb/s-R:Unknown
```

Obr. 5.2: Súbor *iplogger* pre zachytávanie sieťových informácií.

### 5.2.1 Cookies

Cookies tvoria jednu z najdôležitejších častí pri trackovaní agresora. Ako som už opisoval v kapitole 3, pokiaľ sa jedná o globálneho poskytovateľa internetového pripojenia, je veľmi ťažké daného agresora vystopovať. Cookies v tomto prípade slúžia ako dobré vodítko. Keďže sa jedná o kód, ktorý sa vykonáva sa strane klienta, tak každý jeden cookie je unikátny. Po tom ako agresor navštívi webstránku, vytvorí sa mu cookie, ktoré obsahuje čas a dátum kedy danú webstránku navštívil a číslo, ktoré značí počet návštev webstránky. Pomocou týchto dvoch údajov prichádza možnosť priradiť globálnu IP adresu k jednému človeku. To znamená, že aj keby sa pripojili dvaja ľudia z rovnakej globálnej IP adresy, každému sa vytvorí unikátne cookie, na základe ktorého je možná jeho identifikácia.

### 5.2.2 Geolokácia

Na geolokáciu je v tejto práci použitá knižnica jazyka python nazvaná ip2geotools, ktorá podľa zadanej IP adresy vracia údaje ako sú zemepisná šírka a dĺžka. Na internete existuje mnoho geolokačných nástrojov, kde je možné zadať IP adresu a daná aplikácia vráti polohu zadanej IP adresy. V tomto prípade tak isto závisí na tom či sa jedná o verejnú IP adresu, alebo IP adresu poskytovanú providerom. Pokiaľ sa jedná o verejnú IP adresu, tento nástroj je určiť presnú lokáciu s presnosťou na

niekoľko metrov. Pokiaľ sa jedná o adresu danú providerom, IP adresa ukazuje na sídlo providera.

# 6 SPUSTENIE A PREVÁDZKA APLIKÁCIE

Praktické zadanie tejto bakalárskej práce bolo vytvoriť aplikáciu, ktorá dokáže zachytiť verejnú IP adresu agresora. Výstupom tejto práce je aplikácia nazvaná *Tracer*, ktorá je napísaná v programovacom jazyku Python. Ako je už spomínané vyššie v 5.2, program je hostovaný na servery od Planetlabu. Takže prvým krokom k použitiu programu je pripojenie sa na server, kde sa prihlasuje pomocou súkromného kľúča. Následne po prihlásení je potrebné vojsť do zložky xpauco00 (*cd xpauco00*). V danej zložke sa už nachádza samotný program pod názvom tracer.py a spúšťa sa pomocou príkazu *sudo python3 tracer.py*. Po spustení programu sa zobrazí hlavné menu v ktorom je na výber 8 funkcií, viď obrázok 6.1. Funkcie sú zoradené podľa toho ako by ich mal užívateľ postupne spúšťať.

```
###                  Tracer                  ###
###           Created by Daniel Paučo        ###
###       University of Technology Brno      ###
 This product was created for study purposes.

Select from the menu:

 1) Clone website
 2) Generate a php IP-logger
 3) Create a shorten url
 4) Lookup IP address
 5) Run/Stop httpd
 6) Trace route
 7) Monitor mode
 8) Print logs
99) Exit tracer

Tracer>
```

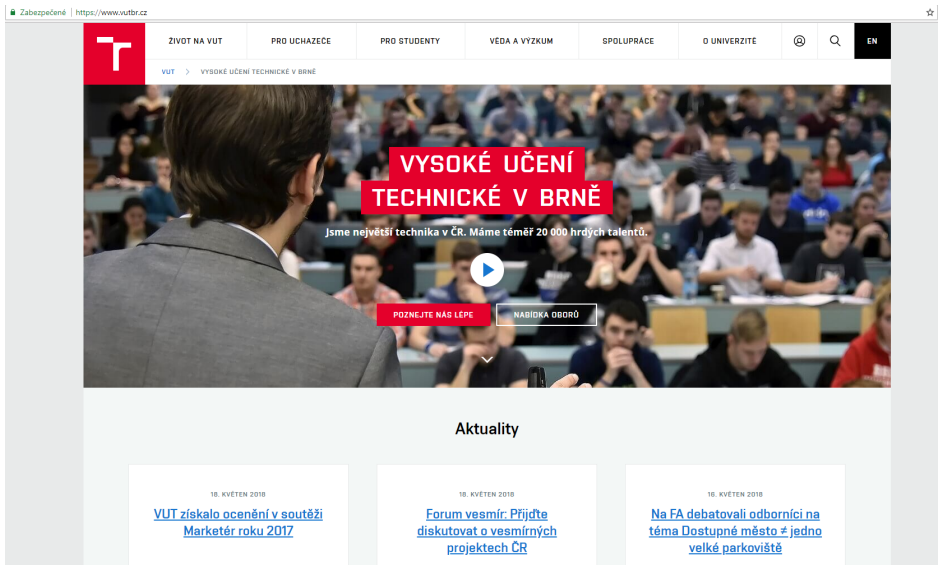
Obr. 6.1: Hlavné menu programu *Tracer*.

***Clone website***

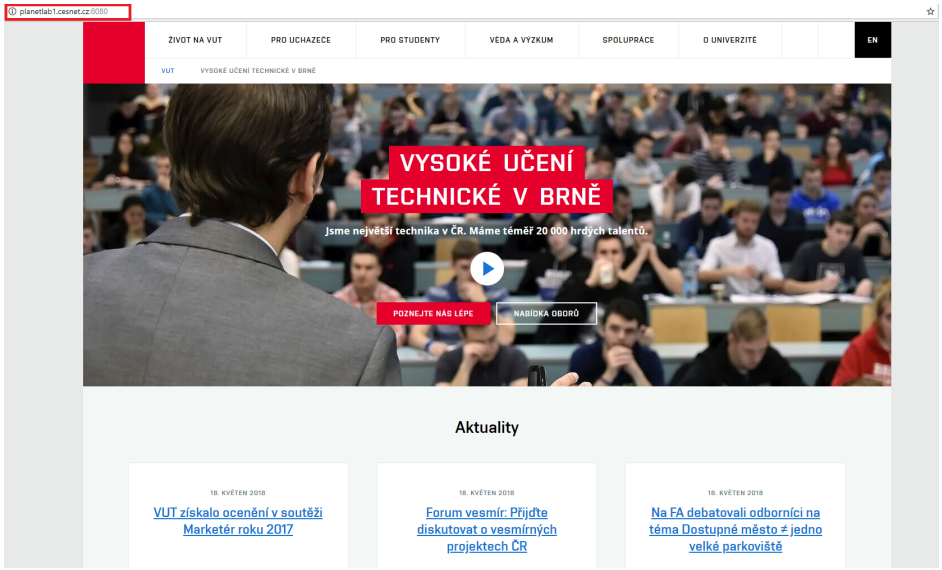
Po výbere tejto funkcie sa zobrazí vstupné pole, do ktorého je potrebné zadať kompletnú URL adresu webstránky, ktorá sa má naklonovať. Najlepší spôsob je URL adresu priamo skopírovať z prehliadača a vložiť ju do aplikácie. Po úspešnom naklonovaní sa stránka uloží do adresára */var/www/html* pod názvom *index.php*. Táto funkcia funguje tak, že aplikácia sa pripojí sa server zadanej webstránky a stiahne si jej aktuálny obsah, ktorý sa neskôr využije ako hlavná stránka pre „phishingový“ web. Túto funkciu nie je nutné využiť, ak má užívateľ dostatočné znalosti, môže si vytvoriť aj vlastnú šablónu stránky. Rozhodol som sa sem pridať túto funkciu z toho dôvodu, že čím dôveryhodnejšie stránka vyzerá, tým je väčšia pravdepodobnosť úspešného phishingu.

```
Tracer>1

To avoid any problems, please copy the exct url from your browser.
Paste the url to clone: https://www.vutbr.cz

The file was saved in /var/www/html/ as index.php
Press enter to continue...
```

Obr. 6.2: Klonovanie webstránky *VUT*.




Originálna stránka www.vutbr.cz




Naklonovaná stránka www.vutbr.cz

Obr. 6.3: Rozdiel medzi originálnou a naklonovanou webstránkou.

***Generate a php IP-Logger***

Po výbere tejto funkcie sa zobrazí sa zobrazí ďalšie menu, kde sú na výber 4 možnosti:

1. `Save IP-logger to the file` – uloží zdrojový kód IP-Loggeru do súboru *iplogger.php*,
2. `Print IP-logger to the screen` – vypíše zdrojový kód IP-Loogeru do terminálového okna ,
3. `Add IP-logger to the file` – pridá zdrojový kód IP-Loggeru na koniec vybraného súboru,
4. `Add IP-logger to the index.php` – pridá zdrojový kód IP-Loggeru na koniec súboru *index.php*.

Závisí čisto na voľbe užívateľa aplikácie, ktorú možnosť si zvolí podľa potreby. Ak si užívateľ v predchádzajucom kroku 6.2 naklonoval stránku, najlepšou voľbou je zvoliť možnosť číslo 4. IP logger je napísaný v skriptovacom jazyku PHP, v ktorom sa nachádzajú aj prvky Javascriptu. Kedže PHP kód sa vykonáva na strane servera, tento kód slúži na zachytávanie informácií ako čas návštevy stránky, IP adresa, user agent (prehliadač), operačný systém a šírka pásma. Javascriptový kód sa naopak vykonáva na strane klienta a tak v tejto funkcií slúži na vytváranie cookies a zisťovanie rozlíšenia okna prehliadača.

```
Tracer>2

1) Save IP-logger to the file
2) Print IP-logger to the screen
3) Add IP-logger to the file
4) Add IP-logger to the index.php

Tracer>1

The file was saved as iplogger.php
Press enter to continue...
```

Obr. 6.4: Uloženie IP-loggeru do súboru.

***Create shorten url***

Po výbere tejto funkcie sa zobrazí vstupné pole, do ktorého je potrebné zadať kompletnú URL adresu webstránky, z ktorej chceme vytvoriť skrátenú, maskovanú adresu pre web, na ktorom je vložený IP logger. Po správnom zadaní adresy, sa v terminálovom okne zobrazí skrátený link na danú webstránku. Táto funkcia je sem

zaradená z jednoduchého dôvodu. Keďže je server hostovaný na adrese http://planetlab1.cesnet.cz:8080, kde je zadaný aj konkrétny port na ktorom server beží je dosť nepravdepodobné, že by niekto klikol na takýto podozrivý link. Skrátené linky sú v dnešnej dobe často používané a tak je vyššia pravdepodobnosť že agresor klikne na takýto link.

```
Tracer>1

Paste the URL of your website to generate a new shorten link.
To avoid any problems, please copy the exct url from your browser.
Paste the url to clone: http://planetlab1.cesnet.cz:8080

Your shortened url: http://tinyurl.com/y6w69q8w
Press enter to continue...
```

Obr. 6.5: Vytvorenie skráteného (maskovacieho) linku na web *Planetlabu*.

***Lookup IP address***

Po výbere tejto funkcie sú na výber dve možnosti. Jedna možnosť je jednoduchý tracing, kde sa zobrazí vstupné pole, do ktorého je potrebné zadať IP adresu, o ktorej sa majú zistiť informácie ako:

- IP adresa,
- Štát,
- Kraj,
- Mesto,
- Zemepisná šírka,
- Zemepisná dĺžka.

```
Tracer>1

Input the IP address you want to trace.
IP: 195.113.2x3.1x
IP traced:
IP:         195.113.2x3.1x
Country:    CZ
Region:     South Moravian
City:       Brno
Latitude:   49.2
Longitude:  16.6333

Press enter to continue...
```

Obr. 6.6: Výstup funkcie *Trace the IP address*.

Druhá možnosť je komplexný sken z WHOIS databázy viď výpis 6.13. Táto funkcia funguje rovnako ako prehliadačová verzia kam sa zadá IP adresa a z databázy sú vypísané všetky informácie o danej adrese. Aby týchto informácií nebolo enormné množstvo a ostali tam len hodnotné informácie, funkcia parsuje iba určité informácie ako sú IP adresy, fyzické adresy a kontakty na vlastníka, administrátora a technickú podporu pod ktorých zadaná IP adresa patrí.

***Run/Stop httpd server***

Po výbere tejto funkcie sa zobrazí v prvom riadku stav *httpd* servera a pod ním sa nachádza menu, v ktorom sú na výber možnosti:

1. `Start httpd` – Spustí httpd server,
2. `Stop httpd` – Zastaví httpd server,
3. `Restart httpd` – Reštartuje httpd server.

```
Tracer>5

Httpd is now   [STOPPED]

1) Start httpd
2) Stop httpd
3) Restart httpd

99) Back to main menu
```

Obr. 6.7: Spustenie httpd servera.

***Trace route***

Po výbere tejto funkcie sa zobrazí vstupné pole, do ktorého je potrebné zadať IP adresu agresora, ktorú cheme vystopovať. V tejto funkcií je použí linuxový príkaz *traceroute*. Ako výstup tejto funkcie sa v terminálovom okne zobrazia všetky „*hopy*“ k danej IP adrese.

```
Tracer>6

Input the IP address you want to trace.
IP: 8.8.8.8
Tracing route to google-public-dns-a.google.com [8.8.8.8]
over a maximum of 30 hops:

1     1 ms     1 ms    <1 ms  192.168.0.1
2     *        *        *     Request timed out.
3    24 ms    24 ms    13 ms  ip-86-49-1-113.net.upcbroadband.cz [86.49.1.113]
4    15 ms    16 ms    13 ms  cz-prg01a-ra4-vla2109.net.upc.cz [84.116.221.37]
5    15 ms    17 ms    12 ms  cz-prg02b-ri1-ae2-0.aorta.net [84.116.136.185]
6    12 ms    13 ms    12 ms  213.46.180.74
7    16 ms    15 ms    13 ms  108.170.245.33
8    12 ms    13 ms    14 ms  216.239.62.183
9    13 ms    11 ms    15 ms  google-public-dns-a.google.com [8.8.8.8]

Press enter to continue...
```

Obr. 6.8: Trace adresy DNS servera googlu.

***Monitor mode***

Táto funkcia funguje v realtime móde. Akonáhle niekto pristúpi na webstránku, všetky nižšie uvedené informácie o danom užívateľovi sa zobrazia v monitorovacom móde viď obr.6.9. Funkcia monitor využíva knižnicu jazyka Python nazvanú ip2geotools, ktorá využíva voľne dostupné api a vracia informácie o IP adrese v json formáte. Ďalšie informácie, ktoré začínajú operačným systémom sú brané zo súboru iplogger.txt odkiaľ sú vyparsované. Najväčšou výhodou tohoto realtime módu je to, že užívateľ môže hneď vidieť koľkokrát už daný človek stránku navštívil a kedy tomu tak bolo naposledy na základe informácií ktorá je uložená v cookies.

```
Tracer>7

Monitor mode:
IP:          185.48.23.x
Country:     Czechia
Region:      Praha
City:        Prague
Latitude:    50.0848
Longitude:   14.4112
OS:          Linux
Browser:     Mozilla Firefox 52
Resolution:  1920x1080
Speed:       7277344 Kb/s
Visits:      14
Last visit:  Tue Apr 10 2018 08:40:34
IP:          78.45.144.x
Country:     Czechia
Region:      Brno
City:        Brno
Latitude:    49.206
Longitude:   16.604
OS:          Windows
Browser:     Google Chrome 65
Resolution:  Unknown
Speed:       5436589 Kb/s
Visits:      1
Last visit:  Tue Apr 10 2018 08:40:39

Press enter to exit monitor mode!
```

Obr. 6.9: Monitorovací mód realtime.

***Print logs***

Funkcia Print logs slúži na vypísanie histórie celého logu návštev webstránky. Všetky zachytené informácie o užívateľovi sa ukladajú na serveri do textového dokumentu, ktorý sa po zavolaní tejto funkcie rozparsuje pomocou regulárnych výrazov na dátum, IP adresu, prehliadač, operačný systém, rozlíšenie, šírka pásma a cookies.

```
Tracer>8
Date:                IP :          Browser:             OS:      Resolution:  Broadband:       Nr. of visits & last visit:
04-04-2018 09:31:31  185.48.23.x   Mozilla Firefox 52   Linux    Unknown      626728.046Kb/s   1        Wed Apr  4  2018 09:31:31
04-04-2018 09:31:34  185.48.23.x   Mozilla Firefox 52   Linux    1920x1080    781045.153Kb/s   1        Wed Apr  4  2018 09:31:34
04-04-2018 09:31:43  185.48.23.x   Mozilla Firefox 52   Linux    1920x1080    555910.859Kb/s   2        Wed Apr  4  2018 09:31:34
04-04-2018 10:59:16  185.48.23.x   Mozilla Firefox 52   Linux    1920x1080    508701.563Kb/s   3        Wed Apr  4  2018 09:31:43
06-04-2018 11:32:10  78.27.139.x   Mozilla Firefox 9    Windows  Unknown      778638.016Kb/s   1        Fri Apr  6  2018 11:31:10
09-04-2018 17:22:24  195.113.243.x Google Chrome 65     Linux    1920x1080    231067.706Kb/s   1        Mon Apr  9  2018 17:22:24
11-04-2018 08:08:37  185.48.23.x   Mozilla Firefox 52   Windows  1920x983     479831.002Kb/s   4        Wed Apr  4  2018 10:59:16
15-05-2018 08:02:14  185.48.23.x   Mozilla Firefox 52   Windows  1904x967     117029.816Kb/s   5        Tue Apr 11  2018 08:08:37


Press enter to continue...
```

Obr. 6.10: Výpis zalogovaných návštev webstránky.

# Príklady využitia aplikácie

V tejto sekcií sú popísané príklady použitia nástroja *Tracer*. Na obrázku 6.11 je zachytený výpis jednoduchého vyhľadávania informácií o verejnej IP adrese globálneho ISP. Práve na tomto príklade je možné vidieť, že ak má užívateľ zaplatenú verejnú IP adresu, lokalizácia daného užívateľa je v celku jednoduchá viď geolokačné údaje vo výpise na obrázku 6.11. Po zadaní týchto geolokačných údajov do *Google maps* je možné dostať presnú polohu IP adresy viď obrázok 6.12.

```
IP traced: 195.113.243.xx
IP:          195.113.243.xx
Country:     CZ
Region:      South Moravian
City:        Brno
Latitude:    49.2
Longitude:   16.6333

Press enter to continue...
```

Obr. 6.11: Výstup funkcie Lookup IP address -> Simple lookup.


Obr. 6.12: Vyhľadanie adresy pomocou *Google maps*.

V druhom príklade, na obrázku 6.13, sa taktiež jedná o globálneho poskytovateľa s tým rozdielom, že užívateľ nemá zaplatenú verejnú IP adresu. Tu je možné vidieť, že adresa ukazuje na ISP do Prahy. Pre porovnanie som vyhľadal rovnakú IP adresu

cez možnosť jednoduchého vyhľadávania a vo výsledku je vidieť, že api použité vo funkcií jednoduchého vyhľadávania využíva inú databázu a ukazuje na úplne inú lokáciu viď obrázok 6.14.

```
Whois lookup: 78.45.173.xx
Owner:
inetum:          78.45.0.0 - 78.45.173.255
netname:         UPC-BROADBAND-XXXIII
descr:           UPC Broadband Internet Services
country:         CZ
admin-c:         MK23104-RIPE
tech-c:          MK23104-RIPE

Admin:
role:            Mistral Contact Role
address:         UPC Ceska Republika, s.r.o
address:         Zavisova 502/5
address:         Prague Nusle
address:         The Czech Republic

Tech:
person:          Martin Kraxxx
address:         UPC Ceska Republika, s.r.o.
address:         Zavisova 502/5
address:         Prague 4 - Nusle
address:         140 00
address:         Czech Republic
phone:           +420 2 611071xx

Press enter to continue...
```

Obr. 6.13: Výstup funkcie Lookup IP address -> Whois lookup.

```
IP traced: 78.45.173.xx
IP:          78.45.173.xx
Country:     CZ
Region:      Jihocesky kraj
City:        Strakonice
Latitude:    49.3
Longitude:   14.0167

Press enter to continue...
```

Obr. 6.14: Výstup funkcie Lookup IP address -> Simple lookup.

# 7 ZÁVER

V danej bakalárskej práci s tematikou identifikácie agresora kyberšikany, boli rozobrané a popísané témy ako čo je to kyberšikana, aké sú jej druhy, akými médiami sa najčastejšie šíri, ako prebieha identifikácia agresora podľa českej právnej legislatívy, a na záver popis programu, slúžiaceho pre zachytávanie komunikačných údajov agresora.

Hlavným cieľom tejto práce bolo získanie verejenej IP adresy agresora, čo sa aj podarilo vďaka vytvorenému webovému serveru, ktorý vo svojom zdrojovom kóde obsahoval tzv. IP logger, ktorý je schopný zachytiť komunikačné údaje agresora, jeho verejná IP adresa, použitý webový prehliadač, operačný systém, rozlíšenie obrazovky a časová známka.

Pri stopovaní agresora som narazil na niekoľko problémov z ktorých najväčší bol IP adresa od globálneho poskytovateľa. Tento problém som z časti vyriešil pomocou cookies, ktoré sú jedinečné a zanechajú na počítači agresora stopu ktorá dokáže identifikovať že daný počítač bol v určitom čase na stránke planetlabu.

# LITERATÚRA


[1] Anderson, C. A., Bushman, B. J. (2002). Human aggression. *Annual Review of Psychology*, 53, s. 27–28.

[2] Boulton, M.J, Underwood, K. (1992). Bully/victim problems among middleschoolchildren. *British Journal of Educational Psychology*, 62, s. 73–87.

[3] ČERNÁ, A. a kol. Kyberšikana: Průvodce novým fenoménem. Grada, 2013. 152 s. ISBN: 978-80-247-4577-0.

[4] Frissen, A., Jonsson, A., Persson, C. (2007). Adolescent's perception of bullying: Who is the victim? Who is the bully? What can be done to stop bullying? *Adolescence*, 42, s. 749–761.

[5] Hinduja, S., Patchin, J. (2009). *Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying.* Thousand Oaks: Corwin Press.

[6] Kowalski, R. M., Limber, S. P., Agatston, P. W. (2008). *Cyber Bullying: Bullying in the Digital Age*. Malden: Blackwell.

[7] POLČÁK, Radim, František PÚRY a Jakub HARAŠTA. Elektronické důkazy v trestním řízení. Brno: Masarykova univerzita, 2015. ISBN 978-80-210-8073-7.

[8] Urban, J., (2012). *Co dělat, když – Intervence pedagoga: Rizikové chování ve školním prostředí – rámocvý koncept, příloha č. 7 – kyberšikana* [online]. [cit. 2017-11-23]. Dostupné z: http://www.msmt.cz/file/19629?highlightWords=kyber%C5%A1ikana

[9] Willard, N., (2007). The authority and responsibility of school officials in responding to cyberbullying. *Journal of Adolescent Health*, 41, s. 64–65.

[10] Wilton, C., Campbell, M.A. (2011). An exploration of the reasons why adolescents engage in traditional and cyberbullying. *Journal of Educational Sciences & Psychology*, 1, s. 101–109.