Možnosti Open Source Intelligence v současném Internetu

Bc. Michal Kopřiva

Diplomová práce
2022

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav informatiky a umělé inteligence

Akademický rok: 2021/2022

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Michal Kopřiva**
Osobní číslo:	**A20697**
Studijní program:	**N0613A140022 Informační technologie**
Specializace:	**Kybernetická bezpečnost**
Forma studia:	**Kombinovaná**
Téma práce:	**Možnosti Open Source Intelligence v současném Internetu**
Téma práce anglicky:	**Possibilities of Open Source Intelligence in Today's Internet**

Zásady pro vypracování

1. Specifikujte jaké druhy zdrojů spadají do kategorie Open Source Inteligence.
2. Zmapujte a popište metody a nástroje OSINT v současné síti Internet.
3. Popište omezení využití nástrojů vzhledem k nařízením GDPR.
4. Vypracujte metodiku analýzy pomocí OSINT.
5. Ověřte navrženou metodiku na testovacím případu.

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. CHAUHAN, Sudhanshu a Nutan PANDA, 2015. Hacking Web Intelligence. Waltham (Massachusetts): Syngress. ISBN 9780128018675.
2. HASSAN, Nihad A. a Rami HIJAZI, 2018. Open Source Intelligence Methods and Tools. 1. Berkeley, CA: Apress. ISBN 978-1-4842-3212-5.
3. APPEL, Edward J., 2014. Cybervetting: Internet Searches for Vetting, Investigations, and Open-Source Intelligence, Second Edition [online]. 2nd. Boca Raton: CRC Press [cit. 2021-11-26]. ISBN 9780429256387. Dostupné z: [https://doi.org/10.1201/b17651](https://doi.org/10.1201/b17651 „https://doi.org/10.1201/b17651")
4. GIBSON, Helen, Steve RAMWELL a Tony DAY, 2016. Analysis, Interpretation and Validation of Open Source Data. AKHGAR, Babak, P. Saskia BAYERL a Fraser SAMPSON, ed. Open Source Intelligence Investigation [online]. 1. Cham (Switzerland): Springer, s. 95-110 [cit. 2021-11-26]. ISBN 9783319476711. Dostupné z: [https://link.springer.com/content/pdf/10.1007%2F978-3-319-47671-1_6.pdf](https://link.springer.com/content/pdf/10.1007%2F978-3-319-47671-1_6.pdf „https://link.springer.com/content/pdf/10.1007%2f978-3-319-47671-1_6.pdf")
5. GIBSON, Helen, 2016. Acquisition and Preparation of Data for OSINT Investigations. AKHGAR, Babak, P. Saskia BAYERL a Fraser SAMPSON, ed. Open Source Intelligence Investigation [online]. 1. Cham (Switzerland): Springer, s. 69-93 [cit. 2021-11-26]. ISBN 9783319476711. Dostupné z: [https://link.springer.com/content/pdf/10.1007%2F978-3-319-47671-1_6.pdf](https://link.springer.com/content/pdf/10.1007%2F978-3-319-47671-1_6.pdf „https://link.springer.com/content/pdf/10.1007%2f978-3-319-47671-1_6.pdf")
6. NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679, 2016. In: Úřední věstník Evropské unie. Brusel, ročník 2016, číslo 679. Dostupné také z: [https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016R0679&from=CS](https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016R0679&from=CS „https://eur-lex.europa.eu/legal-content/cs/txt/pdf/?uri=celex:32016r0679&from=cs")

Vedoucí diplomové práce: **Ing. David Malaník, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **3. prosince 2021**
Termín odevzdání diplomové práce: **23. května 2022**

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

doc. Mgr. Milan Adámek, Ph.D. v.r.
děkan

prof. Mgr. Roman Jašek, Ph.D., DBA v.r.
ředitel ústavu

Ve Zlíně dne 24. ledna 2022

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 15. 5. 2022 Michal Kopřiva, v. r.

ABSTRAKT

Tato diplomová práce se zabývá možnostmi open source intelligence v současném Internetu. Jsou zde specifikovány zdroje OSINT a popsány nástroje pro jejich využití. Dále je diskutováno omezení využití těchto nástrojů vzhledem k nařízení GDPR. V praktické části diplomové práce byla vypracována metodika analýzy pomocí OSINT a v závěru této práce byla navržená metodika ověřena na testovacích případech.

Klíčová slova: OSINT, Internet, GDPR, informace

ABSTRACT

This thesis deals with the possibilities of open source intelligence in today's Internet. OSINT sources are specified and tools for their use are described. Furthermore, the limitations of the use of these tools in view of the GDPR regulation are discussed. In the practical part of the thesis, a methodology for analysis using OSINT was developed and at the end of this thesis the proposed methodology was validated on test cases.

Keywords: OSINT, Internet, GDPR, information

Rád bych poděkoval panu doktoru Davidu Malaníkovi za odborné vedení a připomínky při vypracování této diplomové práce. Dále bych chtěl poděkovat manželce Zuzaně za trpělivost a podporu během mého studia.

Prohlašuji, že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD **10**
I TEORETICKÁ ČÁST **11**
1 ZPRAVODAJSTVÍ Z OTEVŘENÝCH ZDROJŮ **12**
1.1 HISTORIE OSINT 12
2 METODY A NÁSTROJE OSINT V SOUČASNÉ SÍTI INTERNET **14**
2.1 VYHLEDÁVAČE 14
2.1.1 Google 14
2.1.2 Carrot² 15
2.2 METADATA 16
2.2.1 FOCA 17
2.2.2 ExifTool 17
2.3 VIN 18
2.3.1 VINDecoderZ 18
2.3.2 VinCheck 18
2.4 VYHLEDÁVÁNÍ ZDROJOVÉHO KÓDU 19
2.4.1 NerdyData 19
2.4.2 Searchcode 20
2.4.3 SymbolHound 20
2.5 OBRÁZKY 21
2.5.1 TinEye 21
2.5.2 Current Location 21
2.6 SOCIÁLNÍ SÍTĚ 22
2.6.1 Facebook 22
2.6.1.1 StalkFace 24
2.6.2 Twitter 25
2.6.3 All My Tweets 25
2.6.4 TweetBeaver 26
2.7 E-MAILY 27
2.7.1 Trumail 27
2.7.2 EmailRep 28
2.7.3 MsgEml 29
2.7.4 Mailheader 29
2.7.5 E-Mail Header Analyzer 30
2.7.6 Mail Header Analyzer 30
2.8 UŽIVATELSKÁ JMÉNA 30
2.8.1 KnowEm 30
2.8.2 Instant Username Search 31
2.8.3 WhatsMyName 32
2.9 DOMÉNOVÁ JMÉNA A IP ADRESY 32
2.9.1 ICANN registration data lookup 32
2.9.2 ViewDNS Reverse IP 33
2.9.3 ViewDNS Reverse Whois Lookup 34
2.9.4 ViewDNS IP History 34

2.9.5 WHOIS History Lookup 34
2.9.6 SecurityTrails 35
2.9.7 IP Location Finder 36
2.9.8 IP Lookup Tool 36
2.9.9 Netcraft Site Report 37
2.9.10 DNSDumpster 38
2.10 Úniky dat 38
2.10.1 HIBPW 38
2.10.2 PSBDMP 38
2.11 Wayback Machine 40
2.12 Bitcoin Abuse Database 40
2.13 Certificate Search 41
2.14 Komplexní nástroje 41
2.14.1 AbuseIPDB 41
2.14.2 Alien Labs Open Threat Exchange (OTX) 42
2.14.3 Threat Crowd 44
2.14.4 VirusTotal 44
2.14.5 Shodan 45
2.14.6 IntelOwl 46
3 OSINT A GDPR 48
II PRAKTICKÁ ČÁST 51
4 METODIKA OSINT ANALÝZY 52
4.1 Zdroje dat pro analýzu 52
4.1.1 E-mailové zprávy 52
4.1.2 Datové soubory 53
4.1.3 Multimediální soubory 54
4.1.4 Ostatní zdroje 54
4.2 Nástroje analýzy 54
4.2.1 E-mailová adresa 55
4.2.2 Uživatelské jméno 55
4.2.3 Doménové jméno 56
4.2.4 IP adresa 57
4.2.5 Adresa kryptoměnové peněženky 57
4.2.6 Identifikační číslo certifikátu 57
4.2.7 Obrázek 58
5 TESTOVÁNÍ METODIKY 59
5.1 E-mailová zpráva 59
5.2 Rozbor e-mailové adresy 60
5.3 Rozbor doménového jména 60
5.4 Rozbor IP adresy 62
5.5 Rozbor uživatelského jména 63
5.6 Rozbor kryptoměnové peněženky 63
5.7 Rozbor certifikátu 64
5.8 Rozbor obrázku 65
ZÁVĚR 67

SEZNAM POUŽITÉ LITERATURY **68**
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK **74**
SEZNAM OBRÁZKŮ **76**
SEZNAM TABULEK **78**
SEZNAM PŘÍLOH **79**

ÚVOD

V současné době je existence Internetu a jeho používání vnímáno jako naprosto běžná součást lidského života. Tato síť je používána z pracovních důvodů, pro komunikaci, zábavu a nakupování nebo třeba interakci mezi uživateli. Významnou roli hraje Internet při vzdělávání. Velké skupině lidí se zpřístupnilo obrovské množství informací, které jsou velmi rychle všem dostupné. Vládní úřady a firmy poskytují své služby online a zvyšují tak jejich dostupnost stále většímu počtu uživatelů. Používáním Internetu ovšem také velké množství informací vzniká a zaznamenává se, a to si většina jeho uživatelů vůbec neuvědomuje. Většina služeb vyžaduje registraci uživatelských jmen, e-mailů, osobních údajů. Na sociálních sítí uživatelé ochotně sdílejí množství citlivých informací, údaje o své geografické poloze, majetkové poměry a rodinné vztahy. Dokumenty a multimediální soubory nahrávané do Internetu obsahují informace ve formě metadat. Webové servery ukládají informace z klientských prohlížečů. Zasílané e-mailové zprávy uchovávají informace o poštovních serverech. Poskytovatelé internetového připojení zveřejňují informace o zeměpisných údajích IP (Internet Protocol) adres, registrátoři domén shromažďují kontaktní údaje zákazníků. Díky tomu se Internet stal významným zdrojem informací, které neustále velkým tempem přibývají. Většina uživatelů si také není vědoma skutečnosti, že data z veřejných zdrojů jsou přístupná pro všechny ostatní.

Pro potřeby vyšetřování bezpečnostních incidentů v kybernetice, jsou tyto informace vyhledávány, shromažďovány a vyhodnocovány. Na základě takto získaných údajů lze provádět atribuci, což je proces, který se snaží odpovědět na otázky, kdo stál za nežádoucí aktivitou, jakým způsobem došlo k průniku do systému a jaký byl útočníkův záměr.

Cílem této diplomové práce je identifikovat informace, které lze získat z otevřených zdrojů, kde takové informace získat a jaké nástroje k tomu použít.

Vzhledem k tomu, že zdrojů potřebných informací, které je třeba vyšetřit, bývá velké množství, je nutné postupovat metodicky. K tomu by měl sloužit pracovní postup, uvedený v praktické části této práce.

I. TEORETICKÁ ČÁST

1 ZPRAVODAJSTVÍ Z OTEVŘENÝCH ZDROJŮ

Open Source Intelligence (OSINT), tedy zpravodajství z otevřených zdrojů, je metoda získávání informací z veřejně dostupných kanálů. Tyto informační kanály jsou buď přístupné volně, bez omezení nebo je přístup k nim zpoplatněn a mohou nabývat mnoha forem. Jedná se například o denní tisk, časopisy, knihy, televizní a rozhlasové vysílání, zprávy tiskových agentur, komerční databáze, nosiče audio a video záznamů, výzkumné zprávy, kresby, mapové podklady, sociální média, šedá literatura, deep a dark web a Internet obecně. Tento druh zdrojů má výhodu v okamžité dostupnosti, ale zároveň je nutné takto získané informace ověřovat, obzvláště v případech, kdy se vyskytují pochybnosti o důvěryhodnosti určitého zdroje. Při ověřování otevřeného zdroje by se měla posuzovat autentičnost zdroje, přesnost v porovnání s jinými zdroji, objektivita zdroje, platnost zdroje a dosah zdroje. Poté lze získané zpravodajské informace považovat za vysoce spolehlivé [1, 2, 3].

Mezi takto získané informace patří údaje o osobách, jako jméno, datum narození, bydliště, e-mailové adresy, uživatelská jména, hesla, dosažené vzdělání, zaměstnání, rodinné a sociální vazby mezi uživateli (Významným zdrojem těchto informací jsou sociální sítě. Pro tento druh zpravodajství se používá výraz SOCMINT, tedy Social Media Intelligence), fotografie, vlastnictví kryptoměnových peněženek, IP adresy a jejich poloha, domény, služby využívané uživatelem, geografická poloha uživatelů, informace o softwarovém vybavení počítačů používaných při prohlížení Internetu [2].

1.1 Historie OSINT

První významný moment systematického shromažďování informací z otevřených zdrojů nastává v 15. století, kdy Benátská republika a republika Ragusa ve snaze o kontrolu Středozemního moře významně přispěly k rozvoji zpravodajství. Obě republiky disponovaly strukturovanými zpravodajskými sítěmi, které si systematicky předávaly informace. V souvislosti s výskytem většího množství tištěných médií a jejich šíření je zaznamenána snaha o systematický sběr těchto informací. Benátští agenti shromažďovali informace o peněžních tocích, trzích a obchodu v Evropě, které byly využívány ve státním zájmu. Dalším mezníkem ve vývoji OSINT je okamžik, kdy strukturovaná zpravodajská síť ovlivnila a ovládla tištěná média. V roce 1865 byla za vlády Otty von Bismarcka, jako pruského premiéra, vytvořena tajná organizace, čítající více než 45 000 agentů, kterou koordinoval Wilhelm Stieber. Tato síť získávala domácí i zahraniční informace a často prováděla mise proti diplomatickým cílům. Prováděla například psychologickou válku s cílem zlepšit morálku vlastní armády a oslabit

morálku nepřítele tím, že zveřejňovala falešné zprávy o neúspěších a ztrátách nepřítele a zdůrazňovala vlastní úspěchy. Wilhelm Stieber byl prvním šéfem národní zpravodajské služby, která využívala agenty ke sledování a kontrole tisku. Od tohoto okamžiku musely zpravodajské služby informace získané z tisku ověřovat. Třetím významným momentem je okamžik, kdy se zpravodajské služby transformovaly do státních institucí a rozšířily se. Kvůli společenskému napětí, které vzniklo v důsledku akcí prováděných tajnými službami, se zpravodajské služby staly veřejnou posedlostí a vlády, živené těmito obavami, začaly zakládat první národní organizace. V roce 1909 tak vzniká ve Velké Británii Úřad tajných služeb, z kterého později vzniká kontrarozvědka MI5 a rozvědka MI6, pro zahraniční operace. Rozmach těchto zpravodajských služeb nepřímo vedl k rozvoji OSINT. Čtvrtým mezníkem byl vznik rozhlasu a televize. Během obou světových válek nabylo zpravodajství podstatně většího významu. V USA byl založen Úřad strategických služeb (OSS), předchůdce CIA. Své tajné služby rozvíjel také Sovětský Svaz. V tomto kontextu neustále se rozšiřujících zpravodajských služeb se ukázala potřeba rozvoje OSINT. Vzhledem k tomu, že studená válka byla válkou zpravodajskou, bylo třeba získat přístup ke všem typům zdrojů a používat všechny známé metody sběru informací, přičemž OSINT hrál stále důležitější roli, a to i vzhledem k tomu, že toto období se shodovalo s rozvojem rozhlasového a televizního vysílání. Zatímco dříve se zpravodajské služby zaměřovaly na sběr, uchovávání a zpřístupňování písemných informací, nyní se začaly zabývat převodem hlasu na text, aby mohly zpracovávat informace šířené prostřednictvím rozhlasu. V této době se také objevila potřeba zachycovat, ukládat a zpřístupňovat video informace. Pátým mezníkem pro OSINT je masové využívání Internetu. Nárůst dat na Internetu po roce 2000 a rozvoj sociálních sítích, umožněný mimo jiné díky rozvoji mobilních komunikacích, poskytl nové kategorie údajů a metadat. Tato data jsou dostupná kdykoliv a komukoliv [4].

2 METODY A NÁSTROJE OSINT V SOUČASNÉ SÍTI INTERNET

2.1 Vyhledávače

Webový vyhledávač je softwarová aplikace, která prochází Internet, indexuje jeho obsah a následně uživateli poskytuje informace na základě jeho vyhledávacího dotazu.

2.1.1 Google

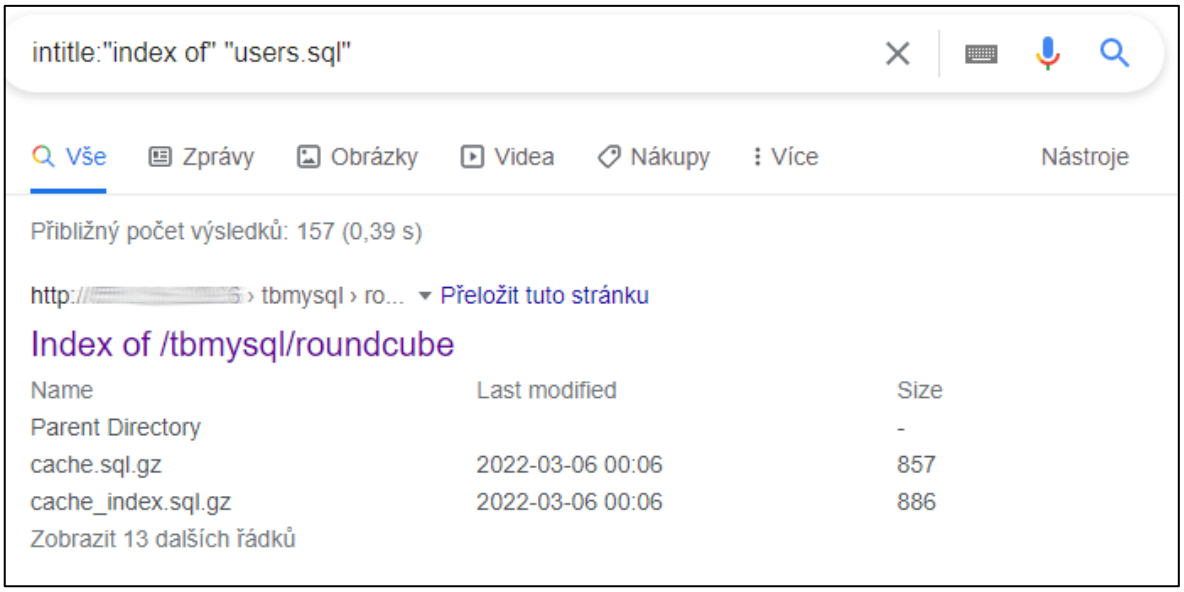
Google je stejnojmenný vyhledávač společnosti Google, patřící do holdingu firmy Alphabet. Mimo běžného vyhledávání lze využít tzv. Google hacking. Tato metoda, někdy označovaná jako Google dorking, je sběr informací, který využívá pokročilé techniky vyhledávání v Googlu. Kombinováním vhodných logických a pokročilých operátorů ve vyhledávacím řetězci lze dotazování zaměřit na specifický cíl. V tabulce č. 1 je uvedeno několik těchto pokročilých operátorů s popisem jejich funkce [5, 6].

Tabulka 1. Operátory vyhledávání Google hacking

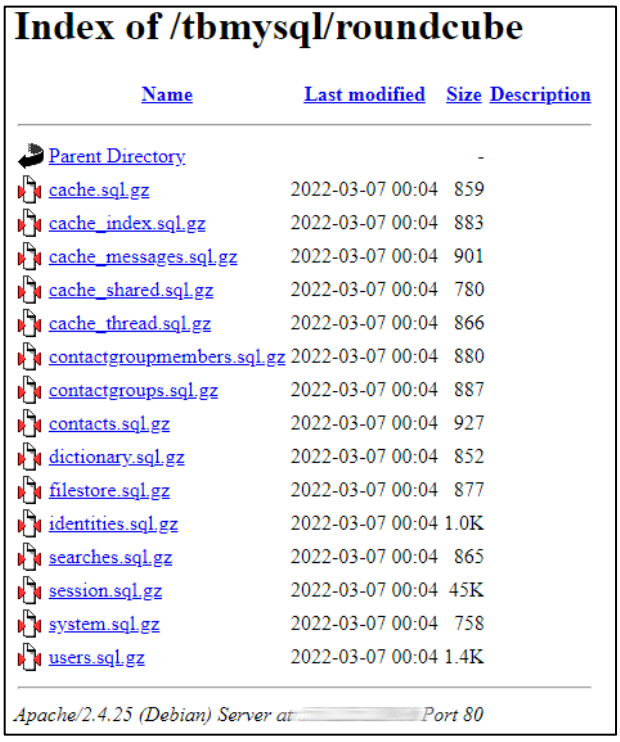
site:	Omezení vyhledávacího dotazu na konkrétní doménu nebo webovou stránku.
filetype:	Vyhledávání textu v určitém typu souboru.
link:	Vyhledání stránek s požadovanou URL (Uniform Resource Locator) adresou.
cache:	Vyhledá kešovanou verzi požadovaných webových stránek.
intitle:	Vyhledání řetězce v názvu stránky.
inurl:	Hledání řetězce v URL adrese.
allintext:	Vyhledá stránky obsahující zadané výrazy v textu stránky.

Existuje také databáze těchto vyhledávacích dotazů, s názvem Google Hacking Database, roztříděných do různých kategorií (jsou to např. chybové zprávy, soubory obsahující zajímavé informace, soubory obsahující hesla, stránky obsahující přihlašovací portál a další) [7].

Obrázky č. 1 a 2 ukazují výsledek dotazu „intitle:"index of" "users.sql"“, který vyhledává soubory „users.sql“ na stránkách, v jejichž názvu se vyskytuje fráze „index of“.



Obrázek 1. Výsledek vyhledávání intitle:"index of" "users.sql"

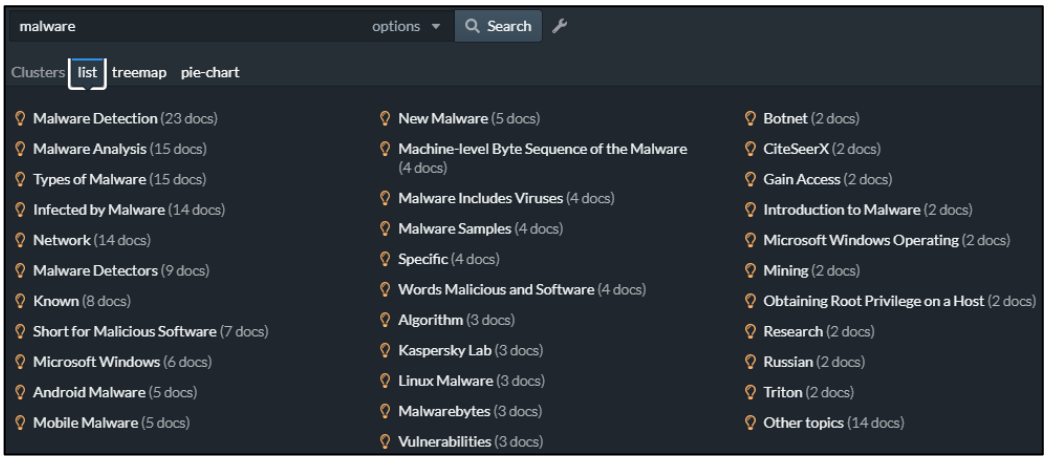


Obrázek 2. Obsah stránky nalezený pomocí Google hacking

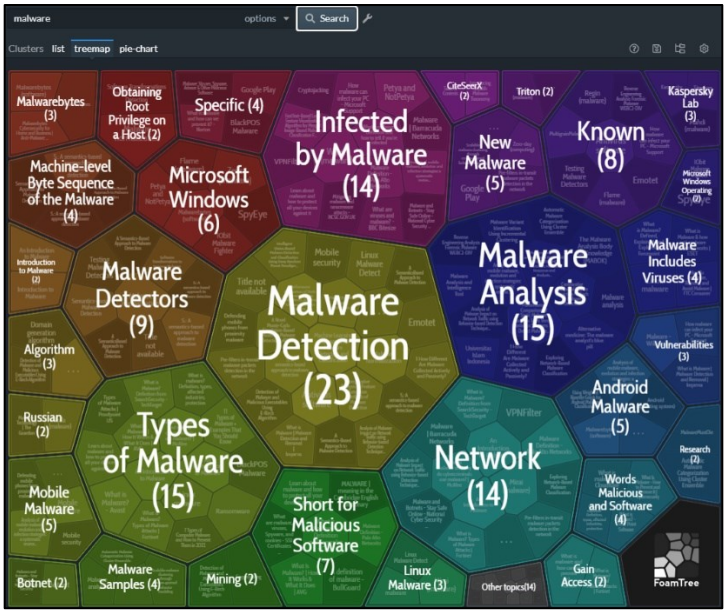
2.1.2 Carrot²

Carrot² je vyhledávací engine, který dokáže shlukovat nalezené výsledky do tematických kategorií a tyto skupiny opatřit klíčovými frázemi. Pro vyhledávání na webu používá vyhledávací engine eTools a pro seskupování výsledků využívá algoritmy Lingo, Suffix Tree

Clustering (SFC) a K-means. Obrázky č. 3 a 4 ukazují výsledky vyhledávání výrazu „malware“, roztřídění do kategorií a grafické znázornění shluků [8].



Obrázek 3. Kategorie výsledků vyhledávání



Obrázek 4. Grafické znázornění shluků vyhledávače Carrot2

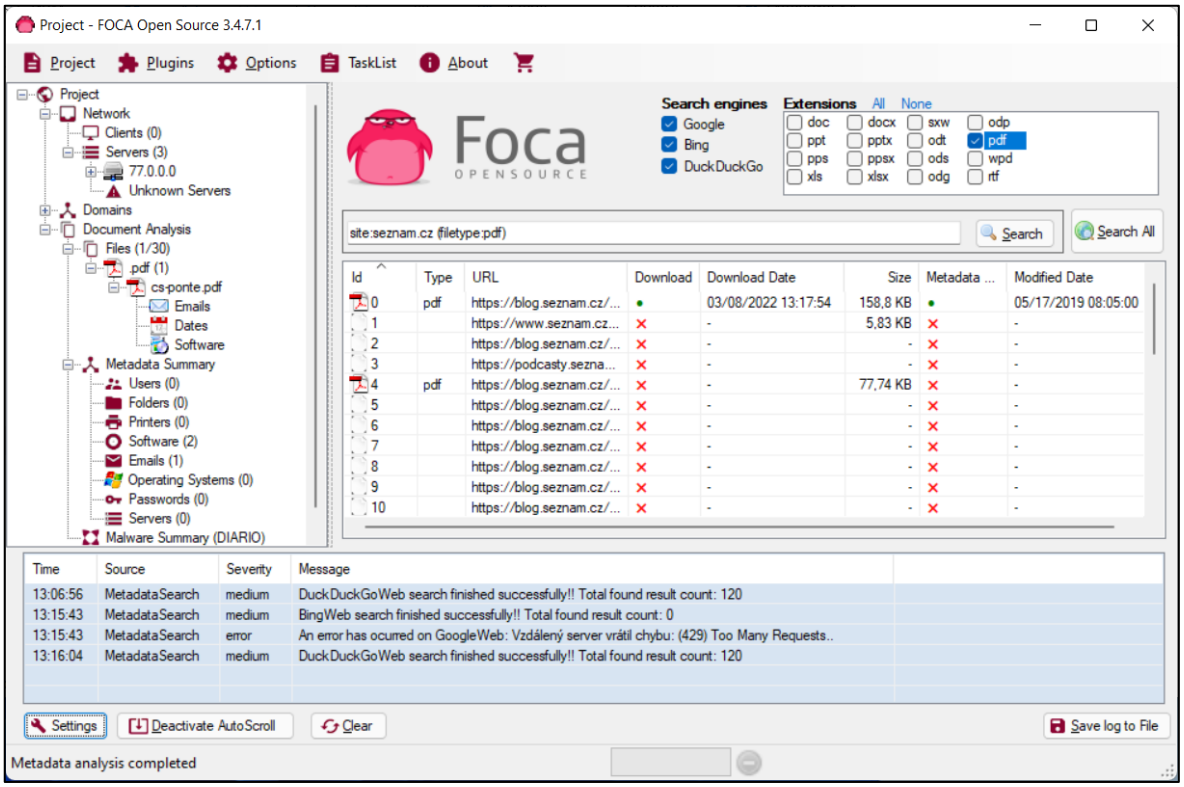
2.2 Metadata

Metadata jsou dat o datech, tedy informace, které nějakým způsobem popisují obsah, ale nejsou součástí obsahu. U video souboru to může být údaj o délce videa nebo u souboru s fotografií se může jednat o datum pořízení, zeměpisné údaje o poloze zařízení nebo parametrech fotoaparátu. Textové dokumenty obsahují údaje o autorovy, datum vytvoření, datum poslední úpravy, údaje o použitém softwaru, statistické údaje o obsahu a mnohé další. Všechna tato data mohou být cenným zdrojem informací. U jednotlivých souborů lze

metadata zobrazit pomocí vlastností souboru nebo lze s výhodou využít specializovaných aplikací k tomu určených [5].

2.2.1 FOCA

FOCA (Fingerprinting Organizations with Collected Archives) je nástroj sloužící k vyhledávání metadat a skrytých informací v dokumentech. Pomocí tohoto nástroje lze stahovat a analyzovat dokumenty umístěné na webových stránkách a je také možné analyzovat soubory uložené na lokálním počítači. Tyto dokumenty jsou vyhledávány pomocí vyhledávačů Google, Bing a DuckDuckGo. Obrázek č. 5 ukazuje vyhledávání souborů s příponou PDF v doméně seznam.cz [9].



Obrázek 5. Výsledek vyhledávání aplikace FOCA

2.2.2 ExifTool

ExifTool je multiplatformní konzolová aplikace pro čtení, zápis a úpravu metadat v nejrůznějších typech datových souborů. Zobrazuje mnoho typů metadat, jako např. EXIF (Exchangeable Image File Format), GPS (Global Positioning System), IPTC (International Press Telecommunications Council), XMP (Extensible Metadata Platform), JFIF (JPEG File Interchange Format) a GeoTIFF. Výstupem tohoto programu může být např. CSV soubor obsahující získaná metadata, jak je vidět na obrázku č. 6 [10].

SourceFile	AppVersic	CreateDat	ExifToolV	FileAcces	FileCreate	FileDescri	FileFlags	FileModif	FileName	FileOS	FilePermi	FileSize
prednaska-3.pptx	16.0000	2014:08:1	12.40	2022:03:0	2022:03:08	13:45:33+01:00		2022:02:1	prednaska-AK9FA-3.		-rw-rw-rw	78 MiB

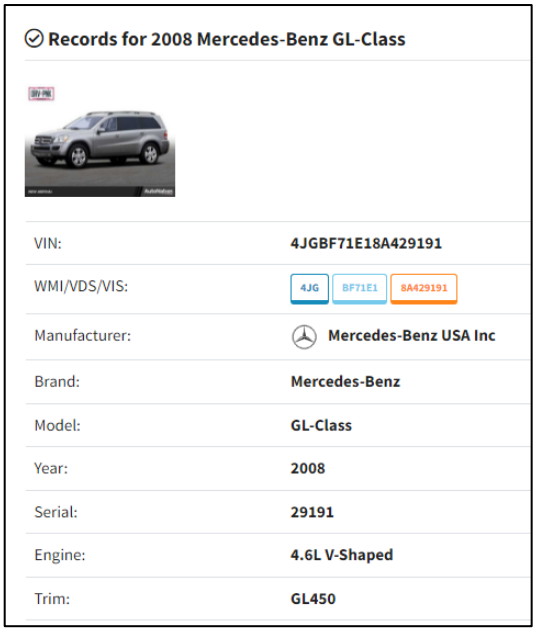
Obrázek 6. Metadata získaná aplikací ExifTool

2.3 VIN

VIN (Vehicle Identification Number) je kód složený ze 17 znaků, který jednoznačně identifikuje každé vozidlo. Tento kód obsahuje informace o zemi původu a výrobci, popis a výrobní číslo konkrétního modelu vozidla. Dvě níže uvedené aplikace dokázaly zobrazit informace o vozidle z generátoru náhodných VIN čísel, ale také data o reálném vozidle registrovaném v Česku.

2.3.1 VINDecoderZ

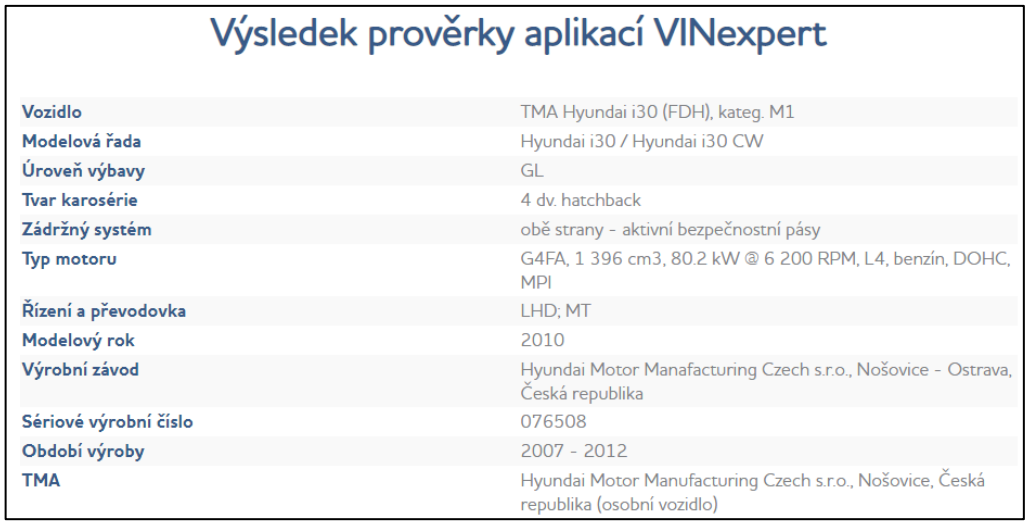
Aplikace zobrazí data o vozidle, jako je výrobce, značka, model, druh motoru, rok výroby a sériové číslo. Obrázek č. 7 ukazuje údaje o vozidle na základě náhodně generovaného VIN kódu. U reálného vozidla registrovaného v Česku nebyly údaje o modelu a roku výroby dostatečně konkrétní [11].



Obrázek 7. Údaje o vozidle z aplikace VINDecoderZ

2.3.2 VinCheck

Stejně jako předchozí aplikace, zobrazí data o vozidle, jako je výrobce, značka, model, druh motoru, rok výroby a sériové číslo. V případě aplikace VinCheck jsou však data u reálného vozidla registrováno v Česku detailnější a přesnější, jak je vidět na obrázku č. 8 [12].



Výsledek prověrky aplikací VINexpert

Vozidlo	TMA Hyundai i30 (FDH), kateg. M1
Modelová řada	Hyundai i30 / Hyundai i30 CW
Úroveň výbavy	GL
Tvar karosérie	4 dv. hatchback
Zádržný systém	obě strany - aktivní bezpečnostní pásy
Typ motoru	G4FA, 1 396 cm3, 80.2 kW @ 6 200 RPM, L4, benzín, DOHC, MPI
Řízení a převodovka	LHD; MT
Modelový rok	2010
Výrobní závod	Hyundai Motor Manafacturing Czech s.r.o., Nošovice - Ostrava, Česká republika
Sériové výrobní číslo	076508
Období výroby	2007 - 2012
TMA	Hyundai Motor Manufacturing Czech s.r.o., Nošovice, Česká republika (osobní vozidlo)

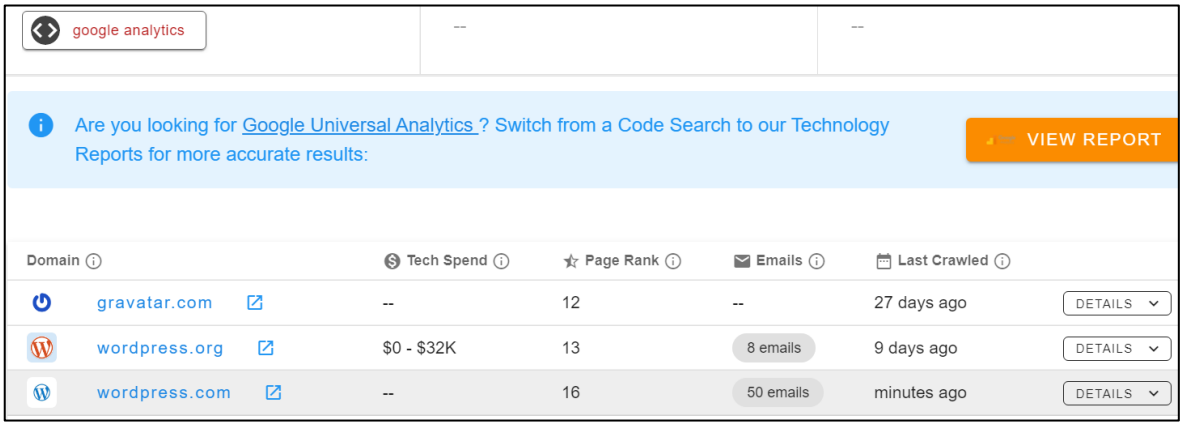
Obrázek 8. Data z aplikace VinCheck

2.4 Vyhledávání zdrojového kódu

Pomocí těchto nástrojů je možné vyhledávat na základě části zdrojových kódů nebo použitých technologií [5, 13].

2.4.1 NerdyData

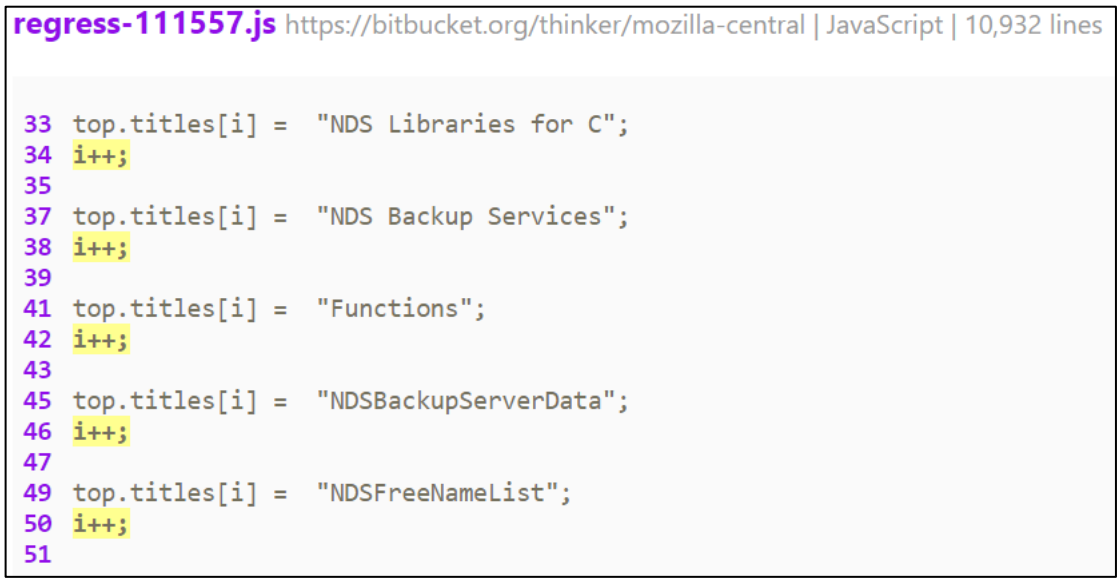
NerdyData prochází a indexuje miliony webových stránek a umožňuje jejich prohledávání. Pomocí této aplikace lze vyhledat konkrétní část kódu a zjistit, které webové stránky ji používají. Na obrázku č. 9 jsou zobrazeny výsledky vyhledávání webových stránek používajících službu Google [14].



Obrázek 9. Výsledky aplikace NerdyData

2.4.2 Searchcode

Aplikace vyhledává zdrojové kódy v depozitářích jako je GitHub, Bitbucket, GitLab nebo třeba Sourceforge. Výsledky je možné dále filtrovat podle použitých programovacích jazyků. Obrázek č. 10 ukazuje výsledek vyhledávání řetězce „i++;“ aplikací Searchcode [15].



Obrázek 10. Výsledek hledání řetězce „i++;“ aplikací Searchcode

2.4.3 SymbolHound

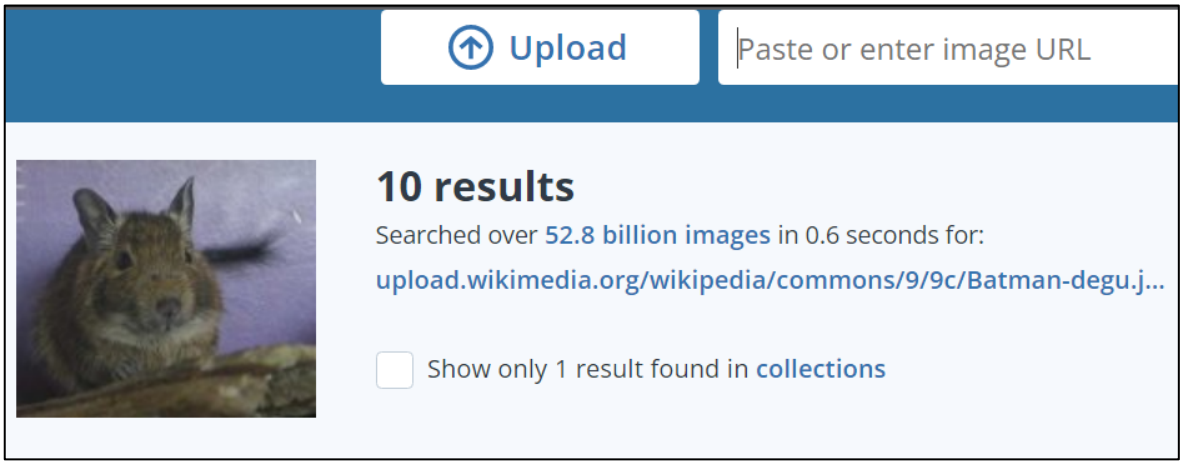
Aplikace určená pro prohledávání webových stránek, která umožňuje vyhledávat také speciální znaky, jako např. &, % nebo #. Obrázek č. 11 ukazuje výsledek vyhledávání řetězce „i++;“ [16].

Obrázek 11. Výsledek hledání řetězce „i++;“ aplikací SymbolHound

2.5 Obrázky

2.5.1 TinEye

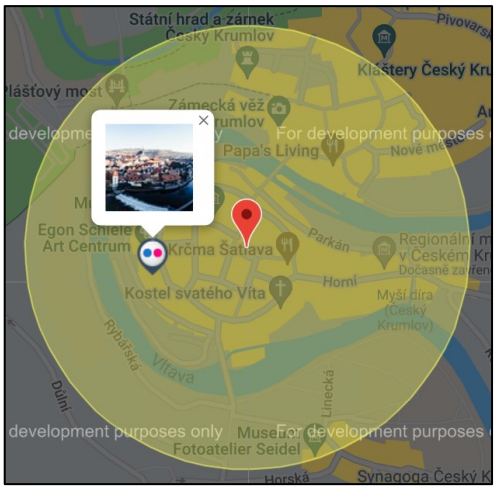
TinEye je reverzní vyhledávač obrázků na Internetu. Po nahrání obrázku je možné zjistit odkud pochází, jak je používán, zda existují jeho upravené verze nebo najít stejný obrázek ve vyšším rozlišení. Nástroj nevyužívá klíčová slova nebo metadata, ale technologii rozpoznávání obrázků. Umožňuje vyhledávat i obrázky oříznuté, upravené nebo s pozměněnou velikostí. Obrázek č. 12 ukazuje výsledek vyhledávání [17].



Obrázek 12. Vyhledávání obrázku nástrojem TinEye

2.5.2 Current Location

Webová aplikace, která umožňuje prohlížet obrázky obsahující údaje o poloze, sdílené pomocí Instagramu, Flickru a služby 500px na základě vybrané polohy na mapě. Na obrázku č. 13 je zobrazen výsledek vyhledávání v aplikaci Current Location [18].



Obrázek 13. Vyhledávání v aplikaci Current Location

2.6 Sociální sítě

Veřejné profily na sociálních sítí jsou bohatým zdrojem dat, která sdílejí jejich uživatelé. Jedná se o osobní a kontaktní údaje uživatelů, údaje o vzdělání a zaměstnání, propojení na rodinné příslušníky a partnery, sdílení vazeb na ostatní uživatele, fotografie a často jsou to i data o geografické poloze. Například největší sociální síť, Facebook, použilo v lednu 2022 přibližně 2,9 miliard aktivních uživatelů. Síť Twitter měla ve stejné době přibližně 440 milionů uživatelů. Z toho lze usoudit, že sociální sítě jsou vhodným potencionálním zdrojem informací. Získávání informací ze sociálních sítí se nazývá SOCMINT (Social Media Intelligence) [19].

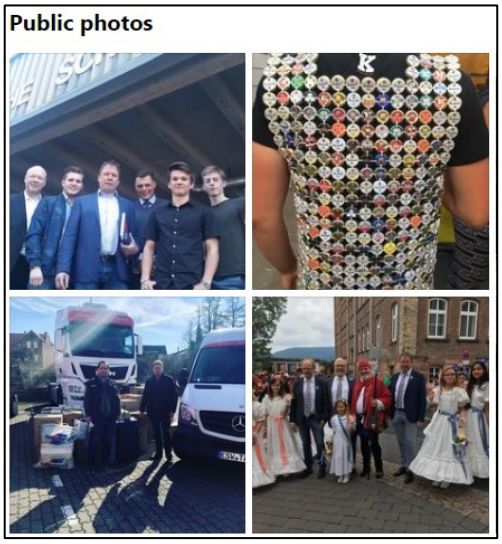
2.6.1 Facebook

Vyhledání objektu zájmu se provádí na stránce aplikace. Vyhledávání údajů je možné pouze po přihlášení do aplikace. Po nalezení konkrétního uživatele je výhodné zjistit jeho identifikační číslo, které je jedinečné a umožní detailnější vyhledávání. Toto číslo lze zjistit ve zdrojovém kódy webové stránky s profilem uživatele Facebook, kde se vyskytuje řetězec ve tvaru "userID":"číslo". Vyhledávání se pak provádí pomocí URL adresy, která obsahuje doménu, instrukci pro vyhledávání, požadovaná data a filtr s identifikačním číslem uživatele. Část adresy s filtrem je kódována kódem Base64. {"rp_author":"{\"name\":\"author\",\"args\":\"[USERID]\"} "}. Po nahrazení slova [USERID] číslem 100024536552581 a kódováním Base64 obdržíme řetězec
eyJycF9hdXRob3IiOiJ7XCJuYW1lXCI6XCJhdXRob3JcIixcImFyZ3NcIjpcIjEwMDAyNDUzNjU1MjU4MVwifSJ9
Nyní lze sestavovat URL adresu pro vyhledávání následujících informací.

Obrázek č. 14 ukazuje výsledek vyhledávání příspěvků uživatele „Knut John“ pomocí adresy https://facebook.com/search/posts/?q=post&epa=FILTERS&filters=
eyJycF9hdXRob3IiOiJ7XCJuYW1lXCI6XCJhdXRob3JcIixcImFyZ3NcIjpcIjEwMDAyNDUzNjU1MjU4MVwifSJ9

Obrázek 14. Příspěvky uživatele

Vyhledávání fotografií uživatele „Knut John“ pomocí adresy https://facebook.com/search/photos/?q=photos&epa=FILTERS&filters=eyJycF9hdXRob3IiOiJ7XCJuYW1lXCI6XCJhdXRob3JcIixcImFyZ3NcIjpcIjEwMDAyNDUzNjU1MjU4MVwifSJ9. Výsledek je znázorněn na obrázku č. 15.



Obrázek 15. Fotografie uživatele

Vyhledávání videí uživatele „Knut John“ pomocí adresy https://facebook.com/search/videos/?q=videos&epa=FILTERS&filters=eyJycF9hdXRob3IiOiJ7XCJuYW1lXCI6XCJhdXRob3JcIixcImFyZ3NcIjpcIjEwMDAyNDUzNjU1MjU4MVwifSJ9. V tomto případě vyhledávání nebylo úspěšné.

Doplněním klíčového slova lze vyhledávání více upřesnit.

Vyhledávání příspěvků uživatele „Knut John“ s klíčovým slovem „hilfe“ pomocí adresy https://facebook.com/search/posts/?q=HILFE&epa=FILTERS&filters=eyJycF9hdXRob3IiOiJ7XCJuYW1lXCI6XCJhdXRob3JcIixcImFyZ3NcIjpcIjEwMDAyNDUzNjU1MjU4MVwifSJ9. Výsledek vyhledávání je zobrazen na obrázku č. 16.

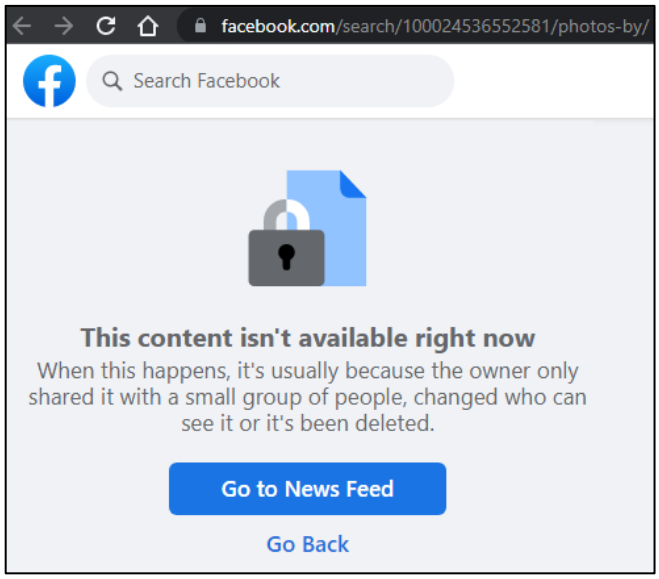
Obrázek 16. Příspěvek uživatele vyhledaný na základě klíčového slova

Vyhledání fotografií uživatele „Knut John“ s klíčovým slovem „hilfe“ pomocí adresy https://facebook.com/search/photos/?q=HILFE&epa=FILTERS&filters=eyJycF9hdXRob3IiOiJ7XCJuYW1lXCI6XCJhdXRob3JcIixcImFyZ3NcIjpcIjEwMDAyNDUzNjU1MjU4MVwifSJ9. Ukázka tohoto vyhledávání je zobrazena na obrázku č. 17 [20].

Obrázek 17. Fotografie uživatele vyhledané na základě klíčového slova

2.6.1.1 StalkFace

Pokročilé vyhledávání umožňovala aplikace StalkFace, ale to v současné době (březen 2022) není funkční, protože využívá vyhledávací metody, které Facebook od června 2019 přestal podporovat. Po zadání URL adresy Facebook profilu tak sice vrátí ID uživatele, ale použití dalších funkcionalit aplikace končí chybou, jak je vidět na obrázku č. 18 [21].



Obrázek 18. Chyba vyhledávání v aplikaci StalkFace

2.6.2 Twitter

Vedle běžného vyhledávání v aplikaci, nabízí Twitter také vyhledávání pokročilé. Díky této funkcionalitě lze hledání více upřesnit. Je možné například vyhledat přesnou frázi nebo konkrétní hashtagy, alespoň jedno ze zadaných slov, vynechat z hledání určené výrazy. Další kritérium pro hledání může být uživatelský účet, hledání příspěvků podle počtu odpovědí, lajků nebo retweetů a v neposlední řadě lze také výsledek hledání omezit určitým časovým úsekem.

2.6.3 All My Tweets

Tato aplikace přehledně zobrazuje všechny příspěvky uživatele na Twitteru a řadí je od nejnovějšího po starší. Dále je možné zobrazit příspěvky, které uživatel označil „lajkem“ a také uživatele sledované a sledující. Obrázek č. 19 ukazuje výsledek vyhledávání Tweetů uživatele @stevewoz [22].

Obrázek 19. Výsledek hledání v aplikaci All My Tweets

2.6.4 TweetBeaver

Aplikace pro získávání informací z Twitterových účtů, vyhledávání vztahů mezi účty a stahování dat z Twitteru. Stránka obsahuje 17 funkčních nástrojů (duben 2022).

- Převod uživatelského jména na ID
- Převod ID na uživatelské jméno
- Ověření, zda se dva účty vzájemně sledují
- Zobrazení a stažení oblíbených příspěvků uživatele
- Vyhledávání klíčových slov v oblíbených příspěvcích uživatele
- Vyhledávání klíčových slov v příspěvcích uživatele
- Zobrazení údajů z účtu uživatele
- Hromadné vyhledávání nad uživatelským účtem
- Hromadné zobrazení údajů z více účtu najednou
- Zobrazení a stažení seznamu „přátel" daného uživatele
- Zobrazení a stažení seznamu „sledujících" daného uživatele
- Vyhledávání společných „sledujících“ dvou různých účtů
- Vyhledávání společných „přátel“ dvou různých účtů
- Zobrazení konverzace mezi dvěma účty
- Zobrazení seznamů „sledujících“ a „přátel“ daného účtu

- Vyhledávání účtů sledovaných jedním uživatelem, které sledují i jiného zadaného uživatele
- Vyhledávání prvních 25 „sledujících“ daného uživatele (funkční pro uživatele s maximálně 75000 „sledujících“)
- Vyhledávání prvních 25 „přátel“ daného uživatele (funkční pro uživatele s maximálně 75000 „přátel“)

Na obrázku č. 20 jsou zobrazeny údaje účtu uživatele @stevewoz, získané pomocí aplikace TweetBeaver [24].

Screen name	Twitter ID	Name	Biography	Account created date	
@stevewoz	22938914	Steve Wozniak	Engineers first! Human rights. Gadgets. Jokes and pranks. Segways. Music and concerts. Gameboy Tetris.	Thu Mar 05 16:24:20 +0000 2009	
Location	**URL**	**Time zone**	**Geo enabled**	**Language**	
Los Gatos, California	http://woz.org	not set	1	not set	
Verified	**Tweets**	**Followers**	**Friends**	**Protected**	**Profile image URL**
verified	7577	645358	95	not protected	https://pbs.twimg.com/profile_images/1365311061/Janet_and_Woz_normal.jpg

Obrázek 20. Výsledek hledání údajů k účtu v aplikaci TweetBeaver

2.7 E-maily

2.7.1 Trumail

Trumail je služba poskytující ověřování platnosti e-mailových adres a pracuje za použití API aplikace Emailchecker. Dotazy lze zadávat přes webovou aplikaci nebo pomocí API, kdy je možné zdarma zadat 10 dotazů denně. Z vrácených informací lze například zjistit, zda zadaná adresa odpovídá standardu RFC (Request for Comments), zda je případná zpráva doručitelná na tuto adresu, jestli není cílová schránka plná, jestli se nejedná o známou jednorázovou adresu a další. Obrázek č. 21 ukazuje výsledek dotazu na e-mailovou adresu info@sreality.cz [24, 25].

Your lookup results


```
{
    "address": "info@sreality.cz",
    "username": "info",
    "domain": "sreality.cz",
    "md5Hash": "a7ea3b791947678a88f1d938e99fe6a2",
    "suggestion": "",
    "validFormat": true,
    "deliverable": true,
    "fullInbox": false,
    "hostExists": true,
    "catchAll": true,
    "gravatar": false,
    "role": true,
    "disposable": false,
    "free": false
}
```


Obrázek 21. Hledání ve službě Trumail

2.7.2 EmailRep

Tato služba shromažďuje údaje o e-mailových adresách, doménách a internetových uživatelích. EmailRep využívá datové zdroje ze sociálních sítí, úniky dat a přihlašovacích údajů, seznamy spamovacích e-mailů, údaje o doménách a na základě těchto údajů určuje rizikovost e-mailových adres. Aplikace zobrazí například informace o reputaci adresy, zda je adresa považována za podezřelou nebo rizikovou, zda e-mailová adresa vykazuje škodlivé chování, jestli se daná adresa neobjevila v nějakém úniku dat a další. Na obrázku č. 22 jsou údaje o e-mailové adrese info@sreality.cz, které poskytla tato služba [26, 27].


```
curl emailrep.io/info@sreality.cz
{
    "email": "info@sreality.cz",
    "reputation": "high",
    "suspicious": false,
    "references": 4,
    "details": {
        "blacklisted": false,
        "malicious_activity": false,
        "malicious_activity_recent": false,
        "credentials_leaked": true,
        "credentials_leaked_recent": false,
        "data_breach": true,
        "first_seen": "08/28/2017",
        "last_seen": "11/04/2020",
        "domain_exists": true,
        "domain_reputation": "high",
        "new_domain": false,
        "days_since_domain_creation": 7088,
        "suspicious_tld": false,
        "spam": false,
        "free_provider": false,
        "disposable": false,
        "deliverable": true,
        "accept_all": false,
        "valid_mx": true,
        "primary_mx": "firma-smtp1.seznam.cz",
        "spoofable": true,
        "spf_strict": true,
        "dmarc_enforced": false,
        "profiles": []
```


Obrázek 22. Zobrazení informací pomocí služby EmailRep

2.7.3 MsgEml

Pomocí tohoto nástroje lze zobrazovat obsah e-mailové zprávy ve formátu „.msg“ a „.eml“. Je také možné zobrazit samotnou hlavičku a tu poté použít pro další zkoumání pomocí nástrojů, které jsou uvedeny níže [28].

2.7.4 Mailheader

Nástroj pro lepší čitelnost záznamů v hlavičce e-mailové zprávy. Mimo přehledného zobrazení samotných dat, obsažených v hlavičce, přidává také informace o geografickém umístění IP adres, informace o autonomních systémech, ve kterých se nachází mailové servery, přes které zpráva prošla. Na obrázcích č. 23, 24 a 25 je zobrazena část takto získaných informací [29].

Message Transfer Agent (MTA) - Transfer Details

Mail Server From:	mta14-ab1.mtasv.net	**Mail Server To:**	gmmr4.centrum.cz
Mail Server From IP:	50.31.205.14	**Mail Server To IP:**	46.255.227.253
Mail Country From:	United States	**Mail Country To:**	Czechia
AS Name From:	SERVERCENTRAL	**AS Name To:**	Economia a.s.
AS Number From:	AS23352	**AS Number To:**	AS43614
Distance (All Hops/Summary):	16334.92/ KM	**Hops (All/Public):**	5 / 3
MTA Encryption	Poor (*)	**Delivery Time:**	0 days, 0 hours, 0 min, 23 sec
Your IP:	78.80.81.128	**Your GeoLoc:**	Lat:50.0848 Lon:14.4112

Obrázek 23. Informace z hlavičky e-mailu získané v aplikaci Mailheader

Spam Scoring Details

Score	Spam Description
0.0	**ADMINISTRATOR NOTICE: The query to URIBL was**
0.0	**SPF: HELO does not publish an SPF Record**
1.1	**Date: is 3 to 6 hours before Received: date**
0.1	**Message has a DKIM or DK signature, not necessarily**
0.1	**DKIM or DK signature exists, but is not valid**

Total Score (Max:5.0)	Spamassassin prediction
1.3	**No Spam = Good!**

Obrázek 24. Informace z hlavičky e-mailu získané v aplikaci Mailheader

Hop 4/5	Public Mail Routing		
By MTA	bx.virusfree.cz	By IP	185.145.37.162 (*)
By AS Number	AS61317	By AS Name	Ipxo Uk Limited
By Geo	Lat:50.1188 Lon:8.6843	By Next City	(*)
From MTA	mta14-ab1.mtasv.net	From IP	50.31.205.14 (*)
From AS Nbr	AS23352	From AS Name	SERVERCENTRAL
From Geo	Lat:41.8874 Lon:-87.6318	From Next City	(*)
Distance	10705.10 KM	Del.Time (*)	
MTA Encryption	TLSv1.2, ECDHE-RSA-AES256-GCM-SHA384		
RAW	Received: from mta14-ab1.mtasv.net (50.31.205.14) by bx.virusfree.cz with ESMTPS (TLSv1.2, ECDHE-RSA-AES256-GCM-SHA384); 11 Feb 2022 03:24:49 +0100 Received-SPF: pass (bq.virusfree.cz: domain of pm-bounces.mojang.com designates 50.31.205.14 as permitted sender) client-ip=50.31.205.14; envelope-from=pm_bounces@pm-bounces.mojang.com; helo=mta14-ab1.mtasv.net;		

Obrázek 25. Informace z hlavičky e-mailu získané v aplikaci Mailheader

2.7.5 E-Mail Header Analyzer

Další nástroj pro vylepšení čitelnosti hlaviček e-mailových zpráv. Oproti předchozí aplikaci nezobrazuje geografické umístění IP adres na mapových podkladech, ale poskytované informace zobrazuje v přehlednější formě [30].

2.7.6 Mail Header Analyzer

Nástroj pro analýzu hlaviček e-mailů a jejich převod do čitelného formátu, který také umí identifikovat zdroj e-mailové zprávy, zpoždění při přeposílání na serverech a zemi umístění serveru. Tato služba se dá využívat nejen jako online nástroj, ale také je možné ho instalovat a provozovat na vlastním zařízení [31].

2.8 Uživatelská jména

Nástroje pro ověřování uživatelských jmen mohou sloužit pro vyhledávání online služeb, které uživatel využívá. K hledání se využívá konkrétní uživatelské jméno nebo lze také použít část e-mailové adresy před znakem zavináč, protože tento způsob identifikace je mezi internetovými uživateli hojně rozšířen.

2.8.1 KnowEm

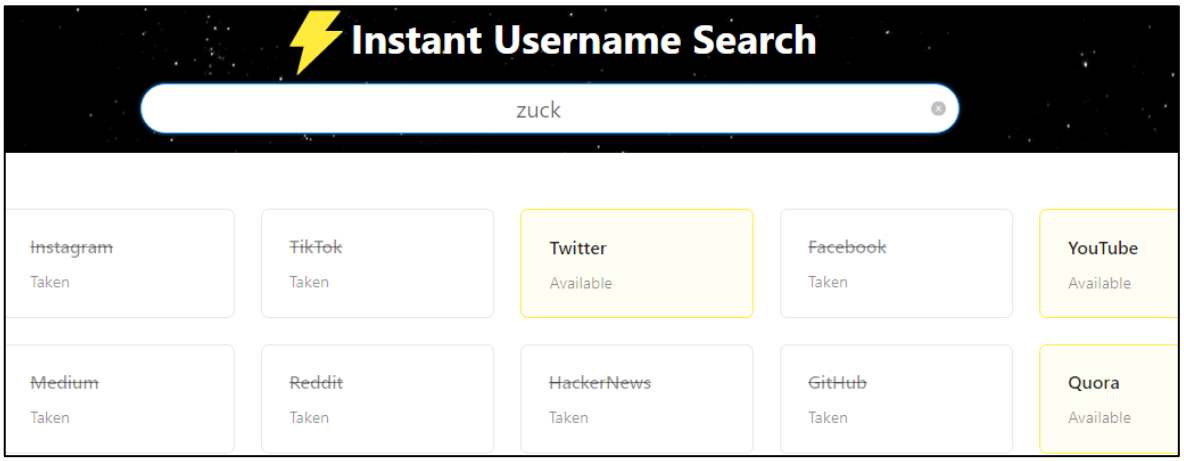
Aplikace určená pro ověření, zda je jméno uživatele nebo název firmy používán v některé ze sociálních sítích. Díky tomu je možné usuzovat, které služby uživatel využívá. Aplikace zobrazí výsledek hledání pro 25 vybraných nejpopulárnějších sítí nebo lze získat informace z téměř 490 různých služeb. Na obrázku č. 26 je ukázán výsledek hledání uživatele „zuck“ získaný z nejpopulárnějších sítí podle aplikace KnowEm. Přeškrtnutý text „available“ vedle

loga sítě značí, že dané uživatelské jméno je již použito. Nevýhodou této aplikace je, že neposkytuje přímé linky na dané uživatelské profily [32].

Obrázek 26. Informace získané z aplikace KnowEm

2.8.2 Instant Username Search

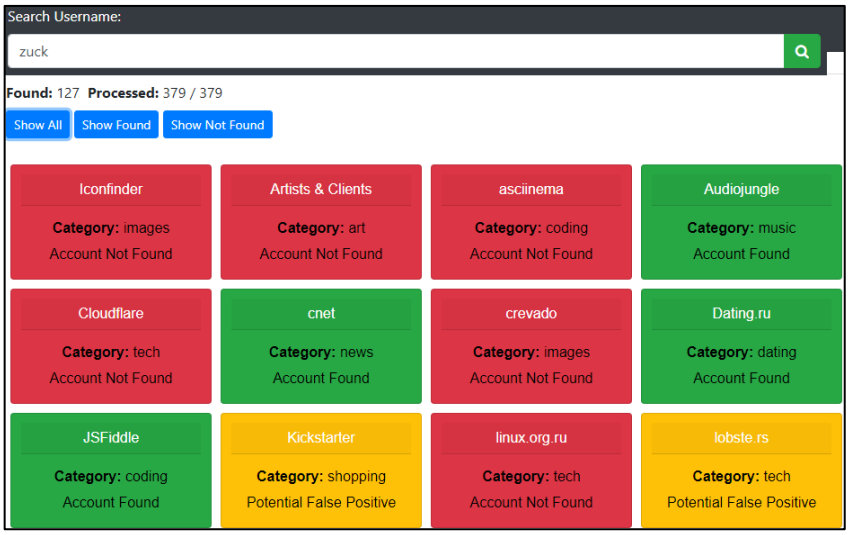
Aplikace pro vyhledávání uživatelského jména na celkem 133 sociálních sítí. Během zadávání jména do vyhledávacího pole se výsledek na obrazovce průběžně aktualizuje. Na jednotlivé profily konkrétních uživatelů dané sociální sítě lze přistupovat přímo, pomocí linků. Obrázek č. 27 ukazuje výsledek hledání uživatele „zuck“. Výraz „Taken“ značí, že v dané sociální síti je toto uživatelské jméno již použito [33].



Obrázek 27. Výsledek hledání v aplikaci Instant Username Search

2.8.3 WhatsMyName

Nástroj pro vyhledávání uživatelů v téměř 400 webových aplikací a sociálních sítí. Nalezené výsledky lze mimo prohlížení přímo v aplikaci také uložit jako soubor, ve formátech XLSX, CSV nebo PDF. Na obrázku č. 28 je zobrazen výsledek vyhledávání uživatele „zuck“. Je zde vidět i označení pro možné falešně pozitivní výsledky [34].



Obrázek 28. Výsledek hledání v aplikace WhatMyName

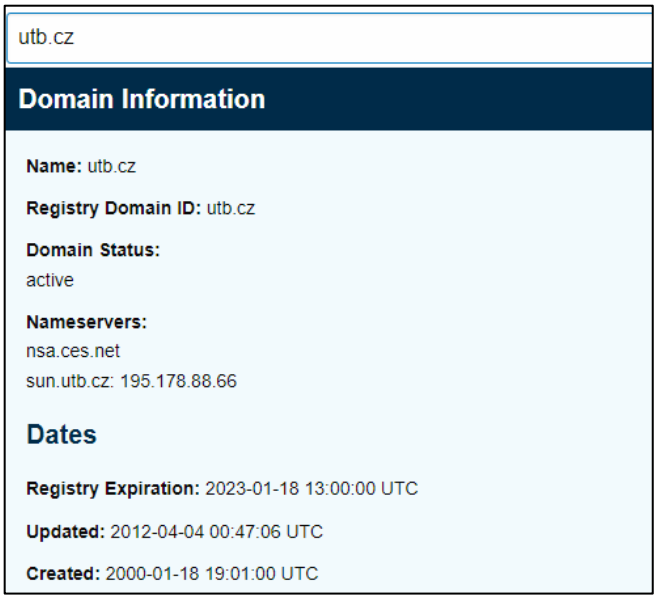
2.9 Doménová jména a IP adresy

Při registraci webové stránky jsou vyžadovány informace o registrovaném subjektu, technický a administrativní kontakt spojený s doménou. Kontaktní informace mohou obsahovat celé jméno, název subjektu, fyzickou adresu, telefonní číslo a e-mailovou adresu. Tyto údaje poskytuje registrující subjekt registrátorovi, u kterého byla doména zakoupena. Cestou centrálního registru jsou poté tyto údaje poskytovány organizaci ICANN (Internet Corporation for Assigned Names and Numbers). Odtud jsou tyto informace veřejně dostupné a poskytuje je mnoho online aplikací. Jsou to takzvané „WHOIS“ databáze. Největší problém s těmito daty je kontrola osobních údajů. V mnoha případech se však využívá skrytá registrace pomocí dalších firem nebo poskytovatelů webhostingu a skutečný majitel domény tak bývá skryt [20].

2.9.1 ICANN registration data lookup

Nástroj pro vyhledávání registračních údajů, který využívá protokol RDAP (Registration Data Access Protocol), který byl vytvořen jako alternativa protokolu WHOIS na portu 43. Podle typu vstupních dat jsou vráceny nejrůznější registrační údaje, jako například název

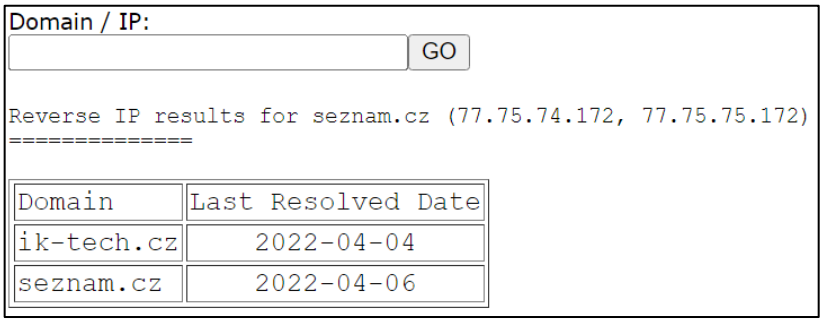
domény, DNS (Domain Name Server), datum registrace domény a její platnost pro doménové jméno, adresný rozsah, název adresného rozsahu, kód země registrace a kontakty na registrující subjekt pro IP adresu a identifikační údaje a kontakty v případě autonomního systému. Obrázek č. 29 ukazuje část výsledku dotazu na doménu „utb.cz“ [35, 36].



Obrázek 29. ICANN registration data

2.9.2 ViewDNS Reverse IP

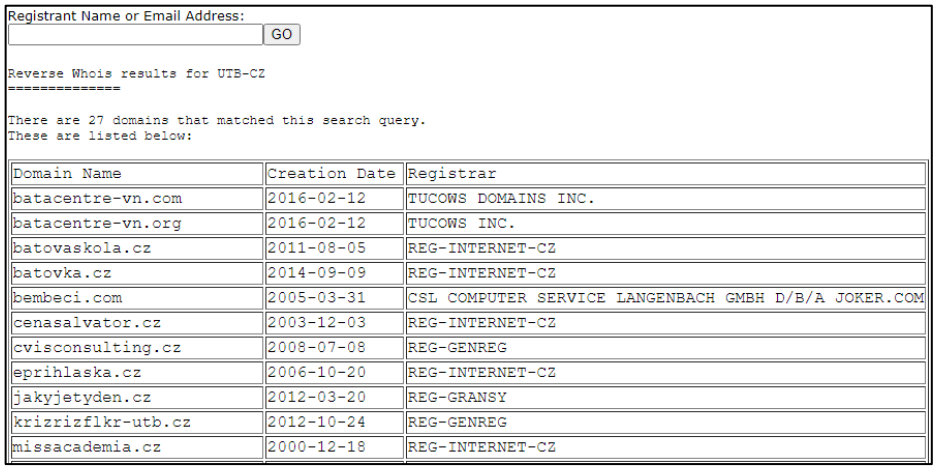
Tato služba umožňuje vkládat doménové jméno nebo IP adresu a na základě těchto údajů zobrazuje další domény, hostované na stejném serveru a jeho další IP adresy. Domény na stejné IP adrese se ale objeví v seznamu, pokud byl dříve zaslán požadavek na překlad adresy z této aplikace. Výsledek takového dotazu pro doménu „seznam.cz“ je ukázán na obrázku č. 30 [37].



Obrázek 30. Výsledek dotazu na doménu „seznam.cz“

2.9.3 ViewDNS Reverse Whois Lookup

Tento nástroj slouží pro vyhledávání domén se stejným názvem registrujícího subjektu nebo uvedeného e-mailu. Výsledek hledání výrazu „UTB-CZ“ ukazuje domény registrované tímto subjektem na obrázku č. 31 [38].



Registrant Name or Email Address:
GO

Reverse Whois results for UTB-CZ
==========

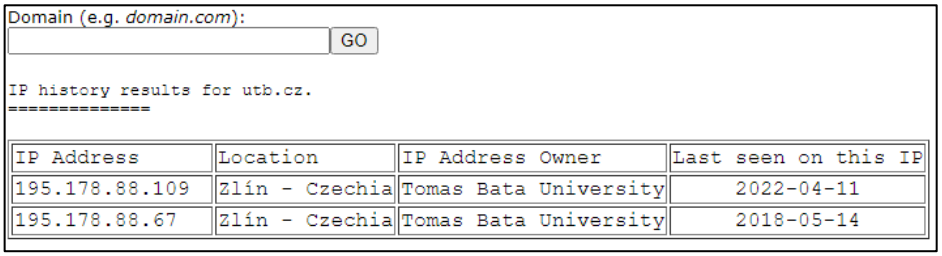
There are 27 domains that matched this search query.
These are listed below:

Domain Name	Creation Date	Registrar
batacentre-vn.com	2016-02-12	TUCOWS DOMAINS INC.
batacentre-vn.org	2016-02-12	TUCOWS INC.
batovaskola.cz	2011-08-05	REG-INTERNET-CZ
batovka.cz	2014-09-09	REG-INTERNET-CZ
bembeci.com	2005-03-31	CSL COMPUTER SERVICE LANGENBACH GMBH D/B/A JOKER.COM
cenasalvator.cz	2003-12-03	REG-INTERNET-CZ
cvisconsulting.cz	2008-07-08	REG-GENREG
eprihlaska.cz	2006-10-20	REG-INTERNET-CZ
jakyjetyden.cz	2012-03-20	REG-GRANSY
krizrizflkr-utb.cz	2012-10-24	REG-GENREG
missacademia.cz	2000-12-18	REG-INTERNET-CZ

Obrázek 31. Domény registrované subjektem „UTB-CZ“

2.9.4 ViewDNS IP History

Tento nástroj umožňuje zobrazovat historický seznam IP adres, na kterých byla daná doména hostována, geografickou polohu IP adresy a jejího vlastníka. Příklad takového dotazu na doménu „utb.cz“ lze vidět na obrázku č. 32 [39].



Domain (e.g. *domain.com*):
GO

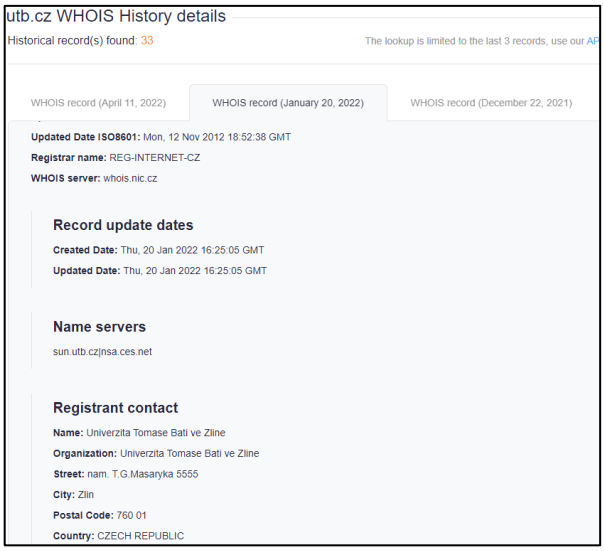
IP history results for utb.cz.
==========

IP Address	Location	IP Address Owner	Last seen on this IP
195.178.88.109	Zlín - Czechia	Tomas Bata University	2022-04-11
195.178.88.67	Zlín - Czechia	Tomas Bata University	2018-05-14

Obrázek 32. IP adresy, na kterých byla hostována doména „utb.cz“

2.9.5 WHOIS History Lookup

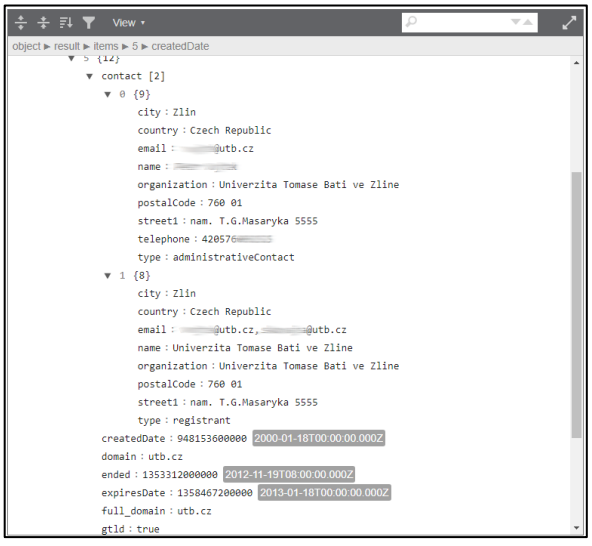
Tento nástroj zpřístupní registrační údaje o předchozích vlastnících dané domény. Bez předchozí registrace zobrazí program pouze poslední tři záznamy, jak je patrné z obrázku č. 33, kde je výsledek dotazu na doménu „utb.cz“ [40].



Obrázek 33. Výsledek hledání v aplikaci WHOIS History Lookup

2.9.6 SecurityTrails

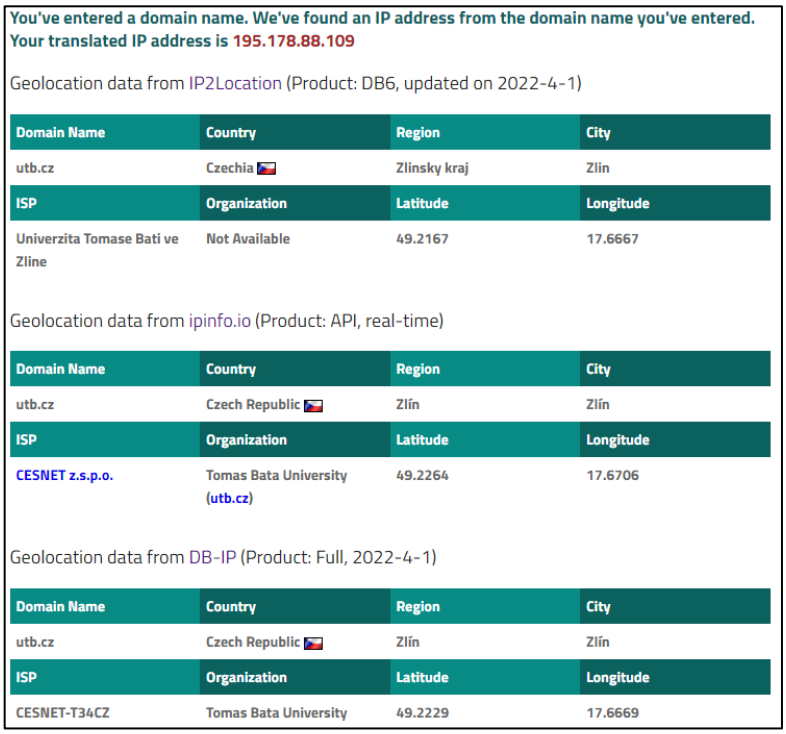
Další nástroj pro zobrazení historických registračních údajů konkrétní domény. Tato data lze získat pomocí poskytovaného API (Application Programming Interface). V tomto případě je nutná registrace na stránkách aplikace kvůli získání klíče pro ověření uživatele. Pro užití API není třeba vytvářet vlastní programový kód a stačí využít testovací prostředí na stránkách dokumentace. Takto získaná data jsou ve formátu JSON (JavaScript Object Notation), kdy jsou datumy udávány ve formátu ISO 8601 (International Organization for Standardization) a pro jejich zobrazení je vhodné použít JSON prohlížeč, například JSON Viewer. Obrázek č. 34 ukazuje část výsledku takového dotazu na doménu „utb.cz“ [41, 42].



Obrázek 34. Registrační údaje domény „utb.cz“

2.9.7 IP Location Finder

Tato webová stránka umožňuje vyhledávat informace o poloze IP adresy pomocí osmi různých nástrojů najednou. Jedná se o tyto aplikace: IP2Location, ipinfo.io, DB-IP, IPregistry.co, IPGeolocation.io, IPapi.co, IPAPI, ipdata.co. U každé služby se vyskytuje informace, jestli údaje pochází z off-line databáze nebo jsou získána pomocí API. Data o poloze zobrazují zemi, region, město a zeměpisnou šířku a délku, jak je vidět na obrázku č. 35, který ukazuje část výsledku, vráceného pro doménu „utb.cz“ [43, 44, 45, 46, 47, 48, 49, 50].


You've entered a domain name. We've found an IP address from the domain name you've entered.
Your translated IP address is 195.178.88.109

Geolocation data from IP2Location (Product: DB6, updated on 2022-4-1)

Domain Name	Country	Region	City
utb.cz	Czechia	Zlinsky kraj	Zlin
ISP	**Organization**	**Latitude**	**Longitude**
Univerzita Tomase Bati ve Zline	Not Available	49.2167	17.6667

Geolocation data from ipinfo.io (Product: API, real-time)

Domain Name	Country	Region	City
utb.cz	Czech Republic	Zlín	Zlín
ISP	**Organization**	**Latitude**	**Longitude**
CESNET z.s.p.o.	Tomas Bata University (utb.cz)	49.2264	17.6706

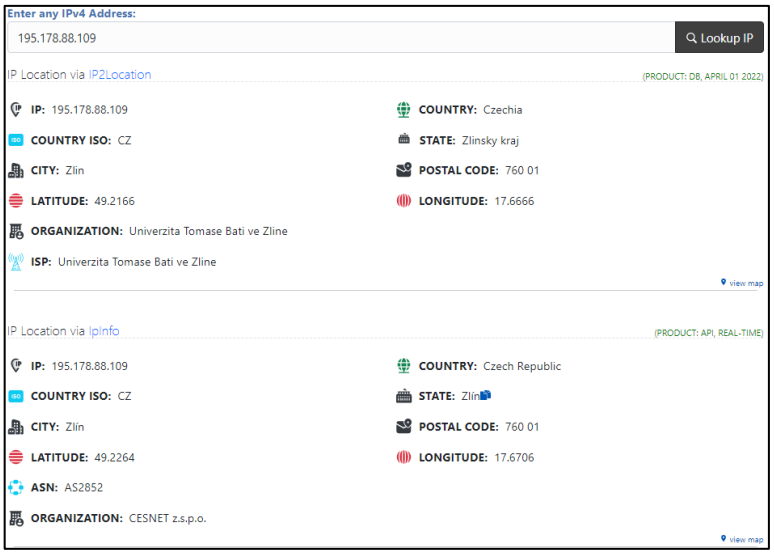
Geolocation data from DB-IP (Product: Full, 2022-4-1)

Domain Name	Country	Region	City
utb.cz	Czech Republic	Zlín	Zlín
ISP	**Organization**	**Latitude**	**Longitude**
CESNET-T34CZ	Tomas Bata University	49.2229	17.6669

Obrázek 35. Údaje o poloze IP adresy 195.178.88.109

2.9.8 IP Lookup Tool

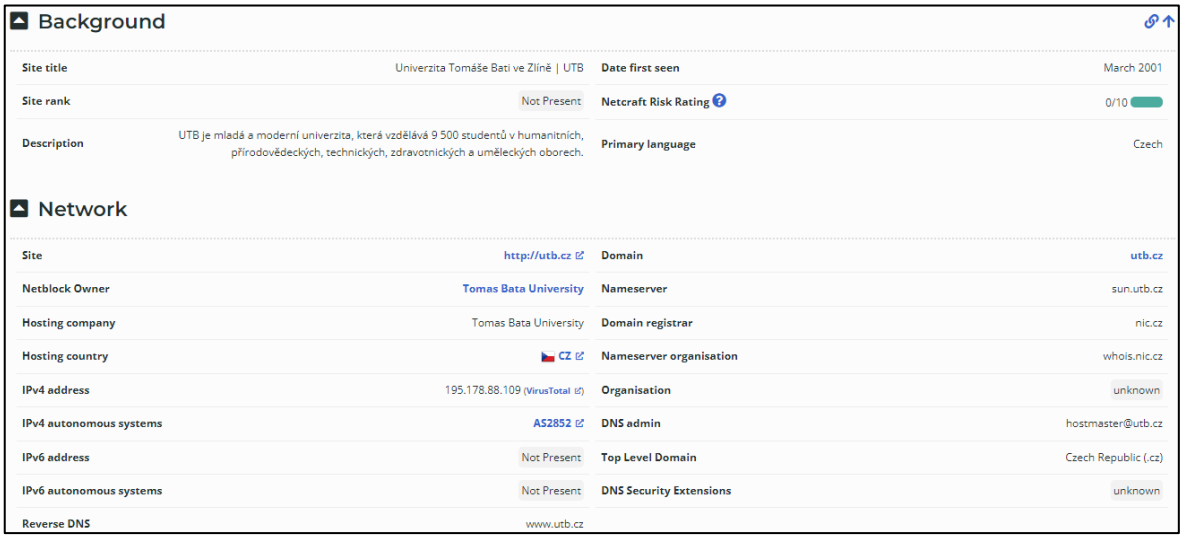
Další podobnou službou je stránka IP Lookup Tool, která sdružuje čtyři nástroje pro vyhledávání geografických údajích o IP adrese. Proti výše uvedené stránce obsahuje tato navíc možnost zobrazení dané polohy přímo na mapě. Část výsledku hledání údajů o IP adrese domény „utb.cz“ je vidět na obrázku č. 36 [51].



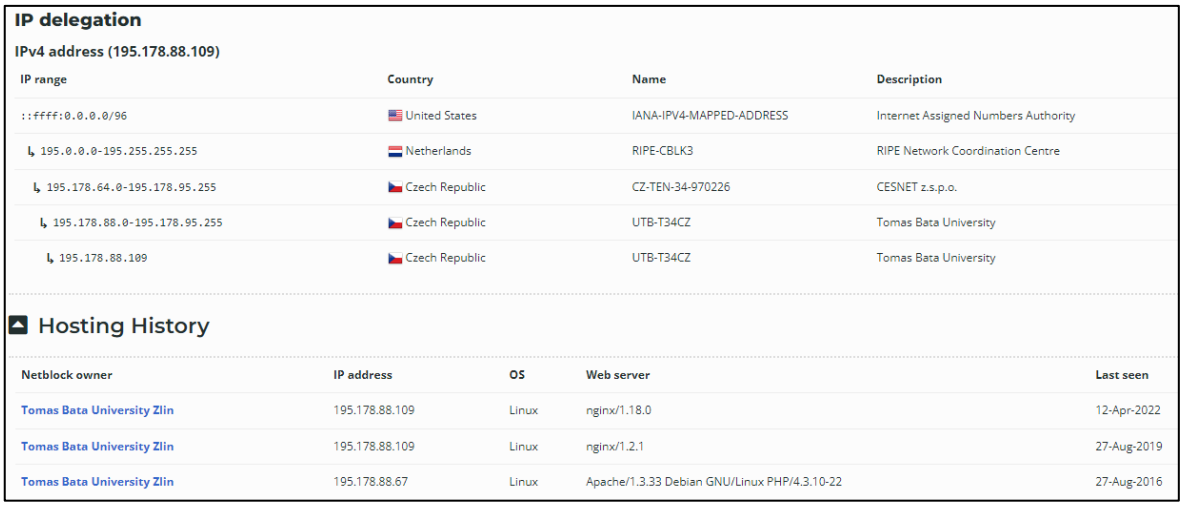
Obrázek 36. Údaje o poloze IP adresy 195.178.88.109

2.9.9 Netcraft Site Report

Nástroj pro získávání informací o infrastruktuře a technologiích používaných na webových stránkách. Zobrazuje například IP adresu daného serveru, vlastníka adresného rozsahu sítě, autonomní systém tohoto adresného rozsahu, společnost poskytující hosting a zemi jejího sídla a registrátora domény. V části „historie hostingu“ jsou uvedeny IP adresy, operační systémy a webové technologie dříve na serveru použité. Také je možné získat detailní informace o SSL (Secure Sockets Layer) nebo TLS (Transport Layer Security) certifikátu použitém pro zabezpečení komunikace. Příklady vyhledávání informací o webových stránkách „utb.cz“ jsou vidět na obrázcích č. 37 a 38 [52].



Obrázek 37. Informace o stránkách utb.cz získané ve službě Netcraft Site Report



IP delegation

IPv4 address (195.178.88.109)

IP range	Country	Name	Description
::ffff:0.0.0.0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
↳ 195.0.0.0-195.255.255.255	Netherlands	RIPE-CBLK3	RIPE Network Coordination Centre
↳ 195.178.64.0-195.178.95.255	Czech Republic	CZ-TEN-34-970226	CESNET z.s.p.o.
↳ 195.178.88.0-195.178.95.255	Czech Republic	UTB-T34CZ	Tomas Bata University
↳ 195.178.88.109	Czech Republic	UTB-T34CZ	Tomas Bata University

Hosting History

Netblock owner	IP address	OS	Web server	Last seen
Tomas Bata University Zlin	195.178.88.109	Linux	nginx/1.18.0	12-Apr-2022
Tomas Bata University Zlin	195.178.88.109	Linux	nginx/1.2.1	27-Aug-2019
Tomas Bata University Zlin	195.178.88.67	Linux	Apache/1.3.33 Debian GNU/Linux PHP/4.3.10-22	27-Aug-2016

Obrázek 38. Informace o stránkách utb.cz získané ve službě Netcraft Site Report

2.9.10 DNSDumpster

Nástroj pro vyhledávání domén a subdomén spojených s konkrétním doménovým jménem využívající nejen záznamy DNS, ale i data z jiných služeb, které získávají při procházejí webových stránek [53].

2.10 Úniky dat

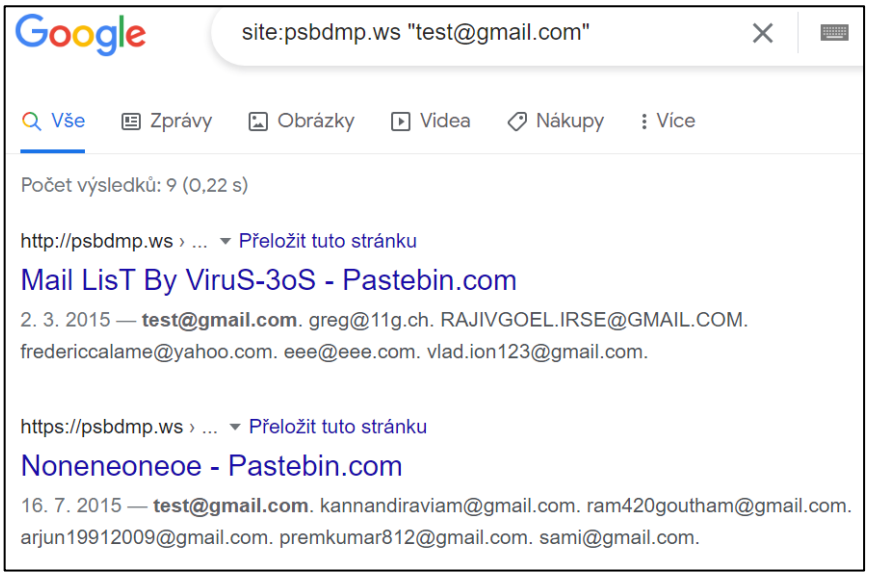
2.10.1 HIBPW

Webová aplikace poskytující informace o e-mailových adresách a heslech pocházejících ze zveřejněných úniků přihlašovacích údajů nebo ze služeb pro sdílení textu. V dubnu 2022 obsahovala stránka data z přibližně 11,8 miliard uživatelských účtů. Pro účely vyšetřování lze tuto aplikaci využít pro zjištění, které služby se stejnou registrační e-mailovou adresou jsou uživatelem používány [54].

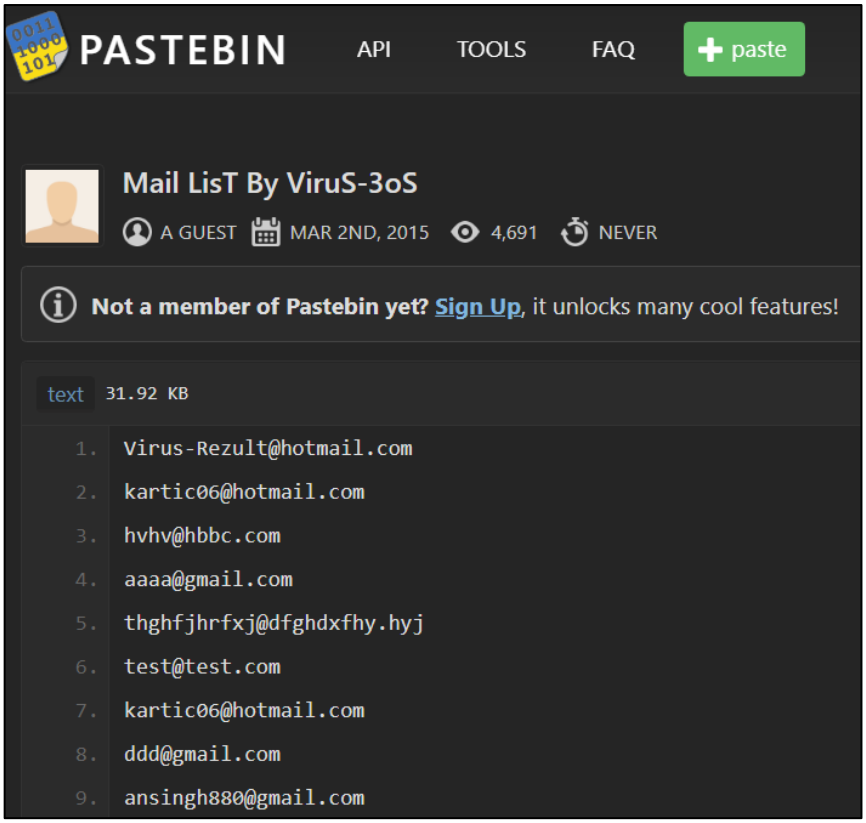
2.10.2 PSBDMP

Aplikace pro vyhledávání dat sdílených pomocí stránky „paste.bin“. Pro vyhledávání výrazů v této službě je ovšem nutné využívat API klíče. Z toho důvodu je nutné vyhledávání provádět metodou Google hacking s operátorem „site“. Například hledání e-mailové adresy „test@gmail.com“ se provádí pomocí řetězce ve tvaru site:psbdmp.ws "test@gmail.com". U takto vrácených výsledků je ještě nutné přepsat část odkazu na stránku do podoby „pastebin.com“. Příklad takového hledání je uveden na obrázcích č. 39 a 40, kdy jako první byl

vyhledán odkaz „http://psbdmp.ws/K7dnzhmc“, který bylo nutné upravit do tvaru „https://pastebin.com/K7dnzhmc“ [20, 55, 56].



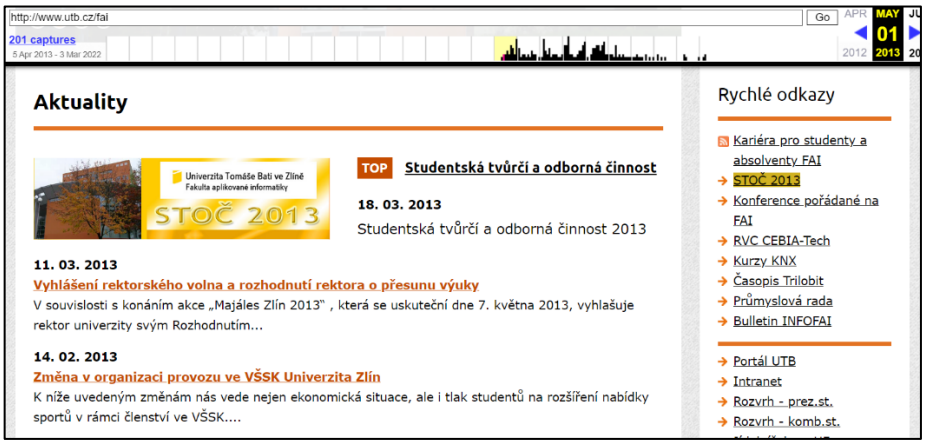
Obrázek 39. Výsledek vyhledávání ve službě Google



Obrázek 40. E-mailové adresy nalezené na stránce pastebin.com

2.11 Wayback Machine

Tato aplikace poskytuje digitální knihovnu internetových stránek. Díky tomu lze zobrazit předchozí verze webových stránek nebo obsah stránek již nefunkčních. V současné době archiv obsahuje přibližně 625 miliard webových stránek. Po zadání URL adresy do vyhledávacího pole se zobrazí časová osa a kalendář s jednotlivými uloženými snímky, které lze vybrat, a tak zobrazit odpovídající obsah dané webové stránky. Na obrázku č. 41 je vidět obsah aktualit stránky „utb.cz/fai“, ze snímku pořízeného 1. května 2013 [57].



Obrázek 41. Obsah webových stránek „utb.cz/fai“ ze snímku z 1. 5. 2013

2.12 Bitcoin Abuse Database

Tato služba je veřejnou databází bitcoinových adres, spojených s nezákonnými aktivitami. Uživatelé zde vytvářejí hlášení o konkrétních bitcoinových adresách s popisem problému. Často jsou zde také uvedeny e-mailové adresy a IP adresy. Obrázek č. 42 ukazuje příklad reportu z aplikace Bitcoin Abuse Database i s nahlášenými e-mailovými a IP adresami [58].

May 6, 2022	sextortion	Same type of email coming from the following senders: petgord34truew@ranninger.at bigjohn@ltis.net brad.ciaverelli@visalign.com boatbuilder@neoburst.net oteosn@cawc.com ohdg.commbeaudry@ohdg.com oteosn@cawc.com patrick.eastwood@pauffley.com wayduehij2783@800alpha.com ludek.straka@sonntag.cz love@laganside.com n.boelger@hagenburger.de qontact@dwbgroup.com sociophagous@akarnam.com orlandohilton@thehotelcard.com lucas@24hotmail.com carmelmoll43@de.syfyman.com rgetter@e-mailfach.de d260019ng@amorana.com heina@heina.ch avnonetheless@mail2libertarian.com b54df1f@songsanpub.co.kr asua@da-gang.de
May 6, 2022	blackmail scam	Not having a cam makes these scams especially hilarious. Header info as follows: Return-Path: [email address redacted] Delivered-To: [email address redacted] Received: (qmail 46213 invoked by uid 0); 6 May 2022 14:29:05 -0000 Received: from unknown (HELO jax4mhib74.registeredsite.com) (64.69.222.84) by 0 with ESMTPS (DHE-RSA-AES256-GCM-SHA384 encrypted); 6 May 2022 14:29:05 -0000 Received: from [49.230.167.31] ([49.230.167.31]) by jax4mhib74.registeredsite.com (8.14.4/8.14.4) with ESMTP id 246ESw2U023564 for [email address redacted]; Fri, 6 May 2022 10:29:01 -0400 From: [email address redacted] To: [email address redacted] Subject: You have an outstanding payment. Debt settlement required. Date: 7 May 2022 03:22:56 +0600 Message-ID: <002d01d86190$036924ee$58b18a84$@therossinis.com> MIME-Version: 1.0 Content-Type: text/plain; charset="windows-1250" Content-Transfer-Encoding: 8bit X-Mailer: Microsoft Outlook 14.0 Thread-Index: Ac7l589usf4mf8217l589usf4mf821== Content-Language: en X-Custom-SpamThreshold: 16 X-SpamScore: 4.502 X-MailHub-Apparently-To: [email address redacted]

Obrázek 42. Report z aplikace Bitcoin Abuse Database

2.13 Certificate Search

Aplikace pro vyhledávání informací o digitálních certifikátech. Umožňuje vyhledávat například podle doménového jména, sériového čísla, hashového otisku, názvu subjektu nebo e-mailové adresy. Na obrázku č. 43 je vidět příklad vyhledávání certifikátů, které v identifikátoru obsahují řetězec „utb.cz“ [59].

Criteria	Type: Identity Match: ILIKE Search: 'utb.cz'

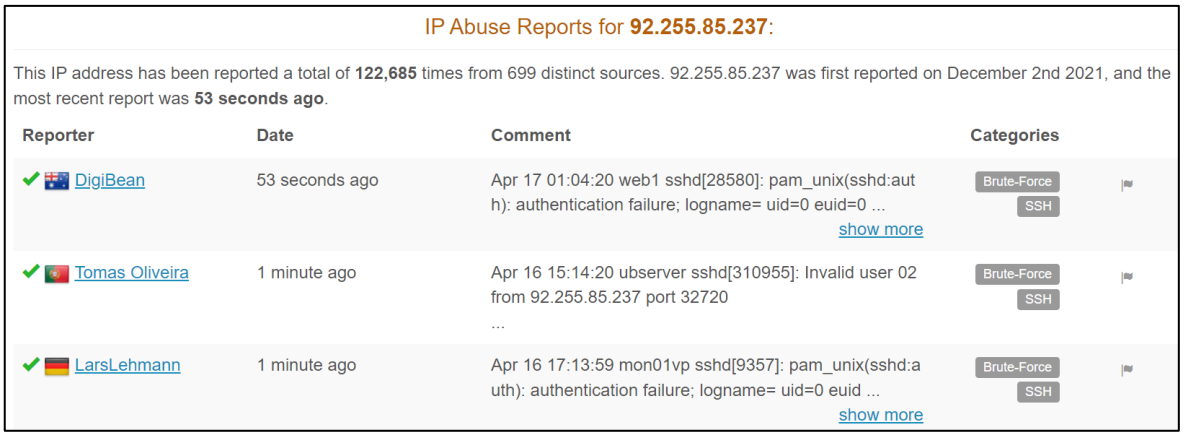
crt.sh ID	Logged At ⇧	Not Before	Not After	Common Name	Matching Identities	Issuer Name
6693150858	2022-05-09	2022-05-09	2023-05-09	nce.fame.utb.cz	nce.fame.utb.cz www.nce.fame.utb.cz	C=NL, O=GEANT Vereniging, CN=GEANT OV RSA CA 4
6692633746	2022-05-09	2022-05-09	2023-05-09	ticket.ptlab.utb.cz	ticket.ptlab.utb.cz	C=NL, O=GEANT Vereniging, CN=GEANT OV ECC CA 4
6692633741	2022-05-09	2022-05-09	2023-05-09	s1.ptlab.utb.cz	s1.ptlab.utb.cz	C=NL, O=GEANT Vereniging, CN=GEANT OV ECC CA 4
6692633565	2022-05-09	2022-05-09	2023-05-09	ipam.ptlab.utb.cz	ipam.ptlab.utb.cz	C=NL, O=GEANT Vereniging, CN=GEANT OV ECC CA 4
6692633275	2022-05-09	2022-05-09	2023-05-09	kimai.ptlab.utb.cz	kimai.ptlab.utb.cz	C=NL, O=GEANT Vereniging, CN=GEANT OV ECC CA 4
6692633501	2022-05-09	2022-05-09	2023-05-09	wekan.ptlab.utb.cz	wekan.ptlab.utb.cz	C=NL, O=GEANT Vereniging, CN=GEANT OV ECC CA 4
6690857282	2022-05-09	2022-05-09	2022-08-07	lamp14.fame.utb.cz	lamp14.fame.utb.cz	C=US, O=Let's Encrypt, CN=R3
6690852596	2022-05-09	2022-05-09	2022-08-07	lamp11.fame.utb.cz	lamp11.fame.utb.cz	C=US, O=Let's Encrypt, CN=R3
6690811924	2022-05-09	2022-05-09	2022-08-07	lamp10.fame.utb.cz	lamp10.fame.utb.cz	C=US, O=Let's Encrypt, CN=R3
6690806234	2022-05-09	2022-05-09	2022-08-07	lamp1.fame.utb.cz	lamp1.fame.utb.cz	C=US, O=Let's Encrypt, CN=R3
6690806057	2022-05-09	2022-05-09	2022-08-07	finport.fame.utb.cz	finport.fame.utb.cz	C=US, O=Let's Encrypt, CN=R3
6690843088	2022-05-09	2022-05-09	2022-08-07	finftp.fame.utb.cz	finftp.fame.utb.cz	C=US, O=Let's Encrypt, CN=R3
6690798982	2022-05-09	2022-05-09	2022-08-07	booking.fame.utb.cz	booking.fame.utb.cz	C=US, O=Let's Encrypt, CN=R3
6671394794	2022-05-05	2022-05-05	2022-08-03	www-new.k.utb.cz	www-new.k.utb.cz	C=US, O=Let's Encrypt, CN=R3
6668471387	2022-05-05	2022-05-05	2023-05-05	glpi.fmk.utb.cz	glpi.fmk.utb.cz	C=NL, O=GEANT Vereniging, CN=GEANT OV RSA CA 4

Obrázek 43. Výsledek vyhledávání v aplikaci Certificate Search

2.14 Komplexní nástroje

2.14.1 AbuseIPDB

Tento projekt slouží k reportování a ověřování IP adres a domén, které jsou spojené se škodlivou činností na Internetu. Uživatelé zde mohou vkládat škodlivé IP adresy a doménová jména i s určením kategorie zneužití nebo je zde možné získat informace o adrese již dříve reportované. Pro účely vyhledávání lze zadat IP adresu, doménové jméno nebo adresný rozsah. Vedle základních údajů o vyhledané IP adrese nebo doméně se zobrazí také ukazatel „jistoty zneužití“ v rozsahu 0 až 100 %. Toto číslo se zvyšuje postupně podle to, jak je daná adresa nahlášena od více uživatelů. Dále je zde také uvedena tabulka jednotlivých hlášení analyzované adresy s uvedeným uživatelským jménem, datem hlášení, komentářem s popisem a kategorií zneužití. Na obrázku č. 44 je ukázán takový výsledek pro IP adresu 92.255.85.237 [60].



IP Abuse Reports for **92.255.85.237**:

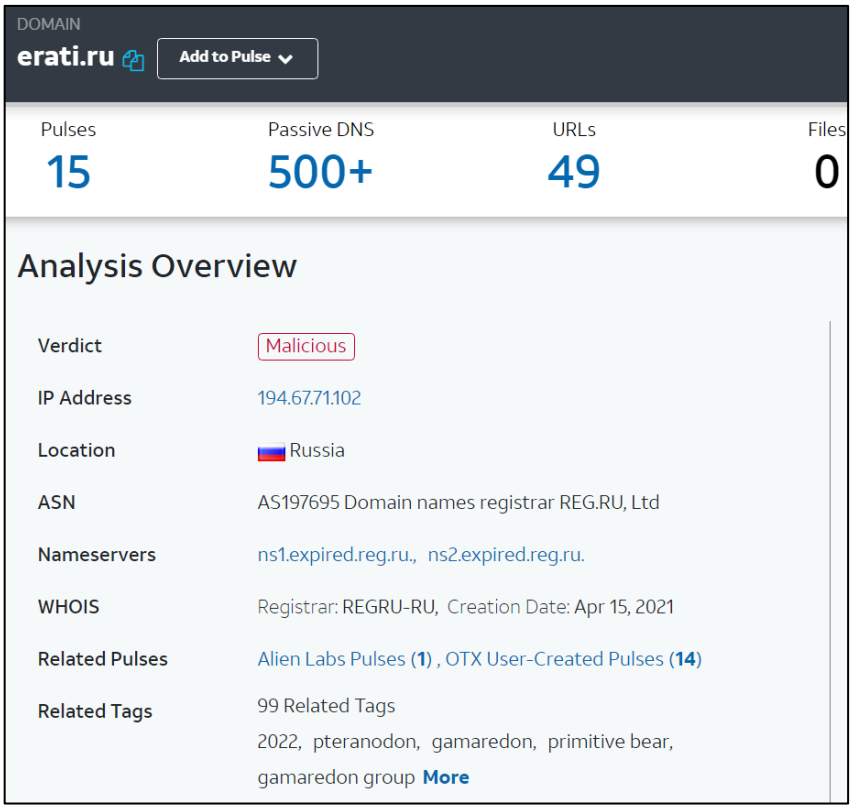
This IP address has been reported a total of **122,685** times from 699 distinct sources. 92.255.85.237 was first reported on December 2nd 2021, and the most recent report was **53 seconds ago**.

Reporter	Date	Comment	Categories
DigiBean	53 seconds ago	Apr 17 01:04:20 web1 sshd[28580]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 ... show more	Brute-Force SSH
Tomas Oliveira	1 minute ago	Apr 16 15:14:20 ubserver sshd[310955]: Invalid user 02 from 92.255.85.237 port 32720 ...	Brute-Force SSH
LarsLehmann	1 minute ago	Apr 16 17:13:59 mon01vp sshd[9357]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid ... show more	Brute-Force SSH

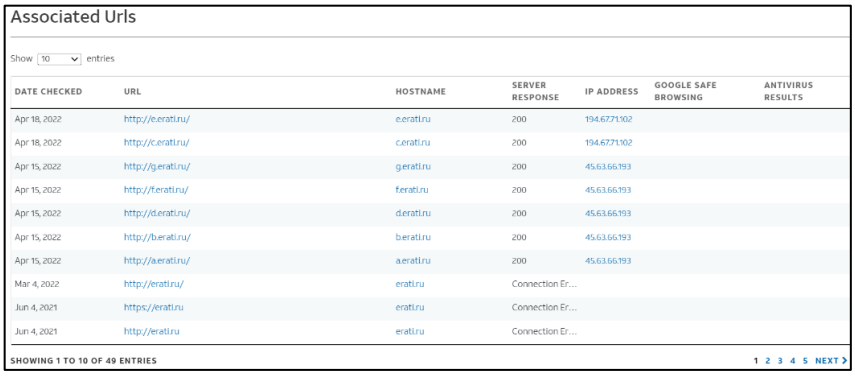
Obrázek 44. Výsledek vyhledávání IP adresy 92.255.85.237 ve službě AbuseIPDB

2.14.2 Alien Labs Open Threat Exchange (OTX)

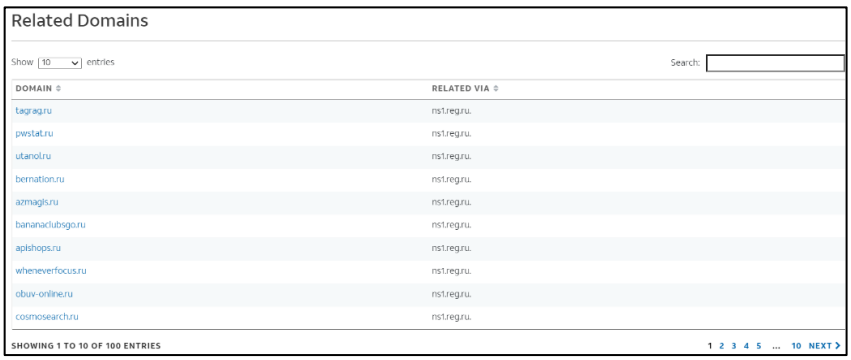
Tato platforma firmy AT&T slouží ke shromažďování a sdílení informací o probíhajících kybernetických útocích a bezpečnostních hrozbách. V současné době má projekt více než 100 000 uživatelů ze 140 zemí, kteří denně přispívají více než 19 miliony indikátory hrozeb. OTX umožňuje členům bezpečnostní komunity diskutovat, zkoumat, ověřovat a sdílet nejnovější data o kybernetických hrozbách, trendy a techniky. Pro účely OSINT analýzy je možné vyhledávat indikátory hrozeb, jako jsou například IP adresy, názvy domén, e-mailové adresy a hashe souborů. Výsledkem takového dotazu je seznam provedených analýz a takzvaných pulzů, což jsou shrnující informace o určité kybernetické hrozbě, obsahující popis hrozby, seznam indikátorů hrozeb vztahujících se k pulzu a odkazy na další související pulzy. Obrázky č. 45, 46 a 47 ukazují části výsledků vyhledávání informací o doméně „erati.ru“ [61].



Obrázek 45. Přehled analýzy ve službě OTX



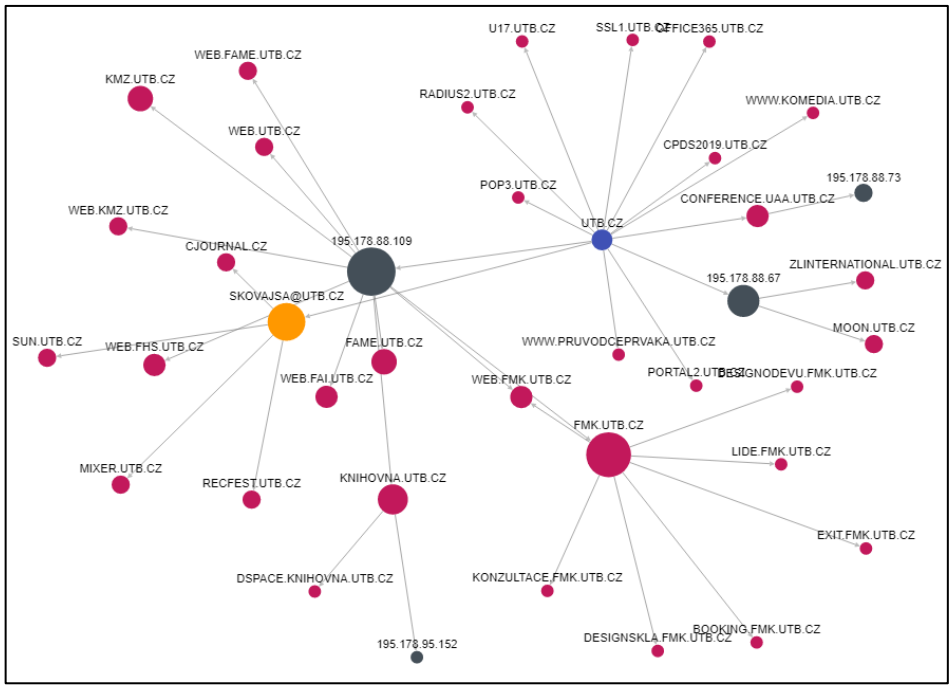
Obrázek 46. Související URL adresy vyhledané ve službě OTX



Obrázek 47. Vyhledané domény související s hledaným výrazem

2.14.3 Threat Crowd

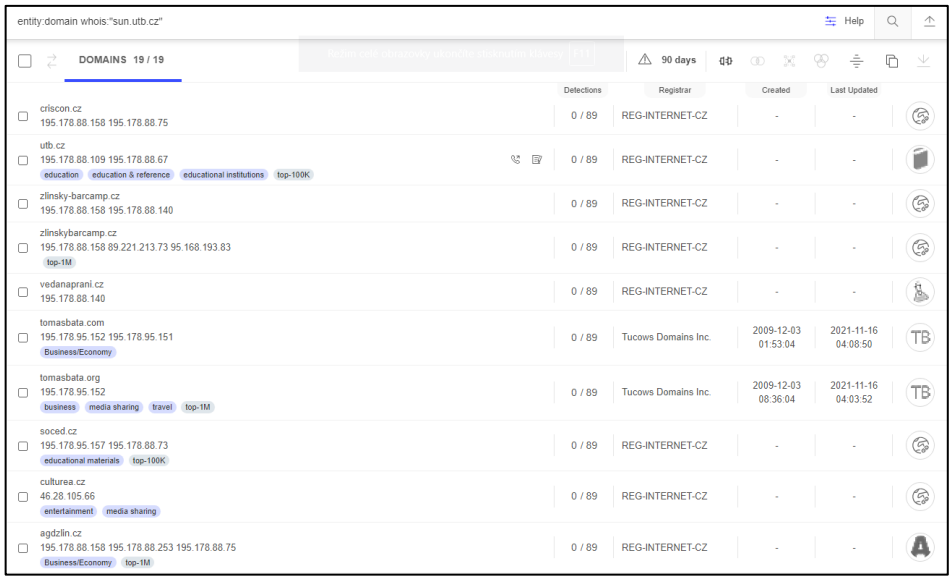
Aplikace využívající služeb společnosti AlienVault pro vyhledávání informací o doménách. Proti službě OTX navíc zobrazuje graf s vazbami souvisejících domén, subdomén a IP adres. Vyhledávání lze provádět pomocí domény, IP adresy, e-mailové adresy nebo názvu organizace. Výsledek takového dotazu na doménu „utb.cz“ lze vidět na obrázku č. 48 [62].



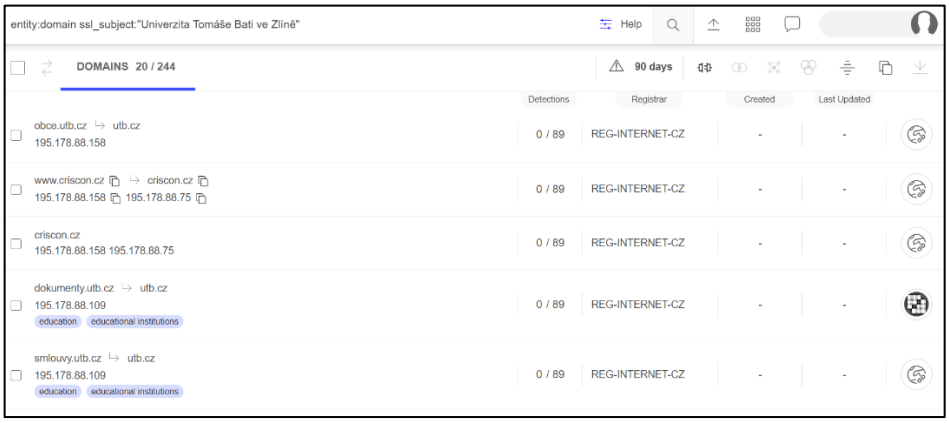
Obrázek 48. Výsledek dotazu na vazby domény „utb.cz“ v aplikaci Threat Crowd

2.14.4 VirusTotal

Tato aplikace shromažďuje informace z více než 70 antivirových skenerů a služeb pro skenování domén a webových stránek, nástrojů pro analýzu chování a popis souborů, data ze systémů IDS (Intrusion Detection System) a příspěvků uživatelů. Vedle základních informací o souborech a doménách je možné, v rámci placené služby VT Enterprise, využívat množství modifikátorů pro vyhledávání v doménách, IP adresách, adresách URL a souborech, a to pak umožňuje lépe rozkrývat síťovou infrastrukturu. Například pomocí dotazu „entity:domain whois:"sun.utb.cz"“ lze vyhledat domény používající DNS server „sun.utb.cz“. Výsledek dotazu lze vidět na obrázku č. 49. Dalším příkladem může být vyhledávání domén, které používají SSL/TLS certifikát obsahující řetězec „Univerzita Tomáše Bati ve Zlíně“ v poli subjekt. Dotaz má pak tento tvar: „entity:domain ssl_subject:"Univerzita Tomáše Bati ve Zlíně"“. Výsledek tohoto vyhledávání lze vidět na obrázku č. 50 [63, 64, 65].



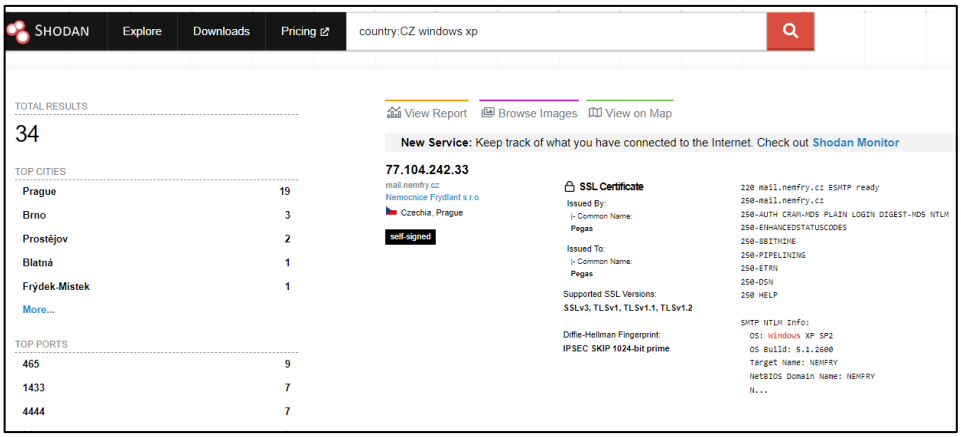
Obrázek 49. Vyhledávání domén se jmenným serverem „sun.utb.cz“



Obrázek 50. Vyhledávání domén používajících stejný certifikát

2.14.5 Shodan

Aplikace pro vyhledávání informací o zařízeních připojených k Internetu. Tato zařízení komunikují s okolím prostřednictvím služeb, které si s klienty vyměňují úvodní informace. Tato metadata o softwaru jsou uložena v takzvaných bannerech, které Shodan shromažďuje a ve kterých probíhá vyhledávání. Vyhledávat lze pomocí klíčových slov a po přihlášení lze dotazy upřesňovat pomocí filtrů. Pomocí dotazu „country:CZ windows xp“ lze například vyhledat zařízení v Česku s operačním systémem Windows XP, která jsou připojená do Internetu. Výsledek takového dotazu ukazuje obrázek č. 51, kdy bylo vyhledáno 34 takových zařízení [66, 67]

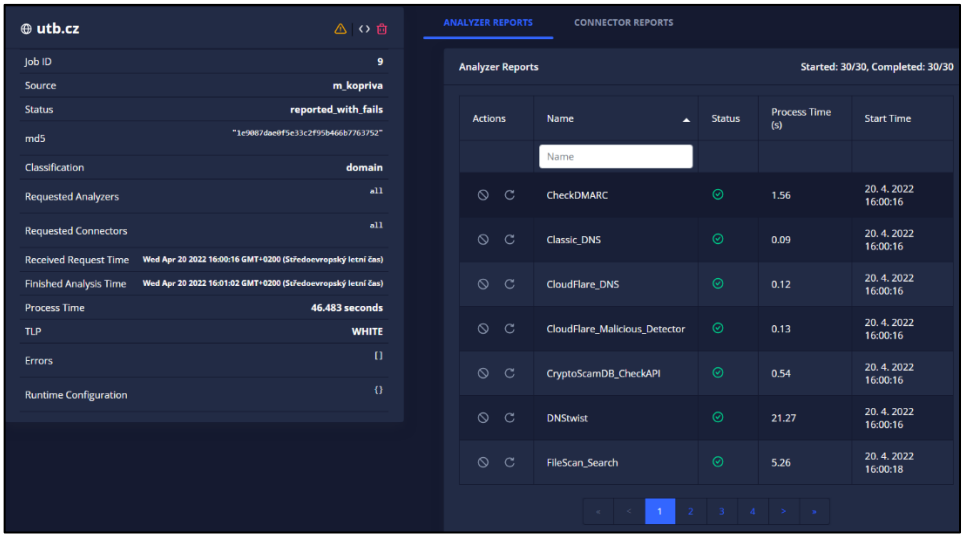


Obrázek 51. Výsledek hledání ve službě Shodan

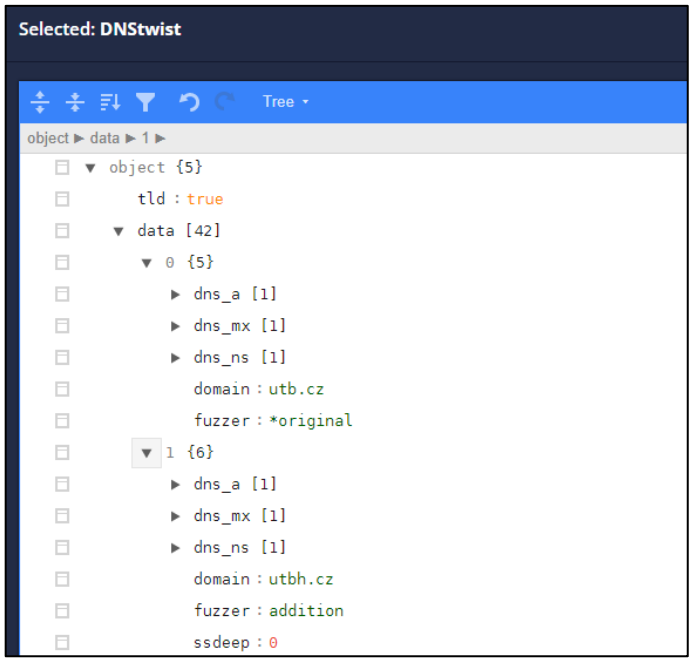
2.14.6 IntelOwl

Aplikace pro získávání informací o IP adresách, doménách a souborech z více služeb pomocí jediného dotazu. Integruje řadu online analyzátorů a nástrojů pro analýzu malwaru. U některých těchto nástrojů je nutné zadat API klíče pro nastavení ověřování uživatele. Požadované úlohy lze automatizovat a po každé úspěšné analýze jsou získaná data exportována do dalších externích aplikací, jako je například OpenCTI nebo MISP (Malware Information Sharing Platform). Jako nevýhoda se jeví nemožnost rozboru více identifikátorů najednou, například jako seznam IP adres. Na obrázku č. 52 je zobrazen souhrn analýz a na obrázku č. 53 detail jedné z nich, provedené pro doménu „utb.cz“ v aplikaci IntelOwl [68].

Dalším příkladem aplikace pro automatizované shromažďování dat za účelem OSINT může být služba SpiderFoot [69].



Obrázek 52. Souhrn provedené analýzy domény „utb.cz“



Obrázek 53. Detail konkrétní analýzy domény „utb.cz“

3 OSINT A GDPR

GDPR (General Data Protection Regulation), celým názvem Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (Obecné nařízení o ochraně osobních údajů), které vstoupilo v platnost 25. května 2018, stanovuje pravidla pro zpracování a ochranu osobních údajů fyzických osob (i podnikajících) a sjednocuje právní výklad v evropském prostoru. Tato právní norma se vztahuje také na společnosti, které se nenacházejí v Evropské unii, ale nabízejí své služby a zboží osobám fyzicky se nacházejícím v EU. Dle definic tohoto nařízení jsou osobními údaji veškeré informace o identifikované nebo identifikovatelné fyzické osobě. Identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokalizační údaje, síťový identifikátor atd. Pro účely této práce je to tedy především jméno, adresa, telefonní číslo, e-mailová adresa, IP adresa, audio a video záznamy. Nařízení GDPR omezuje zpracování osobních údajů na situace, kdy existuje alespoň je-den ze šesti zákonných podmínek pro zpracování osobních údajů z článku 6. Pro účely získávání informací metodami OSINT jsou relevantní pododstavce 1a (udělení souhlasu), 1c (splnění právní povinnosti) a 1f (oprávněný zájem). Podmínka splnění právní povinnosti je aplikovatelná například když má regulovaná finanční instituce povinnost identifikovat své zákazníky a zdroj jejich finančních prostředků. Oprávněný zájem shromažďovat osobní údaje uplatní například firma při výběru nových zaměstnanců, aby zjistila, koho bude zaměstnávat a jaká rizika jí hrozí z hlediska její pověsti. Dále by měly být dodržovány zásady zpracování osobních údajů podle článku 5. Údaje musí být zpracovávány korektně a zákonným a transparentním způsobem. Nesmí být uloženy déle, než je nezbytné pro zamyšlené účely. Data musí být zabezpečena proti neoprávněnému zpracování, ztrátou, poškozením nebo zničením. V článku 4 jsou také definovány role správce, což je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který určuje účely a prostředky zpracování osobních údajů a zpracovatelem, což je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce. V článku 85 tohoto nařízení jsou stanoveny určité výjimky z těchto pravidel pro novinářské účely nebo pro účely akademického, uměleckého či literárního projevu [70, 71, 72].

Organizace ICANN na nařízení GDPR reagovala a 17. května 2018 schválila dočasnou specifikaci registračních údajů gTLD (generic Top Level Domain). Tato specifikace poskytuje

jednotný model, který zajišťuje rámec pro nakládání s registračními údaji. Jejím cílem je zajistit trvalou dostupnost služby WHOIS a zároveň zachovat bezpečnost a stabilitu systému jedinečných identifikátorů na Internetu. Podle této normy jsou registrátoři stále povinni evidovat všechny údaje, ale po zadání dotazu do systému WHOIS jsou vráceny pouze technické údaje o registraci, bez osobní údajů. Při registraci některých domén lze využít služeb „Whois Privacy“, kdy jsou údaje o registrujícím subjektu skryty. Existuje ale řada domén, kde kompletní skrytí kontaktních údajů není možné. Například při registraci CZ domény nelze skrýt jméno kontaktu a v případě, že kontakt není ověřen, ani jeho adresu. U podnikající fyzické osoby nelze maskovat ani adresu kontaktu. Neveřejné informace, které jsou veřejně nepřístupné, jsou na vyžádání u registrátora dostupné subjektům s oprávněným zájmem. Na obrázku č. 54 jsou vidět historické registrační údaje domény „mvcr.cz“ z února roku 2018. V tu dobu bylo možné získat jméno, e-mailovou adresu a telefonní číslo administrativního kontaktu, zadané při registraci domény. Proti tomu obrázek č. 55 ukazuje registrační údaje získané v dubnu roku 2022 [72, 73, 74, 75, 76, 77].

Obrázek 54. Historické registrační údaje domény „mvcr.cz“

Doména	mvcr.cz
Registrace od	12.06.1995
Poslední aktualizace	18.06.2020
Datum expirace	13.10.2022
Držitel	NAKIT-SERVER-CMS Nakit s.p.
Administrativní kontakt	NAKIT-SERVER-CMS Nakit s.p.
Určený registrátor	REG-ZONER ZONER software, a. s. od 12. listopadu 2018 11:31

Obrázek 55. Aktuální registrační údaje domény „mvcr.cz“

I přesto, že nařízení GDPR zpřísňuje podmínky pro nakládání z osobními údaji a za porušení těchto pravidel hrozí vysoké pokuty, je stále možné pozorovat úniky takových dat. Výskyt těchto událostí, které obecně představují bezpečnostní problém, jsou samozřejmě pro účely OSINTu výhodné. Jako příklad může sloužit únik dat přibližně 400 tisíc zákazníků společnosti British Airways v roce 2018. Dalším příkladem je únik údajů 5 milionů občanů Bulharska z místního finančního úřadu v roce 2019. V obou případech uložily místní regulační úřady pokuty pro nedodržování zabezpečení osobních údajů ve správě dotčených subjektů [78].

II. PRAKTICKÁ ČÁST

4 METODIKA OSINT ANALÝZY

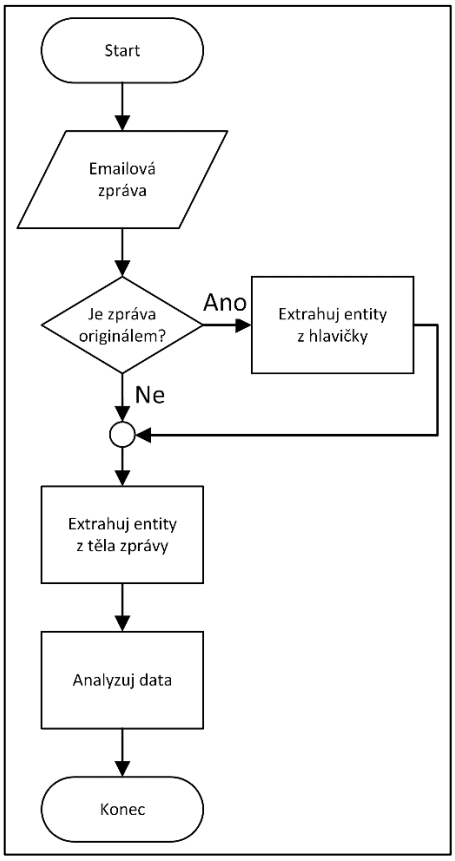
Při získávání informací pomocí OSINT je pravděpodobné, že bude nalezeno velké množství zdrojů a informací v nich obsažených a není možné postupovat nahodile. Je vhodné si ujasnit, jaké vstupní informace existují na začátku analýzy a jakých cílů je třeba dosáhnout, jaké informace jsou požadovány. Pro samotnou analýzu je výhodné mít vytvoření opakovatelný pracovní návod, který umožní efektivní a promyšlený postup pro získávání informací. V následující části této kapitoly bude takový postup zobrazen. A to pomocí vývojových diagramů, které popisují získávání dat, nad kterými se provádí analýza a pomocí tabulek s nástroji, které slouží pro samotnou analýzu jednotlivých ukazatelů a byly představeny v kapitole 2 této práce.

4.1 Zdroje dat pro analýzu

Zdrojem ukazatelů pro analýzu OSINT je velké množství. Ať už se jedná o informace v elektronické podobě, jako e-mailové zprávy nebo datové soubory, anebo se jedná o informace v analogové podobě, jako jsou papírové dokumenty nebo zjištění sdělená osobně. Před zahájením samotné analýzy je nutné taková data extrahovat, odstranit duplicity, případně převést do elektronické formy. Následná práce s daty je pak přehlednější a systematičtější.

4.1.1 E-mailové zprávy

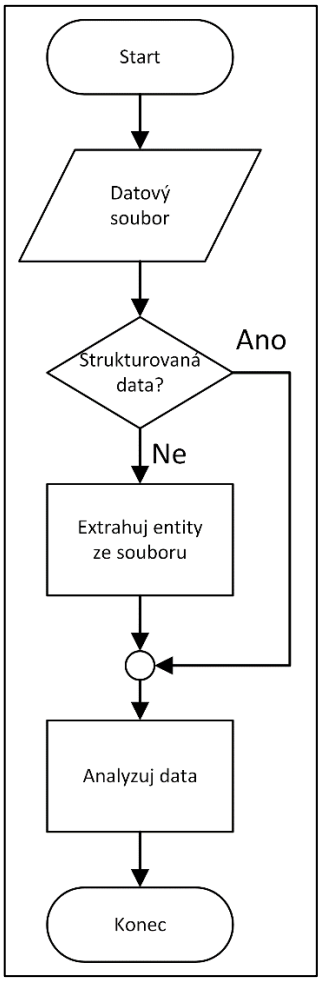
U e-mailových zpráv je zdrojem dat jejich obsah a v případě, že existuje originální zpráva, také hlavička e-mailu. Pro zlepšení čitelnosti dat z hlavičky lze použít nástroje Mailheader nebo Mail Header Analyser. Takto lze získat e-mailové adresy, IP adresy, doménová jména, adresy kryptoměnových peněženek, jména osob a další informace. Na obrázku č. 56 je zobrazen vývojový diagram získávání dat z e-mailové zprávy.



Obrázek 56. Extrakce dat z e-mailové zprávy

4.1.2 Datové soubory

Datové soubory mohou pocházet z různých dohledových systémů pro provozní monitoring, bezpečnostní monitoring, jako jsou SIM (Security Information Management), SEM (Security Event Management), SIEM (Security Information and Event Management) systémy. Zdrojem dat mohou být výstupy z ETL (Extract Transform Load) systémů, které slouží k vytěžování, upravování a spojování různorodých informačních zdrojů. A v neposlední řadě to mohou být jakékoliv soubory obsahující zájmová data. Obrázek č. 57 ukazuje potup při extrahování informací z datového souboru, v závislosti na tom, jestli se jedná o strukturovaná, polostrukturovaná nebo nestrukturovaná data.



Obrázek 57. Extrakce dat ze souboru

4.1.3 Multimediální soubory

Tyto soubory jsou kromě obsahu samotného zdrojem metadat. Je to například údaj o délce videa, datum pořízení, údaje o zeměpisné poloze záznamu a podobně.

4.1.4 Ostatní zdroje

Do této kategorie zdrojů spadají různé papírové dokumenty, osobní nebo telefonická sdělení. Informace takto získané je nutné převést do elektronické podoby, ve formě strukturovaných dat.

4.2 Nástroje analýzy

V této části jsou v tabulkách č. 2 až 8 uvedeny konkrétní, dříve popsané nástroje, pomocí kterých se postupně provádí samotná analýza. Tabulky jsou rozděleny do jednotlivých oddílů podle druhu ukazatele, který nástroj analyzuje. Pokud v průběhu zkoumání dojde

ke zjištění dalších, nových informaci, které je možné analyzovat, je nutné provést s těmito ukazateli další proces analýzy.

4.2.1 E-mailová adresa

Tabulka 2. Nástroje pro analýzu e-mailové adresy

Nástroj	Odkaz	Kapitola
Trumail	https://trumail.io	2.7.1
Google	https://www.google.com	2.1.1
Carrot	https://search.carrot2.org	2.1.2
EmailRep	https://emailrep.io	2.7.2
Reverse Whois Lookup	https://viewdns.info/reversewhois	2.9.5
HIBPW	https://haveibeenpwned.com	2.10.1
PSBDMP	https://www.google.com	2.10.2
Certificate Search	https://crt.sh	2.13
OTX	https://otx.alienvault.com	2.14.2
Threat Crowd	https://www.threatcrowd.org	2.14.3

4.2.2 Uživatelské jméno

Tabulka 3. Nástroje pro analýzu uživatelského jména

Nástroj	Odkaz	Kapitola
Google	https://www.google.com	2.1.1
Carrot	https://search.carrot2.org	2.1.2
KnowEm	https://knowem.com	2.8.1
Instant Username Search	https://instantusername.com	2.8.2
WhatsMyName	https://whatsmyname.app	2.8.3
PSBDMP	https://www.google.com	2.10.2

Facebook	https://www.facebook.com	2.6.1
Twitter	https://twitter.com/search-advanced	2.6.2
All My Tweets	https://www.allmytweets.net	2.6.3

4.2.3 Doménové jméno

Tabulka 4. Nástroje pro analýzu doménového jména

Nástroj	Odkaz	Kapitola
Google	https://www.google.com	2.1.1
Carrot	https://search.carrot2.org	2.1.2
ICANN registration data lookup	https://lookup.icann.org	2.9.1
ViewDNS Reverse IP	https://viewdns.info/reverseip	2.9.2
ViewDNS IP History	https://viewdns.info/iphistory	2.9.4
WHOIS History Lookup	https://whois-history.whoisxmlapi.com/lookup	2.9.5
SecurityTrails	https://docs.securitytrails.com/reference/history-whois	2.9.6
IP Location Finder	https://www.iplocation.net	2.9.7
IP Lookup Tool	https://iplocation.io	2.9.8
Netcraft Site Report	https://sitereport.netcraft.com	2.9.9
DNSDumpster	https://dnsdumpster.com	2.9.10
Wayback Machine	https://archive.org/web	2.11
Certificate Search	https://crt.sh	2.13
AbuseIPDB	https://www.abuseipdb.com	2.14.1
OTX	https://otx.alienvault.com	2.14.2
Threat Crowd	https://www.threatcrowd.org	2.14.3
VirusTotal	https://www.virustotal.com	2.14.4

Shodan	https://www.shodan.io	2.14.5

4.2.4 IP adresa

Tabulka 5. Nástroje pro analýzu IP adresy

Nástroj	Odkaz	Kapitola
Google	https://www.google.com	2.1.1
Carrot	https://search.carrot2.org	2.1.2
ICANN registration data lookup	https://lookup.icann.org	2.9.1
ViewDNS Reverse IP	https://viewdns.info/reverseip	2.9.2
IP Location Finder	https://www.iplocation.net	2.9.7
IP Lookup Tool	https://iplocation.io	2.9.8
Netcraft Site Report	https://sitereport.netcraft.com	2.9.9
AbuseIPDB	https://www.abuseipdb.com	2.14.1
OTX	https://otx.alienvault.com	2.14.2
Threat Crowd	https://www.threatcrowd.org	2.14.3
VirusTotal	https://www.virustotal.com	2.14.4
Shodan	https://www.shodan.io	2.14.5

4.2.5 Adresa kryptoměnové peněženky

Tabulka 6. Nástroje pro kryptoměnové peněženky

Nástroj	Odkaz	Kapitola
Bitcoin Abuse Database	https://www.bitcoinabuse.com	2.12

4.2.6 Identifikační číslo certifikátu

Tabulka 7. Nástroje pro analýzu certifikátu

Nástroj	Odkaz	Kapitola

Certificate Search	https://crt.sh	2.13
VirusTotal	https://www.virustotal.com	2.14.4
Shodan	https://www.shodan.io	2.14.5

4.2.7 Obrázek

Tabulka 8. Nástroje pro analýzu obrázků

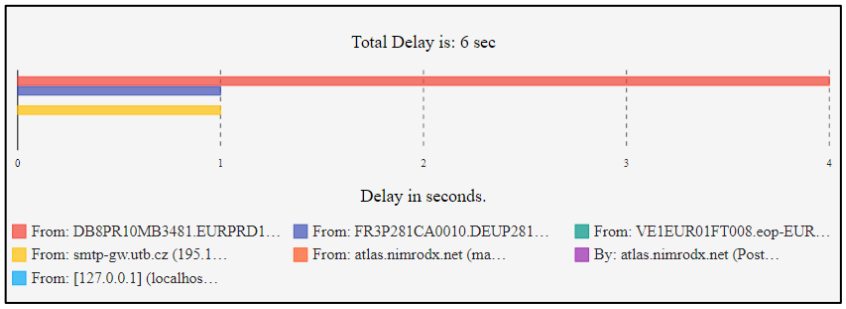
Nástroj	Odkaz	Kapitola
ExifTool	https://exiftool.org	2.2.2
TinEye	https://tineye.com/	2.5.1

5 TESTOVÁNÍ METODIKY

V této části je navržená metodika otestována. Pomocí výše uvedených postupů je provedena extrakce dat a také ověřena funkčnost jednotlivých nástrojů na vzorových datech.

5.1 E-mailová zpráva

Vstupem pro tuto analýzu je e-mailová zpráva zachycená jako spam. Extrakce dat proběhla podle schématu na obrázku č. 56. Jedná se o původní e-mailovou zprávu v elektronické podobě a to znamená, že je možné využít jako zdroj informací nejen obsah zprávy samotné, ale i její hlavičku. Pomocí nástroje MsgEml z kapitoly 2.7.3 byla nejdříve získána hlavička původní zprávy a z ní byly poté extrahovány údaje použitím nástroje Mail Header Analyzer, z kapitoly 2.7.5. Obrázek č. 58 ukazuje graficky znázorněné zpoždění e-mailu při průchody servery a na obrázku č. 59 jsou vidět názvy a IP adresy serverů, přes které byl e-mail doručován.



Obrázek 58. Zpoždění e-mailu na serverech

Hop	From	By	With	Time (UTC)	Delay
1	[127.0.0.1] (localhost [127.0.0.1])	atlas.nimrodx.net (Postfix)	SMTP	02/28/2022 10:49:53 AM	0
2		atlas.nimrodx.net (Postfix, from userid 0)		02/28/2022 10:49:53 AM	0
3	atlas.nimrodx.net (mars.mpdn.net [217.155.16.33])	smtp-gw.utb.cz (Postfix)	ESMTP	02/28/2022 10:49:53 AM	0
4	smtp-gw.utb.cz (195.178.88.16)	VE1EUR01FT008.mail.protection.outlook.com (10.152.2.67)	Microsoft SMTP Server	02/28/2022 10:49:54 AM	1 sec
5	VE1EUR01FT008.eop-EUR01.prod.protection.outlook.com (2603:10a6:d10:1d:cafe::21)	FR3P281CA0010.outlook.office365.com (2603:10a6:d10:1d::9)	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)	02/28/2022 10:49:54 AM	0
6	FR3P281CA0010.DEUP281.PROD.OUTLOOK.COM (2603:10a6:d10:1d::9)	DB8PR10MB3481.EURPRD10.PROD.OUTLOOK.COM (2603:10a6:10:139::8)	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)	02/28/2022 10:49:55 AM	1 sec
7	DB8PR10MB3481.EURPRD10.PROD.OUTLOOK.COM (2603:10a6:10:139::8)	AM6PR10MB1910.EURPRD10.PROD.OUTLOOK.COM	HTTPS	02/28/2022 10:49:59 AM	4 sec

Obrázek 59. Cesta e-mailů při doručování

Informace získané z této e-mailové zprávy jsou uvedeny v tabulce č. 9

Tabulka 9. Data získaná z e-mailové zprávy

Odesílatel	fio.5d08dcbf@mail.www-ib-fio.cz

Název serveru	atlas.nimrodx.net(mars.mpdn.net)
IP adresa serveru	217.155.16.33
Odkaz z těla zprávy	http://www66.zajistit-fio-cz.com/6c32743c8fc440904fa73c34fd2f136d?=ok

5.2 Rozbor e-mailové adresy

E-mailová adresa, získaná z výše uvedené e-mailové zprávy, je postupně analyzována těmito nástroji, z tabulky č. 2: Trumail, Google, Carrot, EmailRep, Reverse Whois Lookup, HIBPW, PSBDMP, crt.sh, OTX, Threat Crowd. Výsledky takového hledání jsou ukázány v tabulce č. 10.

Tabulka 10. Výsledek šetření e-mailové adresy

Vstupní data	fio.5d08dcbf@mail.www-ib-fio.cz
Nástroj	Výsledek vyhledávání
Trumail	Nedoručitelná adresa, s neplatnou doménou.
Google	Vráceno několik článků s varováním na podvodné e-maily.
Carrot	Bez výsledku.
EmailRep	E-mailová adresa označena jako podezřelá.
Reverse Whois Lookup	Nebyla nalezena doména s touto e-mailovou adresou.
HIBPW	Nezjištěn výskyt této e-mailové adresy v únicích údajů.
PSBDMP	Bez výsledku.
crt.sh	Bez výsledku.
OTX	Bez výsledku.
Threat Crowd	Bez výsledku.

Závěr: Tuto e-mailovou adresu lze označit jako škodlivou, využívanou k phishingu.

5.3 Rozbor doménového jména

Doménové jméno, získané z odkazu ve výše uvedené e-mailové zprávě, je postupně analyzováno těmito nástroji, z tabulky č. 4: Google, Carrot, ICANN registration data lookup,

ViewDNS Reverse IP, ViewDNS IP History, WHOIS History Lookup, SecurityTrails, IP Location Finder, IP Lookup Tool, Netcraft Site Report, DNSDumpster, Certificate Search, AbuseIPDB, OTX, Threat Crowd, VirusTotal, Shodan. Výsledky tohoto hledání je zobrazen v tabulce č. 11.

Tabulka 11. Výsledek vyhledávání informací o doménovém jménu

Vstupní data	zajistit-fio-cz.com
Nástroj	Výsledek vyhledávání
Google	Nalezeny odkazy na stránky, kde je adresa označena jako phish a je zařazená do blacklistů spamových filtrů.
Carrot	Stejné výsledky jako Google.
ICANN registration data lookup	Nalezeny 2 DNS servery společnosti Cloudflare a informace o registrátorovy domény.
ViewDNS Reverse IP	Bez výsledku.
ViewDNS IP History	Bez výsledku.
WHOIS History Lookup	Nalezena země registrujícího subjektu, Bermudy a provincie Saskatchewan.
SecurityTrails	Bez výsledku.
IP Location Finder	Bez výsledku.
IP Lookup Tool	Bez výsledku.
Netcraft Site Report	Bez výsledku.
DNSDumpster	Bez výsledku.
Certificate Search	Nalezen 1 certifikát s SHA-1 otiskem 6C194B874E1C8BD7392BB7F8DE0DD7FFBA091CEB
AbuseIPDB	Bez výsledku.
OTX	Bez výsledku.
Threat Crowd	Bez výsledku.

VirusTotal	V 10 případech označena doména jako škodlivá. Nalezeno 25 subdomén, z toho 11 označených jako škodlivá. Nalezeny související IP adresy.
Shodan	Bez výsledku.

Závěr: Tuto doménu lze označit jako škodlivou, využívanou k phishingu a podvodům. Nalezeny subdomény a IP adresy vhodné k další analýze.

5.4 Rozbor IP adresy

V tomto případě je vyšetřována IP adresa 111.206.120.172. Tato adresa je postupně analyzována nástroji, které jsou uvedeny v tabulce č. 5. Jsou to nástroje: Google, Carrot, ICANN registration data lookup, ViewDNS Reverse IP, IP Location Finder, IP Lookup Tool, Netcraft Site Report, AbuseIPDB, OTX, Threat Crowd, VirusTotal, Shodan. Výsledek vyhledávání informací o IP adrese je ukázán v tabulce č. 12.

Tabulka 12. Výsledek vyhledávání informací o IP adrese

Vstupní data	111.206.120.172
Nástroj	Výsledek vyhledávání
Google	Nalezeno několik odkazů do reputačních databází.
Carrot	Podobné výsledky jako Google.
ICANN registration data lookup	Nalezeny e-maily, telefonní čísla a adresy v kontaktních údajích registrace.
ViewDNS Reverse IP	Bez výsledku.
IP Location Finder	Poloha IP adresy: Peking, Čína. Autonomní systém č. 4808. Poskytovatel připojení China Unicom Beijing Province Network.
IP Lookup Tool	Stejné výsledky jako u nástroje IP Location Finder.
Netcraft Site Report	Vysoká hodnota rizikového skóre.
AbuseIPDB	Nalezeno 5900 reportů. Hlášeny aktivity jako útok hrubou silou službou SSH, skenování portů.

OTX	Nalezeno 50 pulzů v souvislosti touto IP adresou.
Threat Crowd	IP adresa označena jako škodlivá.
VirusTotal	9 z 89 služeb označilo IP adresu jako škodlivou.
Shodan	Nalezeny otevřené porty 22 a 443 a webový server Nginx.

Závěr: Tuto IP adresu lze označit za škodlivou.

5.5 Rozbor uživatelského jména

Uživatelské jméno je získané z e-mailové adresy delmarharder@mailcatch.com, odesílatele e-mailové zprávy s vyděračským obsahem a je postupně analyzováno těmito nástroji, z tabulky č. 3: Google, Carrot, KnowEm, Instant Username Search, WhatsMyName, PSBDMP, Facebook, Twitter. Výsledky takového hledání jsou ukázány v tabulce č. 13.

Tabulka 13. Výsledek vyhledávání informací o uživateli

Vstupní data	delmarharder
Nástroj	Výsledek vyhledávání
Google	Bez výsledku.
Carrot	Bez výsledku.
Instant Username Search	Nalezeno 32 účtů, ale žádný účet ve skutečnosti neexistuje.
WhatsMyName	Nalezeno 187 účtů označených jako falešně pozitivní.
PSBDMP	Bez výsledku.
Facebook	Nalezen uživatel se jménem Delmar Harderway Harderway.
Twitter	Bez výsledku.

Závěr: Nebyly nalezeny další informace o daném uživateli. Byl zaznamenám výskyt jedné osoby s podobným uživatelským jménem na síti Facebook.

5.6 Rozbor kryptoměnové peněženky

Informace o bitcoinové peněžence, získané z těla vyděračského e-mailu, jehož část je ukázána na obrázku č. 60. Tato peněženka je analyzována pomocí nástroje Bitcoin Abuse Database. Výsledek takového hledání je uveden v tabulce č. 14.

Hereby, I believe by this time it is already clear for you why I was never detected until I sent this letter...

While compiling all the information related to you, I have also found out that you are a true fan and frequent visitor of adult websites.
You truly enjoy browsing through porn websites, while watching arousing videos and experiencing an unimaginable satisfaction.
To be honest, I could not resist but to record some of your kinky solo sessions and compiled them in several videos, which demonstrate you masturbating and cumming in the end.

If you still don't trust me, all it takes me is several mouse clicks to distribute all those videos with your colleagues, friends and even relatives.
In addition, I can upload them online for entire public to access.
I truly believe, you absolutely don't want such things to occur, bearing in mind the kinky stuff exposed in those videos that you usually watch, (you definitely understand what I am trying to say) it will result in a complete disaster for you.

We can still resolve it in the following manner:
You perform a transfer of $1590 USD to me (a bitcoin equivalent based on the exchange rate during the funds transfer), so after I receive the transfer, I will straight away remove all those lecherous videos without hesitation.
Then we can pretend like it has never happened before. In addition, I assure that all the harmful software will be deactivated and removed from all devices of yours. Don't worry, I am a man of my word.

It is really a good deal with a considerably low the price, bearing in mind that I was monitoring your profile as well as traffic over an extended period.
If you still unaware about the purchase and transfer process of bitcoins - all you can do is find the necessary information online.

My bitcoin wallet is as follows: 1GvxuP9puQCMNQvEKuwNrLeGwp9LWV4822

You are left with 48 hours and the countdown starts right after you open this email (2 days to be specific).

Obrázek 60. Úryvek vyděračského e-mailu.

Tabulka 14. Výsledek vyhledávání informací o kryptoměnové peněžence

Vstupní data	1GvxuP9puQCMNQvEKuwNrLeGwp9LWV4822
Nástroj	Výsledek vyhledávání
Bitcoin Abuse Database	Nalezeno 77 hlášení. Podle reportů je peněženka používána pro výkupné ransomware a podvodné jednání. Na peněžence je zaznamenána jedna transakce a příjem 0,0001 Bitcoinů.

Závěr: Tato bitcoinová peněženka je využívána k podvodnému jednání.

5.7 Rozbor certifikátu

V tomto případě je vyšetřováno sériové číslo SSL certifikátu z IP adresy 36.110.228.254, která je reportována v systému AbuseIPDB jako škodlivá. Toto číslo je postupně analyzováno nástroji, které jsou uvedeny v tabulce č. 7. Jsou to nástroje: Certificate Search, VirusTotal (vyhledávací modifikátor entity:domain ssl_serial: c04874568e14d74c), Shodan (vyhledávácí filtr ssl.cert.serial: c04874568e14d74c). Výsledek tohoto vyhledávání je zobrazen v tabulce č. 15.

Tabulka 15. Výsledek vyhledávání informací spojených s certifikátem

Vstupní data	c04874568e14d74c
Nástroj	Výsledek vyhledávání
Certificate Search	Bez výsledku.

VirusTotal	Bez výsledku.
Shodan	Nalezeno 92 IP adres a domén spojených s tímto číslem certifikátu.

Závěr: Bylo nalezeno mnoho IP adres a domén používající certifikát se stejným sériovým číslem. Nalezené domény a IP adresy jsou vhodné k další analýze.

5.8 Rozbor obrázku

V tomto případě byl vstupem obrázek č. 61, který pochází z aplikace Flickr. Postupně byl analyzován nástroji z tabulky č. 8. Jsou to nástroje ExifTool a TinEye. Výstup z aplikace ExifTool je ukázán na obrázku č. 62.

Obrázek 61. Fotografie domu [79]

Tabulka 16. Výsledek vyhledávání informací o obrázku

Vstupní data	Obrázek č. 61
Nástroj	Výsledek vyhledávání
ExifTool	Výsledek uveden na obrázku č. 62.
TinEye	Nalezeno 371 výskytů stejné fotografie na různých webech.

```
---- ExifTool ----
ExifTool Version Number         : 12.40
---- System ----
File Size                       : 653 KiB
Zone Identifier                 : Exists
File Modification Date/Time     : 2022:05:14 17:19:59+02:00
File Access Date/Time           : 2022:05:14 17:35:48+02:00
File Creation Date/Time         : 2022:05:14 17:19:58+02:00
---- File ----
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
Exif Byte Order                 : Big-endian (Motorola, MM)
Current IPTC Digest             : 5badcf9594a8dc66907320a8b1f243b0
Image Width                     : 2048
Image Height                    : 1536
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:2 (2 1)
---- IFD0 ----
Artist                          : Real Estate Photography
---- IPTC ----
Coded Character Set             : UTF8
Envelope Record Version         : 4
Application Record Version      : 4
Document Notes                  : https://flickr.com/e/jh5dN3itTde1ZhVZkxrb5eVMGcyApR4OvLy9rzBI13I%3D
City:Chicago, Country:USA, Address:Real Estate Photography,
PostalCode:, Region:Illinois, Email:, Phone:, URL:
By-line Title                   : Real Estate Photography
By-line                         : Real Estate Photography
Application Record Version      : 4
---- Composite ----
Image Size                      : 2048x1536
Megapixels                      : 3.1
```

Obrázek 62. Výstup z aplikace ExifTool

Závěr: Testovaný obrázek se vyskytuje na mnoha webových stránkách. Množství získaných metadat, je proti údajům uvedených na webové stránce této fotografie, značně omezené.

ZÁVĚR

Cílem této diplomové práce bylo popsat možnosti Open Source Intelligence, tedy zpravodajství z otevřených zdrojů, v současném Internetu.

Nejprve byly popsány principy OSINT, jaké druhy informací je možné takto získat a také jaké zdroje informací do této kategorie spadají. Také byly uvedeny důvody vzniku a vývoj získávání informací z volně přístupných zdrojů v historii.

Dále bylo zmapováno a popsáno zhruba 40 různých nástrojů OSINT používaných v současném Internetu. Nástroje jsou zde rozděleny do 14 kategorií dle druhů informací, které se těmito nástroji vyšetřují. Funkce zde uvedených nástrojů jsou také otestovány a jsou zobrazeny jejich výstupy.

Ve třetí kapitole je řešena problematika dostupnosti informací po zavedení nařízení GDPR. Stručně jsou zde popsána pravidla pro nakládání s osobními údaji a je zde popsána omezení z toho vyplývající.

Protože zdrojů s informacemi pro získávání informací existuje velké množství, je nutné postupovat systematicky. Ve čtvrté kapitole byla tedy vypracována metodika pro analýzu pomocí OSINT, se zaměřením na získávání informací vztahujících se ke kybernetické bezpečnosti. Toto byl hlavní cíl této práce.

V páté a poslední části diplomové práce byla navržená metodika otestována na konkrétních identifikátorech. Byly zaznamenány výsledky šetření u jednotlivých nástrojů a byly stanoveny závěry o povaze jednotlivých vstupných údajů. Bylo otestováno vyšetřování e-mailové adresy, doménového jména, IP adresy, uživatelského jména, kryptoměnové peněženky, digitálního certifikátu a obrázku.

Vzhledem k tomu, že v průběhu času uvedené nástroje mohou přestat být funkční anebo se naopak mohou na Internetu objevovat nástroje nové, nelze zde představenou metodiku považovat za konečnou. Je nezbytné sledovat trendy a vyhledávat další nástroje a zdroje, které činnost při vyšetřování ulehčují. Protože většina zde uvedených nástrojů nabízí možnost využití API, je také možné vytvořit počítačový program, který by mohl práci s nimi zjednodušit a zautomatizovat.

SEZNAM POUŽITÉ LITERATURY

[1] What is Intelligence? *Office of the Director of National Intelligence* [online]. [cit. 2022-02-27]. Dostupné z: https://www.dni.gov/index.php/what-we-do/what-is-intelligence

[2] GIBSON, Helen, 2016. Acquisition and Preparation of Data for OSINT Investigations. AKHGAR, Babak, P. Saskia BAYERL a Fraser SAMPSON, ed. *Open Source Intelligence Investigation* [online]. 1. Cham (Switzerland): Springer, s. 69-93 [cit. 2021-11-26]. ISBN 978-3-319-47671-1. Dostupné z: https://link.springer.com/content/pdf/10.1007%2F978-3-319-47671-1_6.pdf

[3] GIBSON, Helen, Steve RAMWELL a Tony DAY, 2016. Analysis, Interpretation and Validation of Open Source Data. AKHGAR, Babak, P. Saskia BAYERL a Fraser SAMPSON, ed. *Open Source Intelligence Investigation* [online]. 1. Cham (Switzerland): Springer, s. 95-110 [cit. 2021-11-26]. ISBN 978-3-319-47671-1. Dostupné z: https://link.springer.com/content/pdf/10.1007%2F978-3-319-47671-1_6.pdf

[4] UNGUREANU, Gabriel-traian, 2021. OPEN-SOURCE INTELLIGENCE (OSINT). THE WAY AHEAD. *Journal of Defense Resources Management* [online]. **12**(1), 177-200 [cit. 2021-11-25]. ISSN 20689403. Dostupné z: https://search.ebscohost.com/login.aspx?direct=true&db=edsdoj&an=edsdoj.5e414da202e414390b07033babae658&scope=site

[5] CHAUHAN, Sudhanshu a Nutan PANDA, 2015. *Hacking Web Intelligence*. Waltham (Massachusetts): Syngress. ISBN 978-0-12-801867-5.

[6] Google Hacking: What is a Google Hack? *Acunetix* [online]. c2022 [cit. 2022-03-06]. Dostupné z: https://www.acunetix.com/websitesecurity/google-hacking

[7] Google Hacking Database. *Exploit Database* [online]. c2022 [cit. 2022-03-07]. Dostupné z: https://www.exploit-db.com/google-hacking-database

[8] Carrot2 clustering engine. *Carrot2 search results clustering engine* [online]. [cit. 2022-03-07]. Dostupné z: https://search.carrot2.org/#/about

[9] GitHub - ElevenPaths/FOCA. *GitHub* [online]. c2022 [cit. 2022-03-08]. Dostupné z: https://github.com/ElevenPaths/FOCA

[10] ExifTool. *ExifTool* [online]. [cit. 2022-03-08]. Dostupné z: https://exiftool.org

[11] VIN Decoder & Lookup. *VINDecoderZ* [online]. c2022 [cit. 2022-03-09]. Dostupné z: https://www.vindecoderz.com

[12] VinCheck. *VinCheck* [online]. [cit. 2022-03-09]. Dostupné z: http://www.vincheck.cz

[13] HASSAN, Nihad A. a Rami HIJAZI, 2018. *Open Source Intelligence Methods and Tools*. 1. Berkeley, CA: Apress. ISBN 978-1-4842-3212-5.

[14] Support. *NerdyData* [online]. [cit. 2022-03-09]. Dostupné z: https://www.nerdydata.com/support

[15] About searchcode. *Searchcode* [online]. [cit. 2022-03-09]. Dostupné z: https://searchcode.com/about

[16] What is SymbolHound? *SymbolHound* [online]. [cit. 2022-03-09]. Dostupné z: http://symbolhound.com/about.php

[17] FAQs. *TinEye Reverse Image Search* [online]. c2022 [cit. 2022-03-10]. Dostupné z: https://tineye.com/faq#count

[18] Current Location. *Current Location* [online]. [cit. 2022-03-10]. Dostupné z: https://current-location.com

[19] Most used social media. *Statista* [online]. c2022 [cit. 2022-03-14]. Dostupné z: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users

[20] BAZZELL, Michael. *Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information.* 9th Ed. Wroclaw: Amazon, 2022. ISBN 9798794816983.

[21] *StalkFace* [online]. [cit. 2022-04-02]. Dostupné z: https://stalkface.com/en

[22] *All My Tweets* [online]. c2022 [cit. 2022-04-02]. Dostupné z: https://www.allmytweets.net

[23] *TweetBeaver* [online]. [cit. 2022-04-02]. Dostupné z: https://tweetbeaver.com

[24] *Trumail* [online]. c2018-2019 [cit. 2022-04-04]. Dostupné z: https://trumail.io

[25] API Documentation V3. *Capture Accurate Emails* [online]. c2009-2022 [cit. 2022-04-04]. Dostupné z: https://www.emailchecker.com/api-documentation-v3

[26] EmailRep API. *Simple Email Reputation* [online]. [cit. 2022-04-04]. Dostupné z: https://docs.sublimesecurity.com/docs/emailrep-api

[27] EmailRep Alpha Risk API. *GitHub* [online]. c2022, 7 May 2021 [cit. 2022-04-04]. Dostupné z: https://github.com/sublime-security/emailrep.io

[28] *MsgEml.com: free online .msg and .eml viewer* [online]. c2020 [cit. 2022-04-04]. Dostupné z: https://msgeml.com

[29] *Analyze my mail header* [online]. [cit. 2022-04-04]. Dostupné z: https://mailheader.org

[30] E-Mail Header Analyzer. *Gaijin.at* [online]. c2003-2022 [cit. 2022-04-04]. Dostupné z: https://www.gaijin.at/en/tools/e-mail-header-analyzer

[31] E-Mail Header Analyzer. *GitHub* [online]. c2022 [cit. 2022-04-05]. Dostupné z: https://github.com/cyberdefenders/email-header-analyzer

[32] About Knowem. *KnowEm Username Search* [online]. [cit. 2022-04-05]. Dostupné z: https://knowem.com/about-us.php

[33] Instant-username-search. *GitHub* [online]. c2022 [cit. 2022-04-05]. Dostupné z: https://github.com/instantusername/instant-username-search

[34] WhatsMyName. *GitHub* [online]. c2022 [cit. 2022-04-05]. Dostupné z: https://github.com/webbreacher/whatsmyname

[35] ICANN Lookup. *ICANN* [online]. [cit. 2022-04-06]. Dostupné z: https://lookup.icann.org

[36] Registration Data Access Protocol. *RIPE* [online]. 30 Jun 2021 [cit. 2022-04-06]. Dostupné z: https://www.ripe.net/manage-ips-and-asns/db/registration-data-access-protocol-rdap

[37] Reverse IP Lookup. *ViewDNS.info* [online]. c2022 [cit. 2022-04-06]. Dostupné z: https://viewdns.info/reverseip

[38] Reverse Whois Lookup. *ViewDNS.info* [online]. c2022 [cit. 2022-04-11]. Dostupné z: https://viewdns.info/reversewhois

[39] IP History. *ViewDNS.info* [online]. c2022 [cit. 2022-04-11]. Dostupné z: https://viewdns.info/iphistory

[40] Access domain name history with WHOIS History Lookup. *WhoisXML API* [online]. c2014-2022 [cit. 2022-04-11]. Dostupné z: https://whois-history.whoisxmlapi.com/lookup

[41] Best JSON Viewer and JSON Beautifier Online. *Code Beautify and Formatter For Developers* [online]. c2022 [cit. 2022-04-12]. Dostupné z: https://codebeautify.org/jsonviewer

[42] WHOIS. *SecurityTrails* [online]. c2022 [cit. 2022-04-11]. Dostupné z: https://docs.securitytrails.com/reference/history-whois

[43] *Where is my IP location?* [online]. c2006-2022 [cit. 2022-04-13]. Dostupné z: https://www.iplocation.net

[44] *IP2Location* [online]. c2001-2022 [cit. 2022-04-13]. Dostupné z: https://www.ip2location.com

[45] *Comprehensive IP address data, IP geolocation API and database* [online]. c2022 [cit. 2022-04-13]. Dostupné z: https://ipinfo.io

[46] *IP Geolocation API* [online]. c2022 [cit. 2022-04-13]. Dostupné z: https://db-ip.com

[47] *The Trusted Source for IP Address Data* [online]. c2019-2021 [cit. 2022-04-13]. Dostupné z: https://ipregistry.co

[48] *Free IP Geolocation API and Accurate IP Geolocation Database* [online]. c2022 [cit. 2022-04-13]. Dostupné z: https://ipgeolocation.io

[49] *Ipapi - IP Address Lookup and Geolocation API* [online]. c2016-2022 [cit. 2022-04-13]. Dostupné z: https://ipapi.co

[50] *IP Geolocation AP* [online]. [cit. 2022-04-13]. Dostupné z: https://ipdata.co

[51] *IP Address Lookup* [online]. c2015-2022 [cit. 2022-04-13]. Dostupné z: https://iplocation.io

[52] What's that site running? *Netcraft* [online]. c1995-2022 [cit. 2022-04-14]. Dostupné z: https://sitereport.netcraft.com

[53] *DNSdumpster.com: dns recon and research, find and lookup dns records* [online]. c2019 [cit. 2022-05-11]. Dostupné z: https://dnsdumpster.com

[54] FAQs. *Have I Been Pwned* [online]. [cit. 2022-04-15]. Dostupné z: https://haveibeenpwned.com/FAQs

[55] *Psbdmp* [online]. [cit. 2022-04-15]. Dostupné z: https://psbdmp.ws

[56] *Pastebin.com* [online]. c2022 [cit. 2022-04-15]. Dostupné z: https://pastebin.com

[57] About IA. *Internet Archive* [online]. [cit. 2022-04-15]. Dostupné z: https://archive.org/about

[58] Frequently Asked Questions. *Bitcoin Abuse Database* [online]. c2022 [cit. 2022-04-16]. Dostupné z: https://www.bitcoinabuse.com/faq

[59] *Crt.sh: Certificate Search* [online]. c2015-2022 [cit. 2022-04-16]. Dostupné z: https://crt.sh

[60] About - AbuseIPDB. *AbuseIPDB* [online]. c2022 [cit. 2022-04-16]. Dostupné z: https://www.abuseipdb.com/about.html

[61] Open Threat Exchange (OTX). *AlienVault is now AT&T Cybersecurity* [online]. c2022 [cit. 2022-04-17]. Dostupné z: https://cybersecurity.att.com/open-threat-exchange

[62] *Threat Crowd* [online]. c2022 [cit. 2022-04-19]. Dostupné z: https://www.threatcrowd.org

[63] How it works. *VirusTotal* [online]. [cit. 2022-04-17]. Dostupné z: https://support.virustotal.com/hc/en-us/articles/115002126889-How-it-works

[64] Uncovering threat infrastructure via URL, domain and IP address advanced pivots a.k.a. Netloc Intelligence. *VirusTotal* [online]. c2022, FEBRUARY 26, 2020 [cit. 2022-04-17]. Dostupné z: https://blog.virustotal.com/2020/02/uncovering-threat-infrastructure-via.html

[65] VirusTotal Intelligence Introduction. *VirusTotal* [online]. [cit. 2022-04-19]. Dostupné z: https://support.virustotal.com/hc/en-us/articles/360001387057-VirusTotal-Intelligence-Introduction

[66] What is Shodan. *Shodan Search Engine* [online]. [cit. 2022-04-19]. Dostupné z: https://help.shodan.io/the-basics/what-is-shodan

[67] Filter Reference. *Shodan Search Engine* [online]. [cit. 2022-04-20]. Dostupné z: https://www.shodan.io/search/filters

[68] Intelowlproject/IntelOwl. *GitHub* [online]. c2022 [cit. 2022-04-17]. Dostupné z: https://github.com/intelowlproject/IntelOwl

[69] Documentation. *SpiderFoot* [online]. c2022 [cit. 2022-04-17]. Dostupné z: https://www.spiderfoot.net/documentation

[70] Co je GDPR - Ochrana osobních údajů. *Ministerstvo vnitra České republiky* [online]. c2022 [cit. 2022-04-26]. Dostupné z: https://www.mvcr.cz/gdpr/clanek/co-je-gdpr.aspx

[71] EVROPSKÁ UNIE. NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679. In: *Úřední věstník Evropské unie.* 2016. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016R0679&from=CS

[72] GDPR essentials for OSINT research. *Blockint* [online]. July 28, 2021 [cit. 2022-04-26]. Dostupné z: https://www.blockint.nl/methods/gdpr-essentials-for-osint-research

[73] Data Protection and Privacy Issues. *ICANN* [online]. [cit. 2022-04-28]. Dostupné z: https://www.icann.org/dataprotectionprivacy

[74] Advisory Statement: Temporary Specification for gTLD Registration Data. In: *ICANN* [online]. [cit. 2022-04-28]. Dostupné z: https://www.icann.org/en/system/files/files/advisory-statement-gtld-registration-data-specs-17may18-en.pdf

[75] Sdružení CZ.NIC mění pravidla pro službu WHOIS. *CZ.NIC* [online]. c2022, 16.05.2018 [cit. 2022-04-28]. Dostupné z: https://www.nic.cz/page/3782/sdruzeni-cznic-meni-pravidla-pro-sluzbu-whois

[76] Často kladené dotazy. *CZ.NIC* [online]. c2022 [cit. 2022-04-28]. Dostupné z: https://www.nic.cz/page/383/casto-kladene-dotazy/#faq17

[77] TLDs that do not support Whois Privacy. *Name.com* [online]. c2001-2022, Jan 24, 2022 [cit. 2022-04-28]. Dostupné z: https://www.name.com/support/articles/205188698-TLDs-that-do-not-support-Whois-Privacy

[78] 25 Biggest GDPR Fines To-Date. *Tessian* [online]. 27 January 2022 [cit. 2022-04-28]. Dostupné z: https://www.tessian.com/blog/biggest-gdpr-fines-2020

[79] 9333857345_227b7020bf_k.jpg (2048×1536). In: *Flickr* [online]. [cit. 2022-05-14]. Dostupné z: https://live.staticflickr.com/3733/9333857345_227b7020bf_k.jpg

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

API	Application Programming Interface
DNS	Domain Name Server
ETL	Extract Transform Load
EXIF	Exchangeable Image File Format
FOCA	Fingerprinting Organizations with Collected Archives
GDPR	General Data Protection Regulation
GPS	Global Positioning System
gTLD	generic Top Level Domain
ICANN	Internet Corporation for Assigned Names and Numbers
IDS	Intrusion Detection System
IP	Internet Protocol
IPTC	International Press Telecommunications Council
ISO	International Organization for Standardization
JFIF	JPEG File Interchange Format
JPEG	Joint Photographic Experts Group
JSON	JavaScript Object Notation
MISP	Malware Information Sharing Platform
OSINT	Open Source Intelligence
OTX	Open Threat Exchange
RDAP	Registration Data Access Protocol
RFC	Request for Comments
SEM	Security Event Management
SIM	Security Information Management
SIEM	Security Information and Event Management

SFC	Suffix Tree Clustering
SOCMINT	Social Media Intelligence
SSH	Secure Shell
SSL	Secure Sockets Layer
TLS	Transport Layer Security
URL	Uniform Resource Locator
VIN	Vehicle Identification Number
XMP	Extensible Metadata Platform

SEZNAM OBRÁZKŮ

Obrázek 1. Výsledek vyhledávání intitle:"index of" "users.sql" 15
Obrázek 2. Obsah stránky nalezený pomocí Google hacking 15
Obrázek 3. Kategorie výsledků vyhledávání 16
Obrázek 4. Grafické znázornění shluků vyhledávače Carrot2 16
Obrázek 5. Výsledek vyhledávání aplikace FOCA 17
Obrázek 6. Metadata získaná aplikací ExifTool 18
Obrázek 7. Údaje o vozidle z aplikace VINDecoderZ 18
Obrázek 8. Data z aplikace VinCheck 19
Obrázek 9. Výsledky aplikace NerdyData 19
Obrázek 10. Výsledek hledání řetězce „i++;“ aplikací Searchcode 20
Obrázek 11. Výsledek hledání řetězce „i++;“ aplikací SymbolHound 20
Obrázek 12. Vyhledávání obrázku nástrojem TinEye 21
Obrázek 13. Vyhledávání v aplikaci Current Location 21
Obrázek 14. Příspěvky uživatele 23
Obrázek 15. Fotografie uživatele 23
Obrázek 16. Příspěvek uživatele vyhledaný na základě klíčového slova 24
Obrázek 17. Fotografie uživatele vyhledané na základě klíčového slova 24
Obrázek 18. Chyba vyhledávání v aplikaci StalkFace 25
Obrázek 19. Výsledek hledání v aplikaci All My Tweets 26
Obrázek 20. Výsledek hledání údajů k účtu v aplikaci TweetBeaver 27
Obrázek 21. Hledání ve službě Trumail 28
Obrázek 22. Zobrazení informací pomocí služby EmailRep 28
Obrázek 23. Informace z hlavičky e-mailu získané v aplikaci Mailheader 29
Obrázek 24. Informace z hlavičky e-mailu získané v aplikaci Mailheader 29
Obrázek 25. Informace z hlavičky e-mailu získané v aplikaci Mailheader 30
Obrázek 26. Informace získané z aplikace KnowEm 31
Obrázek 27. Výsledek hledání v aplikaci Instant Username Search 31
Obrázek 28. Výsledek hledání v aplikace WhatMyName 32
Obrázek 29. ICANN registration data 33
Obrázek 30. Výsledek dotazu na doménu „seznam.cz“ 33
Obrázek 31. Domény registrované subjektem „UTB-CZ“ 34
Obrázek 32. IP adresy, na kterých byla hostována doména „utb.cz“ 34

Obrázek 33. Výsledek hledání v aplikaci WHOIS History Lookup 35
Obrázek 34. Registrační údaje domény „utb.cz“ 35
Obrázek 35. Údaje o poloze IP adresy 195.178.88.109 36
Obrázek 36. Údaje o poloze IP adresy 195.178.88.109 37
Obrázek 37. Informace o stránkách utb.cz získané ve službě Netcraft Site Report ... 37
Obrázek 38. Informace o stránkách utb.cz získané ve službě Netcraft Site Report ... 38
Obrázek 39. Výsledek vyhledávání ve službě Google 39
Obrázek 40. E-mailové adresy nalezené na stránce pastebin.com 39
Obrázek 41. Obsah webových stránek „utb.cz/fai“ ze snímku z 1. 5. 2013 40
Obrázek 42. Report z aplikace Bitcoin Abuse Database 40
Obrázek 43. Výsledek vyhledávání v aplikaci Certificate Search 41
Obrázek 44. Výsledek vyhledávání IP adresy 92.255.85.237 ve službě AbuseIPDB 42
Obrázek 45. Přehled analýzy ve službě OTX 43
Obrázek 46. Související URL adresy vyhledané ve službě OTX 43
Obrázek 47. Vyhledané domény související s hledaným výrazem 43
Obrázek 48. Výsledek dotazu na vazby domény „utb.cz“ v aplikaci Threat Crowd .. 44
Obrázek 49. Vyhledávání domén se jmenným serverem „sun.utb.cz“ 45
Obrázek 50. Vyhledávání domén používajících stejný certifikát 45
Obrázek 51. Výsledek hledání ve službě Shodan 46
Obrázek 52. Souhrn provedené analýzy domény „utb.cz“ 46
Obrázek 53. Detail konkrétní analýzy domény „utb.cz“ 47
Obrázek 54. Historické registrační údaje domény „mvcr.cz“ 49
Obrázek 55. Aktuální registrační údaje domény „mvcr.cz“ 50
Obrázek 56. Extrakce dat z e-mailové zprávy 53
Obrázek 57. Extrakce dat ze souboru 54
Obrázek 58. Zpoždění e-mailu na serverech 59
Obrázek 59. Cesta e-mailů při doručování 59
Obrázek 60. Úryvek vyděračského e-mailu. 64
Obrázek 61. Fotografie domu [79] 65
Obrázek 62. Výstup z aplikace ExifTool 66

SEZNAM TABULEK

Tabulka 1. Operátory vyhledávání Google hacking 14
Tabulka 2. Nástroje pro analýzu e-mailové adresy.....55
Tabulka 3. Nástroje pro analýzu uživatelského jména 55
Tabulka 4. Nástroje pro analýzu doménového jména.....56
Tabulka 5. Nástroje pro analýzu IP adresy 57
Tabulka 6. Nástroje pro kryptoměnové peněženky 57
Tabulka 7. Nástroje pro analýzu certifikátu.....57
Tabulka 8. Nástroje pro analýzu obrázků 58
Tabulka 9. Data získaná z e-mailové zprávy 59
Tabulka 10. Výsledek šetření e-mailové adresy 60
Tabulka 11. Výsledek vyhledávání informací o doménovém jménu 61
Tabulka 12. Výsledek vyhledávání informací o IP adrese 62
Tabulka 13. Výsledek vyhledávání informací o uživateli 63
Tabulka 14. Výsledek vyhledávání informací o kryptoměnové peněžence 64
Tabulka 15. Výsledek vyhledávání informací spojených s certifikátem 64
Tabulka 16. Výsledek vyhledávání informací o obrázku 65

SEZNAM PŘÍLOH

Příloha PI: CD-ROM

PŘÍLOHA P I: CD-ROM

Struktura disku:

fulltext.pdf: text této diplomové práce ve formátu PDF.

prilohy.zip: ZIP archiv s instalačními soubory programu FOCA v. 3.4.7.1. a Exif-Tool v. 12.41.