POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostně právní

Katedra informačních technologií

Open source analýza digitálních stop

Bakalářská práce

Open source analysis of digital traces

Bachelor thesis

VEDOUCÍ PRÁCE
RNDr. Václav HNÍK, CSc.

AUTOR PRÁCE
Max LAGRON

PRAHA
2022

Prohlášení

Prohlašuji, že předložená práce je mým původním autorským dílem, které jsem vypracoval samostatně. Veškerou literaturu a další zdroje, z nichž jsem čerpal, v práci řádně cituji a jsou uvedeny v seznamu použité literatury.

V Praze, dne 15. 03. 2022

…….
Max Lagron

ANOTACE

Tématem bakalářské práce je *„open source analýza digitálních stop“*. Práce se dělí na teoretickou a praktickou část, přičemž teoretická část čítá čtyři kapitoly a praktická tři kapitoly. V teoretické části je vysvětleno, co je to analýza a jaké druhy analýzy známe, co je open source a jaká kritéria musí splňovat, jak probíhá přenos dat v internetu a co jsou síťové protokoly, co jsou digitální stopy, jak je klasifikujeme, jaké jsou jejich vlastnosti, využití a jak bývají zneužívány. Praktická část práce staví na poznatcích obsažených v teoretické části a na názorném příkladu popisuje postup, jak odposlouchávat Wi-Fi síť a zachytávat z ní data za pomoci open source softwaru. Završení praktické části spočívá v analýze digitálních stop obsažených v odchycených datech z bezdrátové sítě.

KLÍČOVÁ SLOVA

Digitální stopa * osobní údaje * data * internet * síť * síťový protokol * odposlech sítě * kyberkriminalita * open source

ANNOTATION

The topic of this bachelor thesis is *„open source analysis of digital traces“*. The thesis is divided into theoretical and practical part, while the theoretical part consists of four chapters and practical part of three chapters. The theoretical part explains what is analysis and what types of analysis we distinguish, what is open source and what criteria it must meet, how data are transferred throught the internet and what are network protocols, what are digital traces, how we classify them, what are their properties, utilization and how are being misused. The practical part of the thesis builds on the knowledge contained in the theoretical part and on an illustrative example describes the procedure how to eavesdrop on a Wi-Fi network and capture data from it using open source software. The conclusion of practical part lies in analysis of digital traces contained in captured data from the wireless network.

KEYWORDS

Digital trace * personal data * data * internet * network * network protocol * network eavesdropping * cybercrime * open source

Obsah

Úvod

Šíření povědomí o digitálních stopách, a obecně o bezpečném používání internetu, je s rozvojem informačních technologií stále důležitějším posláním. Na digitálních stopách v dnešní době vydělávají technologické společnosti nemalé peníze, a to samé se dá říct i kyberzločincích, kteří je nelegálně využívají k páchání trestné činnosti. Spousta lidí si v dnešní době neuvědomuje, kolik dat po sobě zanechává v kyberprostoru, a že se na nich někdo může obohatit, i na jejich úkor. Klíčem k ochraně svých dat je využívání bezpečných technologií, a především znalost rizik, které se na internetu skrývají.

Cílem této práce je vysvětlit čtenáři, co jsou to digitální stopy, jaké digitální stopy za sebou můžeme zanechat při používání internetu, jak funguje přenos dat v internetu, a jak přenos dat v internetu lze sledovat. Práce je rozdělena na teoretickou a praktickou část. Teoretická část pojednává o analýze, open source, přenosu dat v internetu a o digitálních stopách. V praktické části práce je pak vysvětlen postup odposlouchávání bezdrátových sítí, a na příkladu je ukázáno, jaká data lze zachytit z komunikace nezabezpečeného aplikačního protokolu HTTP.

Teoretická část

1 Analýza

Analýza je obecně teoretická vědní metoda, spočívající v rozložení většího celku na jednotlivé části. Jde tedy o metodu zkoumající složitější celky rozkladem na jednodušší, elementární části.

Cílem analýzy je rozpoznat klíčové vlastnosti elementárních částí a poznat jejich podstatu, vlastnosti, zákonitosti a vzájemné vztahy. Rovněž umožňuje oddělit podstatné od nepodstatného, odlišit trvalé vztahy od nahodilých. Analýza může být také způsob výkladu, pokud od sebe oddělíme jednotlivé jevy a popisujeme je zvlášť.[1]

Analýzu dále můžeme rozlišit podle jejího zaměření na:[2]

- **Klasifikační analýzu** – rozkládá zkoumaný jev či objekt do jednotlivých tříd, prvků s případným znovuseskupením do jiných tříd a množin.
- **Vztahovou analýzu** – zjišťuje, zda vztahy mezi jevy či objekty jsou závislé, či nezávislé.
- **Kauzální analýzu** – zaměřuje se na příčiny jevů.
- **Systémovou analýzu** – zkoumá jevy či objekt s cílem pochopit je a vysvětlit.

Opakem analýzy je syntéza, což je metoda, která z jednodušších částí skládá celky. Syntéza a analýza sice jsou protikladné metody, ale ve skutečnosti se vzájemně doplňují, proto se také někdy souhrnně nazývají analyticko-syntetickými poznávacími postupy.[3]

„Produktem analýzy je popis skutečnosti, syntéza podává její vysvětlení. Při analýze jednotlivá fakta konstatujeme, syntézou docházíme k jejich pochopení“.[4]

[1] DANEL, Roman. *Analýza projektování systémů* [online]. Ostrava, 2014. E-learningová podpora. Vysoká škola báňská – Technická univerzita Ostrava, Hornicko-geologická fakulta [cit. 16.1.2022]. Dostupné z: https://homel.vsb.cz/~dan11/aps/texty/INOHGF_EL_APS_DANEL.pdf
[2] DOLEŽALOVÁ, Stanislava. *Metodologie vědy, vědecké metody a metodika práce* [online]. [cit. 16.1.2022]. Dostupné z: https://docplayer.cz/7963823-2-metodologie-vedy-vedecke-metody-a-metodika-prace.html
[3] *tamtéž*
[4] ČÍŽEK, František a kol. *Filosofie, metodologie, věda*. 1. vyd. Praha: Svoboda, 1969, str. 53.

2 Open source

Open source[5] je počítačový software s otevřeným zdrojovým kódem. Otevřenost zdrojového kódu znamená jak technickou dostupnost, tak legální dostupnost – licenci softwaru. Licence udává, jaká práva k open source softwaru uživatel získává, a jak s ním může nakládat. Některé licence kupříkladu dovolují uživatelům upravovat zdrojový kód a software dál šířit, na rozdíl od komerčního softwaru s uzavřeným zdrojovým kódem.[6]

Aby mohl být software označený jako open source, musí podle skupiny Open Source Initiative (OSI) splňovat několik předpokladů:[7]

- **Volná redistribuce** – licence by neměla omezovat jakoukoli stranu v úplatné či bezúplatné distribuci softwaru, a tato další distribuce nesmí být podmíněna povinností platit licenční poplatky. Licence dále nesmí omezovat možnost distribuce open source softwaru jako součást jiného programu.
- **Zdrojový kód** – program musí obsahovat otevřený zdrojový kód a umožňovat další distribuci s otevřeným zdrojovým kódem. Ten musí být poskytnut v srozumitelné, modifikovatelné formě.
- **Odvozená díla** – licence by měla umožňovat modifikaci open source softwaru a distribuci takto modifikovaného softwaru za stejných podmínek jako v případě původní verze programu.
- **Integrita zdrojového kódu autora** – licence může omezit distribuci modifikovaného zdrojového kódu v případě, že je společně se zdrojovým kódem originální verze open source softwaru umožněno distribuovat „*patch files*“, které modifikují zdrojový kód během kompilace (spuštění) programu. Licence může dále vyžadovat, aby modifikovaná verze programu byla označena jiným jménem nebo verzí než původní verze programu.

[5] *„Open source“* – v českém překladu *„otevřený zdroj“*.
[6] Otevřený software. *Wikipedia* [online]. 6.2.2022. [cit. 22.1.2022]. Dostupné z: https://cs.wikipedia.org/wiki/Otev%C5%99en%C3%BD_software
[7] The Open Source Definition. *Opensource* [online]. 22.3.2007. [cit. 22.1.2022]. Dostupné z: https://opensource.org/osd

- **Zákaz diskriminace osob či skupin** – licenční podmínky nesmí diskriminovat jakoukoli osobu, nebo skupinu osob.
- **Zákaz diskriminace podle oboru činnosti** – licenční podmínky nesmí bránit použití open source softwaru v určitých oblastech lidské činnosti (například v businessu, genetickém výzkumu atd.).
- **Distribuovatelná licence** – práva a povinnosti vyplývající z licenčních podmínek musejí být aplikovatelné na všechny subjekty, jimž je program redistribuován, a to bez nutnosti uzavírání dalších smluv těmito subjekty.
- **Licence nesmí být určena pro specifický produkt** – práva náležící k programu nesmí být omezena na distribuci, které je open source software součástí. Všichni nabyvatelé licence musí mít stejná práva a povinnosti bez ohledu na to, zdali je open source software distribuován společně s jiným softwarem či nikoli.
- **Licence nesmí omezovat ostatní software v distribuci** – licenční podmínky nesmí nijak omezovat podmínky užití ostatního software, který je distribuovaný společně s licencovaným open source programem. Licence kupříkladu nesmí vynucovat, aby všechny ostatní programy v distribuci byly open source softwarem.
- **Technologicky neutrální licence** – žádné ustanovení v licenčních podmínkách nesmí být závislé na určité technologii, stylu, nebo rozhraní.

V běžné řeči se označení *„open source“* používá i pro řadu vlastností, které s otevřeností zdrojového kódu sice nesouvisí, ale poměrně běžně se u open source programů vyskytují. Může jít například o bezplatnou dostupnost softwaru, vývoj zajištěný dobrovolnickou komunitou, či nekomerčnost.

V posledních letech se podle odborníků stal open source zdrojem inovací v IT[8] a předčil tak proprietární software.[9] Rovněž vzrostl zájem firem o open source zejména v oblasti webových řešení.[10]

[8] *„IT“* – anglicky *„information technology“*, v českém překladu *„informační technologie“*.
[9] *„Proprietární software“* – software s uzavřeným zdrojovým kódem.
[10] PASTUCHOVÁ, Markéta. Open source přebírá v oblasti softwaru klíčovou roli. *ICT manažer* [online]. 5.11.2011. [cit. 30.1.2022]. Dostupné z archivu: https://web.archive.org/web/20120111073224/http://www.ictmanazer.cz/2011/11/open-source-prebira-v-oblasti-softwaru-klicovou-roli/

3 Přenos dat v internetu

3.1 Internet

Internet je celosvětový systém vzájemně propojených počítačových sítí, ve kterém mezi sebou počítače komunikují pomocí síťových protokolů.[11] Internet umožňuje sdílení, komunikaci, přístup k informacím a fungování celé řady síťových služeb.[12]

Počítačovou síť chápejme jako *„soubor (množinu) počítačových systémů, které jsou navzájem propojeny a mezi nimiž dochází k výměně dat či informací“*.[13]

Nejznámější internetovou službou je WWW,[14] která slouží k prohlížení, ukládání a odkazování se na webové stránky umístěné na internetu. Každá tato stránka má svojí webovou adresu, tzv. URL,[15] která udává místo umístění webového serveru[16] v internetu. Pro navštívení webové stránky je třeba zadat tuto URL do webového prohlížeče, což je software, jehož primárními funkcemi je zajištění komunikace s webovým serverem a vykreslení (renderování) webové stránky do uživatelsky přívětivé podoby.

Základní vlastnosti internetu:[17]

- Z hlediska velikosti je označován jako GAN (anglicky *„Global Area Network“*), tedy jako celosvětová síť, která vznikla propojením ostatních menších sítí.
- Internet nemá jednoho vlastníka.

[11] *„Síťový protokol“* – standard, podle kterého probíhá elektronická komunikace a přenos dat.
[12] *Internet* [online]. [cit. 30.1.2022]. Dostupné z: https://www.ssph.cz/vyuka/wp-content/uploads/2020/03/psi-internet.pdf
[13] KOLOUCH, Jan. *Cybercrime*. 1. vyd. Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8, str. 67.
[14] *„WWW“* – anglicky „*World Wide Web*“, v českém překladu „***celosvětová síť***“.
[15] *„URL“* – anglicky *„Uniform Resource Locator“*, v českém překladu *„jednotný lokátor zdroje“*.
[16] *„Server“* – počítač, který poskytuje nějaké služby, nebo počítačový program, který tyto služby realizuje. Webový server je server, který poskytuje požadovaný webový obsah (například webovou stránku).
[17] *Internet* [online]. [cit. 30.1.2022]. Dostupné z: https://www.ssph.cz/vyuka/wp-content/uploads/2020/03/psi-internet.pdf

- Všechny síťové uzly[18] připojené k internetu používají ke komunikaci síťový protokol TCP/IP.
- Propojení mezi jednotlivými sítěmi jsou uskutečněna za pomoci routerů, které provádějí směrování (routing) jednotlivých datových paketů.[19]
- Pro identifikaci síťového zařízení se používá IP adresa.[20]
- Většina služeb na internetu je založena na architektuře klient – server, tedy na stavu, kdy klient (např. webový prohlížeč) zahajuje komunikaci se serverem, server poskytuje své služby na žádosti klienta a řídí přístup k datovému obsahu podle práv, které klient vlastní.
- Internet nemá žádný síťový uzel, který je možný zničit a tím vyřadit z provozu celou síť.
- Spoje mezi síťovými uzly jsou realizovány vícero cestami. V případu výpadku jednoho spoje může router směrovat komunikaci jinými cestami.

3.1.1 Struktura internetu

Základním stavebním prvkem internetu jsou jednotlivé LAN[21] a WLAN[22] sítě, které propojují jednotlivá koncová zařízení (PC, mobily, tiskárny). Vlastníkem LAN bývají domácnosti, instituce, firmy atd. Tyto sítě se pak sdružují do větších celků a tím vznikají sítě MAN[23] a WAN.[24]

WAN sítě nejsou omezené konkrétním územím. Tyto sítě můžou existovat na území kraje, státu, kontinentu atd., může se jednat o propojení všech sítí uvnitř státu, všech poboček a sídel mezinárodní organizace atd.

Základní architekturu internetu tvoří dvě komponenty: routery a datové spoje.

[18] *„Síťový uzel“* – označení pro zařízení v počítačových sítích, které slouží k jejich propojování nebo jako koncový bod.
[19] *„Paket“* – balíček dat.
[20] *„IP adresa“* – číslo, které jednoznačně identifikuje zařízení v koncové síti.
[21] *„LAN“* – anglicky „*Local Area Network*“, v českém překladu *„místní počítačová síť“*.
[22] *„WLAN“* – anglicky „*Wireless Local Area Network*“, v českém překladu *„bezdrátová místní počítačová síť“*.
[23] *„MAN“* – anglicky „*Metropolitan Area Network*“, v českém překladu „*metropolitní počítačová síť*“.
[24] *„WAN“* – anglicky „*Wide Area Network*“, v českém překladu „*rozlehlá počítačová síť*“.

- **Router** je síťové zařízení, jehož úkolem je dopravit data v podobě datových paketů na správné cílové zařízení v síti.
- **Datové spoje** jsou technologie a síťové standardy, které slouží k fyzickému spojení jednotlivých sítí. Jde například o optické a metalické pevné spoje, telefonní sítě, bezdrátové spoje, družicové spoje.

3.2 TCP/IP protokol

Jak již bylo zmíněno, v internetu mezi sebou zařízení komunikují pomocí síťového protokolu TCP/IP. Síťovým protokolem rozumíme soustavu předpisů, definující pravidla pro spolupráci dvou sítí.[25] Jde tedy o standard, který předepisuje, jak má probíhat komunikace mezi zařízeními. Protokol TCP/IP však není pouze jeden protokol, jedná se o sadu protokolů, kterým se také někdy říká *„rodina protokolů TCP/IP“*.

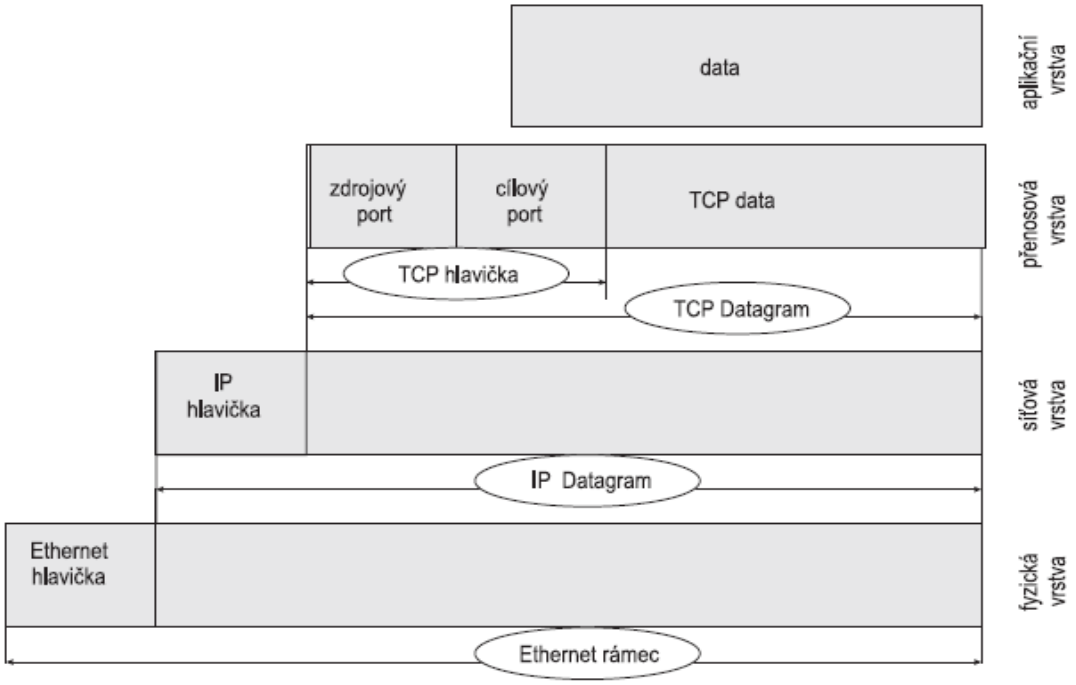
Z funkčního hlediska lze TCP/IP rozdělit do čtyř vrstev:[26]

- **Aplikační vrstvu** – aplikační protokoly, které jsou reprezentované jednotlivými porty.
- **Transportní vrstvu** – protokoly TCP a UDP.
- **Síťovou vrstvu** – protokoly IP.
- **Fyzickou vrstvu** – provádí fyzický přenos dat.

Spolupráce mezi vrstvami probíhá zhruba následovně: program na jednom počítači potřebuje navázat spojení s jiným zařízením v síti. K tomu využije aplikační vrstvu, ze které putuje požadavek na spojení do transportní vrstvy. Ta zajistí organizaci dopravy dat (rozdělí data do jednotlivých segmentů, naváže spojení, a kontroluje přenos dat). Odeslání dat zajišťuje síťová vrstva, která zabalí segmenty obdržené od nadřazené vrstvy do datagramů a odešle přes nejnižší – fyzickou vrstvu do cílového zařízení.[27]

[25] HORÁK, Jaroslav. *Bezpečnost malých počítačových sítí*. 1. vyd. [Praha]: Grada, 2003. ISBN 80-247-0663-6, str. 106.
[26] *tamtéž*
[27] *tamtéž*

Schéma vrstev protokolu TCP/IP můžeme vidět na obrázku 1.[28]



Obrázek 1 - Schéma vrstev protokolu TCP/IP

3.2.1 Aplikační vrstva

Aplikační vrstva je tvořena sadou protokolů určených ke spolupráci mezi jednotlivými programy (aplikacemi). Tyto protokoly udávají, jakým způsobem spolu mají jednotlivé aplikace komunikovat, aby si rozuměly. Například všechny webové servery komunikují s klientem prostřednictvím HTTP protokolu, nehledě na to, že jsou jich miliony, poskytují různé služby, a běží na rozdílných platformách.[29]

Aplikačních protokolů je celá řada, proto musí při přenosu dat transportní vrstva definovat, jakým protokolem aplikační vrstvy chce komunikovat. Z toho důvodu jsou mezi aplikační a transportní vrstvu vloženy síťové porty.[30]

3.2.1.1 Síťový port

Každý síťový port má svoje číslo a reprezentuje komunikační rozhraní určitého aplikačního protokolu (některé porty jsou neobsazené).

[28] HORÁK, Jaroslav. *Bezpečnost malých počítačových sítí*. 1. vyd. [Praha]: Grada, 2003. ISBN 80-247-0663-6, str. 106.
[29] *tamtéž*
[30] *tamtéž*

Označením síťového portu je šestnáctibitové číslo z intervalu 1-65535, které využívají protokoly transportní vrstvy pro identifikaci služeb (a jejich prostřednictví aplikací) na určitém zařízení. Každá aplikace je jednoznačně identifikována číslem portu, jeden port tedy představuje jednu aplikaci.[31]

Tabulka 1[32] umístěná pod textem obsahuje přehled nejvyužívanějších síťových portů, včetně aplikačních protokolů, ke kterým náleží.

Tabulka 1 - Běžně využívané síťové porty.

Port	Protokol	Popis
21, 20	FTP, FTP – data	Přenos souborů (řídící a datové spojení)
22	SSH	Secure shell – šifrovaná obdoba protokolu telnet, přenosy souborů, forwardování portů
23	Telnet	Vzdálený textový terminál – nešifrovaná komunikace
25	SMTP	Simple Mail Transfer Protocol – přenos elektronické pošty
53	DNS	Domain Name System – překlad doménových jmen na IP adresy a zpět
80	HTTP	HyperText Transfer Protocol – přenos WWW stránek i jiných dat
110	POP3	Post Office Protocol version 3 – stahování elektronické pošty
143	IMAP	Internet Message Access Protocol 4 – vzdálená správa poštovní schránky s elektronickou poštou
161	SNMP	Simple Network Management Protocol
443	HTTPS	Šifrovaný přenos HTTP protokolu přes TLS

3.2.1.2 Protokol HTTP

Protokol HTTP[33] je jedním z protokolů aplikační vrstvy TCP/IP, určený pro komunikaci s webovými servery. Slouží pro přenos hypertextových[34] dokumentů ve formátu HTML, XML, JSON a jiných. Společně s protokolem elektronické pošty – SMTP je nejvyužívanějším protokolem, který se zasloužil o obrovský rozmach internetu. Samotný HTTP protokol neumožnuje šifrování ani kontrolu integrity dat.

[31] HORÁK, Jaroslav. *Bezpečnost malých počítačových sítí*. 1. vyd. [Praha]: Grada, 2003. ISBN 80-247-0663-6, str. 106.
[32] Síťový port. *Wikipedia* [online]. 8.8.2021. [cit. 6.2.2022]. Dostupné z: https://cs.wikipedia.org/wiki/S%C3%AD%C5%A5ov%C3%BD_port
[33] *„HTTP“* – anglicky „Hypertext transfer protocol“, v českém překladu „hypertextový přenosový protokol“.
[34] *„Hypertext“* – způsob strukturování textu, který není lineární. Obsahuje tzv. *„hyperlinky“* což jsou odkazy.

Pro zabezpečenou komunikaci se využívá HTTPS protokol, který přenášená data zašifrovává.[35]

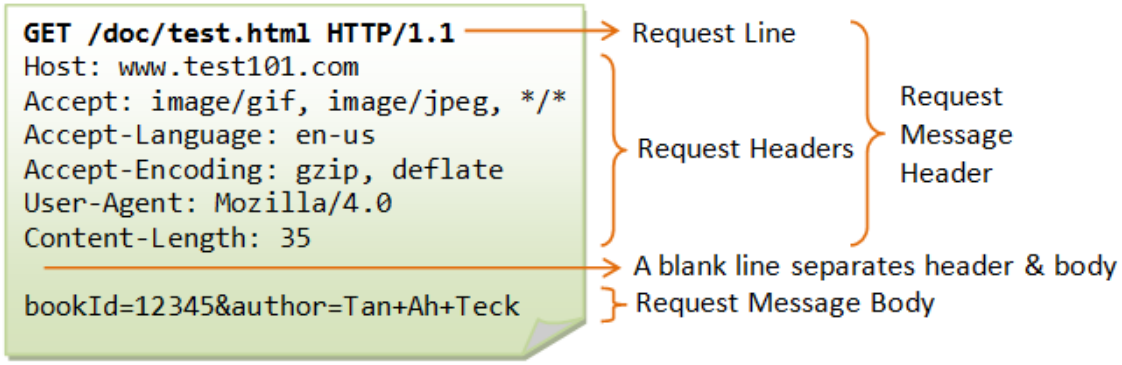
Protokol funguje na principu požadavek – odpověď. To znamená, že klient například za pomoci webového prohlížeče pošle webovému serveru zprávu s požadavkem vyžadujícím zaslání požadovaného dokumentu. Server v reakci odpoví zprávou, do které na několik řádků popíše výsledek dotazu (zda se dokument podařilo najít, jaký je to typ dokumentu atd.), a za ty připojí data samotného dokumentu.[36]

HTTP definuje několik dotazovacích metod, pomocí kterých klient může od serveru požadovat různé druhy služeb:[37]

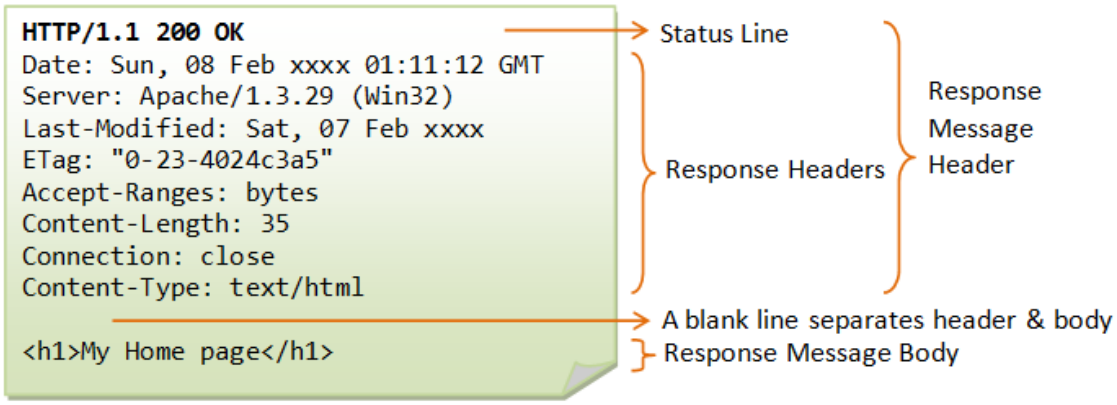
- **GET** – pomocí této metody lze ze serveru získat jakékoli informace o požadovaném objektu. Tyto informace jsou ze serveru vráceny v těle odpovědi. Jde o výchozí metodu pro zobrazování webových stránek.
- **HEAD** – metoda HEAD je podobná metodě GET, s tím rozdílem, že server v odpovědi nepředává data, ale poskytuje pouze metadata[38] o požadovaném cíli.
- **POST** – odesílá uživatelská data na server. Používá se například při odeslání vyplněného formuláře na server.
- **PUT** – nahraje data na server tak, že na cestě uvedené v požadavku vytvoří server soubor s požadovaným názvem.
- **DELETE** – smaže požadovaný objekt (soubor) ze severu.
- **TRACE** – server odešle kopii obdrženého požadavku zpět klientovi. Používá se pro ladící účely.
- **OPTIONS** – server v odpovědi vrátí seznam podporovaných metod.
- **CONNECT** – Spojí se s požadovaným objektem přes uvedený port. Používá se pro připojení k proxy serverům.

[35] Hypertext Transfer Protocol. *Wikipedia* [online]. 14.12.2021. [cit. 6.2.2022]. Dostupné z: https://cs.wikipedia.org/wiki/Hypertext_Transfer_Protocol
[36] *tamtéž*
[37] *tamtéž*
[38] *„Metadata“* – data, která poskytují informace o jiných datech.

Na obrázku 2[39] můžeme vidět příklad HTTP požadavku a na obrázku 3[40] HTTP odpovědi.



Obrázek 3 - příklad HTTP požadavku



Obrázek 2 - Příklad HTTP odpovědi

3.2.2 Transportní vrstva

Transportní vrstva zajišťuje organizaci dopravy dat. Skládá se z protokolů TCP a UDP.

3.2.2.1 Protokol TCP

Protokol TCP[41] přebírá od aplikační vrstvy data, která rozdělí na jednotlivé segmenty, očísluje a seřadí do pořadí, jak mají být odeslány. Před samotným odesíláním dat zahajuje relaci s transportní vrstvou vzdáleného zařízení a po

[39] *HTTP Request Message* [online]. [cit. 6.2.2022]. Dostupné z: https://documentation.help/DogeTool-HTTP-Requests-vt/http_request.htm
[40] *tamtéž*
[41] *„TCP“* – anglicky *„Transmition control protocol“*, v českém překladu *„protokol řízení přenosu“*.

navázání spojení začne s vysíláním segmentů a kontrolováním přenosu. O samotné odesílání se stará nižší síťová vrstva.

V protějším zařízení, přijímajícím data, funguje proces protokolu TCP opačně. Od síťové vrstvy jsou přebírány obdržené segmenty, které jsou následně setříděny. V případě, že nějaký segment chybí, TCP vyšle požadavek o opětovné zaslání. Ze segmentů jsou pak složena data a ty jsou předána skrz aplikační protokol do cílové aplikace.[42]

Předávání dat mezi aplikační a transportní vrstvou probíhá prostřednictvím portů.

3.2.2.2 Protokol UDP

UDP[43] protokol má podobnou funkci jako TCP – převezme data od aplikace, sestaví z nich jednotlivé segmenty a předá je síťové vrstvě k odeslání. Na rozdíl od TCP protokolu však před odesláním dat nenavazuje spojení s protějškem a nekontroluje, zda byly segmenty protějškem obdrženy. Předávání dat mezi aplikační a transportní vrstvou probíhá rovněž prostřednictvím portů.[44]

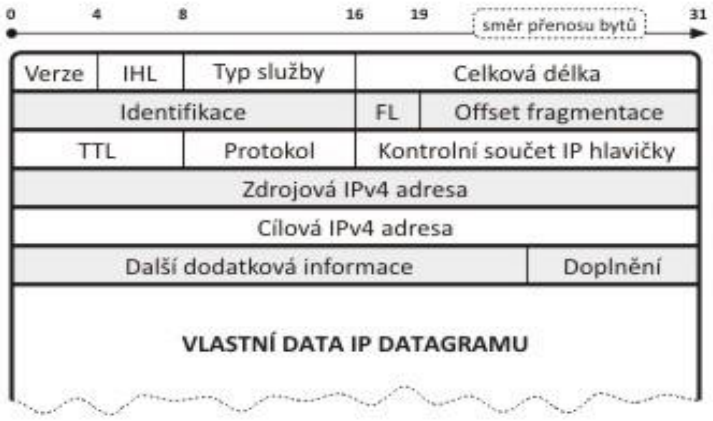
3.2.3 Síťová vrstva

Síťová vrstva zajišťuje adresování, směrování a odesílání paketů. O to se stará řada protokolů, z nichž je nejdůležitějším protokol IP.

[42] HORÁK, Jaroslav. *Bezpečnost malých počítačových sítí*. 1. vyd. [Praha]: Grada, 2003. ISBN 80-247-0663-6, str. 106.
[43] *„UDP“* – anglicky *„User datagram protocol“*, v českém překladu *„uživatelský protokol pro přenos datagramů“*.
[44] HORÁK, Jaroslav. *Bezpečnost malých počítačových sítí*. 1. vyd. [Praha]: Grada, 2003. ISBN 80-247-0663-6, str. 106.

3.2.3.1 Protokol IP

Protokol IP[45] přebírá od nadřazené transportní vrstvy datové segmenty k odeslání. K segmentům připojí svoji hlavičku a vytvoří tak IP datagram (datový paket). V IP hlavičce se mimo jiné nachází IP adresa příjemce a odesílatele.[46] Strukturu datagramu lze vidět na obrázku 4.[47]



Obrázek 4 - Formát IPv4 datagramu

IP protokol je sám o sobě nespolehlivý, jelikož nenavazuje spojení s protějškem a nekontroluje, zdali byly pakety v pořádku doručeny. O toto se stará protokol TCP nadřazené transportní vrstvy.

Aby mohlo zařízení komunikovat v rámci sítě, musí mít přidělenou IP adresu, která je v dané koncové síti (např. LAN) jedinečná. IP adresy mohou být přidělovány staticky (IP adresa je nastavena ručně), či dynamicky, kdy se nově připojenému zařízení do sítě, na základě MAC adresy,[48] přidělí nová IP adresa. IP adresa není standardně anonymní a používá se při komunikaci s jinými zařízeními v síti jako síťový identifikátor.[49]

Kromě dynamické a statické IP adresy ještě existují veřejné a neveřejné IP adresy, přičemž veřejné IP adresy jsou jedinečné v celém internetu a jsou v tomto prostoru i viditelné. Typicky se přidělují serverům, nebo jiným zařízením, se kterými komunikují klienti přes internet. Naproti tomu neveřejná IP adresa není

[45] *„IP“* – anglicky *„Internet protocol“*, v českém překladu *„Internetový protokol“*.
[46] HORÁK, Jaroslav. *Bezpečnost malých počítačových sítí*. 1. vyd. [Praha]: Grada, 2003. ISBN 80-247-0663-6, str. 106.
[47] BOHÁČ, Leoš. *IP protokol* [online]. 2016. [cit. 7.2.2022]. Dostupné z: https://docplayer.cz/1694986-Ip-protokol-leos-bohac.html
[48] MAC adresa – je jednoznačným identifikátorem síťového zařízení, typicky síťové karty. *„MAC“* – anglicky *„Media Access Control“*, v českém doslovném překladu *„řízení přístupu k médiím“*.
[49] KOLOUCH, Jan. *Cybercrime*. 1. vyd. Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8, str. 74.

v internetu viditelná, a jedinečná je pouze v koncové síti. Aby se z takové sítě dalo připojit k internetu, musí jí poskytovatel internetového připojení dynamicky přidělit veřejnou IP adresu, která není stálá.

V současnosti existují 2 verze protokolu IP:[50]

- **Internet protokol version 4 (IPv4)** – Jde o první masově rozšířenou a stále nejpoužívanější verzi IP protokolu. IPv4 používá 32bitové adresy, které jsou tvořeny čtveřicí decimálních čísel vzájemně oddělených tečkou, přičemž hodnota žádného z nich nepřesahuje 255. IP adresa v4 může vypadat například takto: *„192.168.0.1“*, nebo *„64.233.168.99“*. Problém protokolu IPv4 spočívá v tom, že nabízí malý adresní prostor (pouze okolo 4 294 967 296 kombinací) pro přidělování veřejných IP adres. Z toho důvodu byl vytvořen novější protokol IPv6, který má tento problém vyřešit.
- **Internet protokol version 6 (IPv6)** – Je novým protokolem, který by měl v budoucnosti vyřešit problém s nedostatkem veřejných IP adres. IPv6 používá 128bitové adresy, které jsou zapisovány hexadecimálně (např. *„2001:0:5ef5:79fd:386a:e7:4dee:fb51“*). Adresní rozsah je skutečně obrovský, 2^{128} adres, což je 2^{52} adres pro každou hvězdu ve známém vesmíru.[51] Protokol IPv6 přináší kromě většího adresního prostoru i další vylepšení jako například odstranění potřeby překladu síťových adres.

[50] KOLOUCH, Jan. *Cybercrime*. 1. vyd. Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8, str. 74.
[51] IPv6. *Wikipedia* [online]. 15.1.2022. [cit. 5.2.2022]. Dostupné z: https://cs.wikipedia.org/wiki/IPv6

4 Digitální stopy

Digitální stopy (anglicky „*digital trace“*, nebo „*digital footprint“*) jsou autory pojímány různě. Někteří o nich mluví v rámci poučení o bezpečnosti pohybu na internetu jako o datech, která tam po sobě zanecháváme svou činností, především pak na sociálních sítích. Většina lidí se o digitálních stopách dozvěděla nejspíše v této souvislosti.

Takto je například definovaná digitální stopa na stránkách antivirové společnosti Kaspersky: *„A digital footprint – sometimes called a digital shadow or an electronic footprint – refers to the trail of data you leave when using the internet“*.[52] V český překladu zní zhruba takto: *„Digitální stopa – někdy nazývaná digitálním stínem nebo elektronickou stopou – jsou data které po sobě zanecháváme při používání internetu“*.

Jiní autoři na ně zase nahlížejí jako na kriminalistické stopy, tedy jako na důkazní prostředek využívaný v trestním řízení pro objasnění trestné činnosti. Z hlediska kriminalistiky se stopou rozumí jakákoli změna v materiálním prostředí nebo ve vědomí člověka, která je zjistitelná, zajistitelná a využitelná současnými metodami, prostředky a postupy, mající příčinnou, prostorovou nebo časovou souvislost s kriminalisticky relevantní událostí.[53]

V tomto smyslu definují digitální stopu kupříkladu autoři Roman Rak a Viktor Porada takto: „*Digitální stopa je jakákoliv informace s vypovídající hodnotou, uložená nebo přenášená v digitální podobě*“.[54] Je zde zmíněno, že musí mít vypovídající hodnotu, tedy musí být nezpochybnitelná, relevantní k trestné činnosti a musí ji nějakým způsobem objasňovat.

---

[52] What is a digital footprint? And how to protect it from hackers. *Kaspersky* [online]. [cit. 27.11.2021]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/what-is-a-digital-footprint

[53] STRAUS, Jiří a kol. *Úvod do kriminalistiky*. 3. vyd. Plzeň: Aleš Čeněk, 2012. ISBN 978-80-7380-367-4, str. 74.

[54] RAK, Roman a Viktor PORADA. Digitální stopy v kriminalistice a forenzních vědách. *Soudní inženýrství* [online]. 2006, roč. 17. [cit. 8.2.2021]. Dostupné z: http://www.sinz.cz/archiv/docs/si-2005-01-3-23.pdf

Další autoři na digitální stopy nahlíží zeširoka a označují tak veškerá elektronická data, která jsou vytvořena v kyberprostoru. Kyberprostorem chápejme: *„digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací“*.[55]

Tuto širší definici nabízí i autor Jan Kolouch ve své publikaci *„Cybercrime“*: *„Za digitální stopu je možné označit jakákoli data či informace přenesená, vytvořená, uložená či modifikovaná za použití počítačového systému“*.[56]

Digitální stopy tedy lze chápat jako data, která po sobě zanecháváme na internetu, jako kriminalistickou stopu či jako data obecně.

4.1 Dělení digitálních stop

Digitální stopy jsou rozlišovány podle toho, zdali je uživatelé vytvářejí vědomě, nebo bez jejich vědomí a možnosti jejich vznik nějak ovlivnit.

Jan Kolouch rozděluje digitální stopy následovně:[57]

- **Digitální stopa ovlivnitelná**
  - Vědomé využiti služeb,
  - dobrovolné zveřejněni informace,
  - blogy, fóra,
  - sociální sítě,
  - e-mail,
  - datová uložiště,
  - cloudové služby aj,
- **Digitální stopa neovlivnitelná**
  - Informace z počítačového systému,
  - připojení k počítačovým sítím, zejména internetu,
  - využívání poskytovaných služeb aj.

[55] Zákon č. 181/2014 Sb., *zákon o kybernetické bezpečnosti* v posledním znění.
[56] KOLOUCH, Jan. *Cybercrime*. 1. vyd. Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8, str. 403.
[57] KOLOUCH, Jan. *Cybercrime*. 1. vyd. Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8, str. 135.

Obdobný způsob kategorizace používají i jiní autoři s pozměněným názvoslovím. Například ovlivnitelná digitální stopa bývá nazývána aktivní, vědomou či dobrovolnou a neovlivnitelná je označována za pasivní, nevědomou, nedobrovolnou.

Digitální stopy se rovněž mohou rozlišovat i podle jiných kritérií na:[58]

- **Veřejné** – informace, které dohledá kterýkoliv uživatel internetu.
- **Neveřejné** – jde o informace, které dohledá jen určitý okruh uživatelů internetu (např. přátelé na sociálních sítích).
- **Skryté** – například cookies a jiné technické záznamy o zařízení a připojení.
- **Vlastní** – jedná se o digitální stopu, kterou uživatel ve virtuálním prostředí zanechá vlastní činností.
- **Zanechanou jinými osobami** – jde o digitální stopy, které obsahují informace o jiných osobách, než o té, která ji vytvořila. Může jít například o označení v příspěvku, nebo na fotce na nějaké sociální síti. To může mít samozřejmě přátelský i nepřátelský charakter, proto autor dále dělí tuto kategorii na **Digitální stopu zanechanou přáteli** a **digitální stopu zanechanou nepřáteli**.

4.1.1 Digitální stopy ovlivnitelné

Jedná se o data, které uživatel vědomě tvoří, a tedy rozhoduje nad tím, zdali je vytvoří či nikoliv. Web zabývající se internetovou bezpečností – „Internetem bezpečně“ definuje ovlivnitelnou digitální stopu takto: *„Vědomá (aktivní) stopa je zanechaná cílenou a vědomou činností“*.[59]

Jan Kolouch charakterizuje aktivní digitální stopu následovně:

„*Digitální stopa ovlivnitelná představuje veškeré informace, které o sobě uživatel sám dobrovolně předá jine osobě (ať fyzické či právnické, nebo i např. ISP).*[60] *Digitální stopy ovlivnitelné jsou stopami, nad kterými může mít uživatel*

[58] Digitální stopa. *Internetem bezpečně* [online]. [cit. 14.3.2021]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/dobre-vedet/digitalni-stopa/
[59] *tamtéž*
[60] *„ISP“* – anglicky *„Internet service provider“*, v českém překladu *„poskytovatel internetových služeb“.*

relativní kontrolu a je pouze na něm, jaké informace o sobě hodlá zpřístupnit jiným“.[61]

Z toho tedy vyplývá, že uživatel je seznámen s obsahem dat, které vytváří, či předává a rovněž o tom vědomě rozhoduje.

- **V offline prostředí** se jedná například o vytváření souborů – fotografií, textových souborů, zvukových záznamů či jiné tvoření digitálního obsahu.
- **V online prostředí** je to pak to, co do něj vědomě vložíme – nahraní příspěvků na sociální sítě, odeslání emailu, chatování, nahrání souborů na cloudová úložiště atd.

Zmíněný autor dále pod ovlivnitelné digitální stopy zahrnuje data předávaná na základě odsouhlasení smluvních podmínek zvaných EULA[62] (end user licence agreement) poskytovatelům internetových služeb, jako **hypoteticky ovlivnitelné digitální stopy.** Uživatel má totiž možnost se dobrovolně rozhodnout, zdali na podmínky přistoupí či ne, avšak „*uživatelé to běžně nedělají, jelikož by si tím značně omezili možnosti svého fungování v digitálním světě“*. Mezi tuto skupinu lze například zařadit digitální stopy, které vznikají při využívání služeb největších ISP (Microsoft, Apple, Google, Facebook), u kterých je využívání služeb podmíněno odsouhlasením smluvních podmínek.*[63]*

4.1.2 Digitální stopy neovlivnitelné

Jako digitální stopy neovlivnitelné jsou označována data, které vznikají při samotném chodu počítačového systému, při komunikaci s jiným počítačovým systémem, nebo na základě funkčnosti daného počítačového systému a jeho softwaru.[64] Jedná se například o logy programů či operačního systému, metadata, cookies a datové pakety odeslané do sítě internet.

Web *„Internetem bezpečně“* popisuje vznik neovlivnitelné digitální stopy takto: *„Nevědomá stopa vzniká jako vedlejší produkt tvorby vědomé digitální stopy.*

[61] KOLOUCH, Jan. *Cybercrime*. 1. vyd. Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8, str. 144.
[62] *„EULA“* – anglicky *„End user licence agreement“*, v českém překladu *„licenční smlouva s koncovým uživatelem“*.
[63] KOLOUCH, Jan. *Cybercrime*. 1. vyd. Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8, str. 145.
[64] KOLOUCH, Jan. *Cybercrime*. 1. vyd. Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8, str. 135.

Ukládá se bez zásahu uživatele“.[65] Nevím ale, jestli to lze takto generalizovat, jelikož například zápis logů nemusí být nutně reakcí na akci provedenou uživatelem.

Některé tyto stopy však lze měnit, mazat nebo potlačovat,[66] takže nelze tvrdit, že by byly skutečně neovlivnitelné, spíše jejich vznik je dán vlastním fungováním počítačových systémů a jejich softwaru.

4.1.2.1 Metadata

Metadata jsou strukturovaná data, popisující další data a informace, zdroj, ke kterému jsou vázané. Stručně řečeno, jsou to data popisující jiná data.[67]

Metadata souborů jako jsou fotografie se zapisují automaticky po jejich vytvoření, a mohou obsahovat informace jako datum vytvoření, rozlišení, model fotoaparátu, poloha odkud byla fotka pořízena, ISO, délka expozice atd.

Metadata lze specializovanými programy odstranit.

4.1.2.2 Cookies

Cookies jsou informace, které se ukládají v internetovém prohlížeči na straně klienta. Slouží například k uložení informace o tom, co obsahuje nákupní košík při nakupování v e-shopu.[68]

Cookies, do kterých se ukládají uživatelské předvolby pro webové stránky, lze v prohlížeči smazat, či zablokovat, nicméně webové prohlížeče je mají defaultně povoleny.

[65] Digitální stopa. *Internetem bezpečně* [online]. [cit. 14.3.2021]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/dobre-vedet/digitalni-stopa/
[66] KOLOUCH, Jan. *Cybercrime*. 1. vyd. Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8, str. 136.
[67] Metadata. *IT slovník* [online]. [cit. 4.2.2021]. Dostupné z: https://it-slovnik.cz/pojem/metadata
[68] Cookies. *IT slovník* [online]. [cit. 4.2.2021]. Dostupné z: https://it-slovnik.cz/pojem/cookies

4.1.2.3 Logy

„Log je záznam (zpráva) o nějaké činnosti. Například server může logovat (zaznamenávat) všelijaké činnosti, které na něm probíhají, aby jeho správce měl přehled například o tom, kdo se kam kdy přihlásil“.[69]

Logy operačního systému a různých programů lze smazat, ale software, který je vytváří je často nastaven tak, aby je vytvářel kontinuálně, a v některých případech může být složité potlačit jejich tvorbu.

4.1.2.4 Data odeslaná do internetu

Pokud kdykoliv cokoliv nahrajete, přenesete, zprostředkujete, vložíte do kyberprostoru, zůstane to tam „navždy“.[70] Pokud dojde k odeslání dat do internetu, je nad nimi defacto ztracena kontrola a vypátrat kde všude zůstala o odeslání dat nějaká informace je téměř nemožné. K tomuto přenosu dat může docházet i pouhým připojením k internetu, uživatel nemusí ani aktivně *„Surfovat“*.

Jak již bylo popsáno, přenos dat v internetu probíhá prostřednictvím datových paketů, které mimo samotných přenášených dat rovněž obsahují identifikační údaje o odesílateli, které jsou potřebné pro úspěšné navázání kontaktu s cílovým zařízením (například webový server).

Mezi tyto údaje například patří IP adresa a MAC adresa,[71] které se při cestě datových paketů mohou zaznamenávat na jednotlivá zařízení v síťové infrastruktuře a samozřejmě i na koncové zařízení, na který byly datové pakety zaslány. Podle těchto identifikátorů lze zpětně dohledat zařízení ze kterého byly vyslány, a to i v případě, že nemá veřejnou IP adresu (za pomoci poskytovatele připojení k internetu).[72]

[69] Log. *IT slovník* [online]. [cit. 4.2.2021]. Dostupné z: https://it-slovnik.cz/pojem/log
[70] KOLOUCH, Jan. *Cybercrime*. 1. vyd. Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8, str. 134.
[71] *Internet* [online]. [cit. 30.1.2022]. Dostupné z: https://www.ssph.cz/vyuka/wp-content/uploads/2020/03/psi-internet.pdf
[72] KOLOUCH, Jan. *Cybercrime*. 1. vyd. Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8, str. 136.

Webové servery dále mohou logovat veškeré HTTP požadavky, které obdržely, včetně informací o internetovém prohlížeči, operačním systému, cookies atd. které standardně obsahují.[73]

Ukládat se mohou i samotná přenášená data, tedy obsah paketů či požadavků, který je z uživatelova zařízení odeslán (stav operačního systému, přechod na webovou stránku, GPS souřadnice zařízení atd.).

4.2 Vlastnosti digitálních stop

Digitální stopy mají své obecné i individuální druhové charakteristiky a vlastnosti. Vznikají buď působením člověka na aplikační nebo systémový software, jako funkčnost digitálního zařízení nebo softwaru, nebo automatickým působením jednoho zařízení na druhé.[74]

Vlastnosti digitálních stop, především z kriminalistického hlediska, jsou shrnuta v následujícím přehledu, převzatém od autorů Romana Raka a Viktora Porady:[75]

- **Nehmotnost** – data jako taková jsou nehmotná. Pro jejich ukládání je vždy nutné hmotné médium, které má nejrůznější technologické provedení, formát, datovou strukturu, konektivitu, spolehlivost, životnost apod. Digitální stopa, se zaznamenává na takové médium ve formě kódované a digitalizované informace.
- **Latentnost** – digitální stopy jsou neviditelné. Jejich latentnost je rovněž vícenásobná.
    - **První stupeň latentnosti:** Záznamy zpracovávané nebo uchovávané na datovém médiu nelze vidět pouhým okem. Na jejich zviditelnění se musí použít vhodné zařízení.

[73] KOLOUCH, Jan. *Cybercrime*. 1. vyd. Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8, str. 139.
[74] RAK, Roman a Viktor PORADA. Vlastnosti digitálních stop a jejich dopady na forenzní šetření. *Soudní inženýrství* [online]. 2005, roč. 16. [cit. 16.10.2021]. http://www.sinz.cz/archiv/docs/si-2005-04-183-192.pdf
[75] *tamtéž*

    - **Druhý stupeň latentnosti:** Některé soubory mohou být pro běžného uživatele neviditelné, protože mohou být skryté z důvodu systémového nastavení, uživatelské role atd.
    - **Třetí stupeň latentnosti:** Sem patří smazané záznamy, přeformátované disky, či jiným nástroji pozměněná nebo zničená data na datovém médiu. Dále sem spadají soubory zašifrované šifrovacím softwarem, nebo zaheslované. Tyto soubory jsou pro uživatele sice viditelné, ale bez informačního obsahu.
- **Časová tvarovatelnost** – digitální stopy mohou s přesností na milisekundy určit přesné časové vymezení proběhlých procesů. Počítače a stejně tak další elektronická zařízení (telefony, fotoaparáty atd.) mají v sobě zabudované digitální hodiny, které označují aktivity aplikačního, systémového SW nebo jiných činností digitálních zařízení tzv. časovou známkou (timestamp).
- **Vysoká obsažnost** – digitální stopy mohou obsahovat mnoho informací o osobních zájmech a konkrétních aktivitách svého uživatele. Lze z nich například vyčíst navštívené webové stránky (a jejich obsahy), prohlížené fotografie, videa, textové soubory, odeslaná a přijatá data atd.
- **Velmi nízká životnost** – jak již bylo zmíněno, digitální záznamy jsou zapisovány na paměťová média. Zde se informace mohou uchovat po velmi dlouhou dobu, nicméně taktéž odsud mohou být velmi snadno vymazány uživatelem, nebo operačním systémem, popřípadě jiným softwarem, bez vědomí uživatele. Z tohoto hlediska je životnost digitální stopy hodnocena jako velmi nízká.
- **Velký datový objem** – pro výpočetní a komunikační prostředky je dnes typická jejich silná centralizace, vycházející z provozně-ekonomických důvodů. Na paměťových médiích jsou uchovávána obrovská množství dat. K tomu ještě s postupem času vznikají nové a lepší technologie komprimací dat a samotných datových médií, což má za následek, že se do stejného datového prostoru vejde čím dál více dat.
- **Možnost restaurovatelnosti** – smazaná (poškozená) data je možné za určitých okolností úplně či částečně restaurovat. To není zpravidla možné u jiných druhů kriminalisticky relevantních stop provést. Po smazání či

naformátování totiž defacto nedojde ke smazání dat z média, operační systém pouze uvolní místo, na kterém se nacházela smazaná data pro přepis jinými daty. Restaurování tedy musí být provedeno velice rychle, než je místo na paměťovém médiu přepsáno.

- **Vysoký stupeň ochrany** – řada datových přenosů, zejména těch, které probíhají přes internet, včetně datových úložišť či jednotlivých souborů je z bezpečnostních důvodů kryptograficky chráněna. Pokud neznáme příslušný algoritmus, klíč nebo technologický prostředek na jejich rozkódování, nemají pro nás zašifrovaná data informační hodnotu.
- **Uchování a kvalita je ovlivněna řadou subjektivních faktorů** – toto se týká především institucí, kde se uchování a kvalita dat odvíjí od mezinárodní, národní nebo institucionální legislativy, odbornosti administrace systémů z hlediska bezpečnosti dat a závisí i na institucionální kultuře, která rozhoduje o úrovni realizace výše uvedených faktorů.
- **Extrémní dynamičnost prostředí** – s aplikacemi na produkčních prostředích pracuje velké množství uživatelů. Tato aplikační prostředí jsou extrémně dynamické, generují obrovské množství dat, která se mohou navzájem přepisovat, zneplatňovat či mazat. U některých podnikových aplikací může být jejich nepřetržitý provoz pro instituci naprosto kritický, tj. pozastavení provozu aplikace po dobu i řádově minut (průmysl, doprava, telekomunikace, finanční instituce atd.) může mít pro instituci nebo jejího zřizovatele katastrofické existenční dopady. Mnohdy je proto nu zajišťovat kriminalisticky relevantní digitální stopy na živých produkčních prostředích.
- **Heterogennost a komplexnost prostředí** – prostředí ICT[76] je velmi rozmanité, tedy heterogenní. V praxi se používají různé operační systémy, databázové systémy, aplikační software, datová rozhraní, datové formáty, přenosové protokoly, protokoly provozních záznamů, logů atd. Kriminalisticky relevantní digitální stopy mohou být ukryty v nejrůznějších částech ICT a z tohoto důvodu je třeba pro jejich zajištění často potřebné velké množství vysoce kvalifikovaných specialistů.

[76] *„ICT“* – anglicky *„Information and Communication Technologies“*, v českém překladu *„informační a komunikační technologie“*.

- **Velký geografický rozsah prostoru** – počítačové sítě díky vzájemnému propojení přes internet nemají geografických hranic. Digitální stopy mohou být uloženy v různých datacentrech po celém světě**.** Promyšlené kybernetické útoky mohou být cíleně vedeny přes několik serverů v cizích zemích. Vyhledávání a zajišťování digitálních stop takovéto trestné činnosti je pak komplikováno tím, že vyšetřování jsou vždy založena na zákonech platných v dané zemi a v některých případech v ní ani nemusí být trestná. Dalšími komplikacemi jsou spolupráce se zahraničními ošetřovacími týmy, rozdílné vyšetřovací postupy a způsoby zajišťování digitálních stop.
- **Možnost automatizace vyhledání a zpracování** – jelikož jsou digitální stopy vytvořeny vždy určitou technologií, lze je rovněž při zachovaní nezbytných podmínek automaticky vyhodnocovat. Část digitálních stop může být výstupem uživatelského či systémového softwaru naprogramovaného podle určitých principů a algoritmů, takže výstupy z těchto programů mají odpovídající logiku a strukturu plus datový formát.
- **Možnost zahlazování kvalifikovanými pachateli** – největší škody způsobují pachatelé s vysokou odborností v oblasti ICT. Je to dáno tím, že vědí, jak fungují informační systémy, které napadají, dále způsoby ochrany dat, jež dokážou obejít a často i vnitřní procesy a politiku v korporacích. Tito pachatelé se dokážou nabourat do systémů do kterých nemají přístup, získat z nich data a zahladit část digitálních stop které po sobě zanechali například mazáním provozních nebo monitorovacích logů o uživatelských nebo systémových aktivitách. V případě, že útočník dokáže získat přístupové údaje jiné osoby a podniknout pod nimi útok, odvede tím při případném odhalení pozornost jiným směrem.
- **Originálnost** – data se dají velmi snadno kopírovat, přičemž při kopírování nebo přenosu dat nedochází ke ztrátě nebo zkreslení dat. Lze je ale v určitých případech pozměnit, aniž by tyto změny zanechaly další průkazné stopy. Velmi špatně se pak dokazuje, jaká digitální stopa je originál a jaká kopie, což může být problematické při předkládání důkazů v trestním řízení.

Podobně popisuje vlastnosti digitálních stop i Jan Kolouch,[77] který tvrdí, že oproti klasickým stopám jsou digitální stopy **značně datově objemné**, **dynamické**, **umístitelné kdekoli v kyberprostoru** a jejich **životnost může být velmi krátká**.

4.3 Využití digitálních stop

4.3.1 Využití digitálních stop v kriminalistice a forenzní praxi

V kriminalistické praxi jsou digitální stopy brány především jako důkazní materiál vztahují se k vyšetřování trestných činů a přestupků, specifikovaných zákonem. Pro potřeby kriminalistické (stejně tak ovšem i forenzní) praxe je požadována vysoká kvalita a objektivita zajištěných stop. Kriminalistické stopy chápeme jako podmnožinu forenzních stop.[78]

Digitální stopy neobjasňují nutně pouze trestné činy spojené s kyberkriminalitou, ale vzhledem k charakteru, který digitální stopy mohou mít (sms zpráva, telefonní hovor, zvukový záznam, videozáznam, dokument, GPS poloha atd.) je lze využívat pro objasňování všech různých druhů trestné činnosti.

Z hlediska trestního práva procesního je v současnosti digitální stopa subsumována pod ustanovení § 112 odst. 1 a odst. 2 TŘ.[79]

(1) Věcnými důkazy jsou předměty, kterými nebo na kterých byl trestný čin spáchán, jiné předměty, které prokazují nebo vyvracejí dokazovanou skutečnost a mohou být prostředkem k odhalení a zjištění trestného činu a jeho pachatele, jakož i stopy trestného činu.

(2) Listinnými důkazy jsou listiny, které svým obsahem prokazují nebo vyvracejí dokazovanou skutečnost vztahující se k trestnému činu nebo k obviněnému.

[77] KOLOUCH, Jan. *Cybercrime*. 1. vyd. Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8, str. 403.
[78] RAK, Roman a Viktor PORADA. Digitální stopy v kriminalistice a forenzních vědách. *Soudní inženýrství* [online]. 2006, roč. 17. [cit. 8.2.2021]. Dostupné z: http://www.sinz.cz/archiv/docs/si-2005-01-3-23.pdf
[79] Zákon č. 141/1961 Sb., *zákon o trestním řízení soudním (trestní řád)* v posledním znění.

Forenzní praxe na rozdíl od klasického kriminalistického vyšetřování provádí i šetření charakteru forenzních auditů v civilní nebo komerční sféře (například v občanskoprávních sporech). Výstupy vyšetřování jsou připravovány tak, aby svou kvalitou a formálním zpracováním obstály před soudními orgány.[80]

4.3.2 Využití digitálních stop v marketingu

Další oblastí, kde se hojně využívají digitální stopy je marketing, konkrétně behaviorální marketing. Ten se zaměřuje na komplexní analyzování zákazníkova chování pro větší marketingovou efektivitu.

Výsledkem jsou personalizované nabídky či reklamy, které jsou uživatelům v online prostředí zobrazovány na webových stránkách, přičemž o tom, co se uživateli zobrazí, rozhodují algoritmy.[81] Tyto algoritmy sledují chování uživatelů na internetu, popřípadě na konkrétní webové stránce, na které jsou umístěny, a analyzují jej. Výsledkem analýz potom mohou být profily uživatelského chování, podle kterých se tyto nabídky nebo reklamy zobrazují.

Fungování těchto algoritmů lze rozdělit do dvou kategorií:[82]

- **Algoritmy sledující uživatele na konkrétním webu** – typicky na ně lze narazit na například na e-shopech. Tyto algoritmy sledují, z jaké části světa (země) uživatel pochází, z jakých stránek se na web dostal, jestli jde o nového zákazníka, jaké zboží ho nejvíce zajímalo, kolik času kde strávil, z jaké stránky web opustil atd. Na základě těchto dat pak lze například zjišťovat trendy a uzpůsobovat nabídky doporučených produktů pro zákazníka podle jeho profilu, nebo plánovat kampaně podle toho, jak se aktuálně zákazníci chovají.

[80] RAK, Roman a Viktor PORADA. Digitální stopy v kriminalistice a forenzních vědách. *Soudní inženýrství* [online]. 2006, roč. 17. [cit. 8.2.2021]. Dostupné z: http://www.sinz.cz/archiv/docs/si-2005-01-3-23.pdf

[81] *„Algoritmus“* – předpis konečného počtu kroků, kterými je možno řešit stejnorodé úkoly, např. výpočty, programy pro počítač.

[82] Behaviorální marketing. *Mediaguru* [online]. [cit. 24.10.2021]. Dostupné z: https://www.mediaguru.cz/slovnik-a-mediatypy/slovnik/klicova-slova/behavioralni-marketing/

- **Reklamní systémy** – jde o systémy, které na uživatele cílí tzv. personalizovanou reklamu na základě jeho nedávného chování na internetu. Dělí se dále na tři druhy:
    - **Systémy vyhodnocující navštívené weby** – sledují, jaké weby uživatel v minulosti navštívil a podle toho zobrazují reklamu. Například uživateli, který navštívil knižní e-shop se bude spíše zobrazovat reklama na nový knižní bestseller než na nový notebook.
    - **Systémy vyhodnocující vyhledávaná slova** – sledují klíčová slova, které uživatel vyhledával přes internetové prohlížeče a jiné stránky a na základě toho utvoří profil chování uživatele, podle kterého nabízí reklamy.
    - **Systémy vyhodnocující kontext navštívený stránek** – sledují klíčová slova na navštívených stránkách (například nadpisy stránek, tagy atd.) a na základě těchto dat personalizují reklamy.

Na behaviorální marketing lze v dnešní době narazit snad u všech větších webů. Je to dáno tím, že pronájmem virtuálních reklamních ploch lze získat nemalé peníze od podnikatelů, nebo společností, jejichž nabídky se zde mají zobrazovat. Takže dává smysl umisťovat je na weby s vysokou návštěvností.

Například drtivá většina příjmů společnosti Meta Platforms (dříve Facebook), provozující nejpoužívanější sociální sítě (Facebook, Instagram, WhatsApp atd.), pochází právě z prodeje virtuálních reklamních ploch. Podle webu „*investopedia*“ to v roce 2021 bylo 97 % z celkových příjmů.[83]

Právě Meta Platforms je společně s Google jedním z největších poskytovatelů virtuálních reklam a zároveň vývojářem nejsofistikovanějších systémů pro personalizovanou reklamu, která zpracovává digitální stopy uživatelů využívajících jejich služeb.

Nicméně, personalizované reklamy nejsou jediným způsobem, jak na digitálních stopách vydělávat. Tato data se mimo jiné dají zpracovávat za účelem

83 JOHNSTON, Matthew. How Facebook (Meta) Makes Money. *Investopedia* [online]. 4.2.2022 [cit. 8.2.2022]. Dostupné z: https://www.investopedia.com/ask/answers/120114/how-does-facebook-fb-make-money.asp

statistik či analýzy trendů, což může společnostem dát značnou výhodu při boji s konkurencí. Proto existuje řada firem, které z takovýchto činností profitují. Například tuzemská firma Avast přes svůj softwarový produkt „*Avast antivirus*“ sledovala a sbírala data od uživatelů, kteří měli tento antivirus nainstalovaný ve svém počítači. Tyto nashromážděné digitální stopy od uživatelů poté byly analyzovány dceřinou firmou Jumpshot, která se konkrétně zajímala o chování uživatelů na webových stránkách, a vypracované analýzy prodávala svým zákazníkům.[84] Jakmile se informace o této činnosti dostaly na veřejnost, Avast v reakci na negativní PR,[85] které zpráva vyvolala, dceřinou společnost zrušil.[86]

4.3.2.1 Zpracování osobních údajů

Právě business založený na zpracovávání osobních údajů, byl jedním z impulzů v EU k vytvoření legislativy, jež nastaví podmínky pro tuto činnost za účelem ochrany osobních údajů před jejich zneužitím. V roce 2016 vydala evropská rada společně s parlamentem nařízení č. 2016/679 veřejně známé jako GDPR. Společně s tímto nařízením pak ještě zpracování osobních údajů v ČR doplňuje zákon č. 110/2019 Sb. – *zákon o zpracování osobních údajů*.

Jako osobní údaj GDPR definuje: „*veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby“.*[87]

Digitální stopy mohou být i nositelem osobních údajů, jelikož mohou obsahovat informace, podle kterých lze přímo identifikovat osobu která je zanechala, nebo

[84] KAN, Michael. The Cost of Avast's Free Antivirus: Companies Can Spy on Your Clicks. *PCmag* [online]. 27.1.2020. [cit. 27.11.2021]. Dostupné z: https://www.pcmag.com/news/the-cost-of-avasts-free-antivirus-companies-can-spy-on-your-clicks
[85] „PR“ – anglicky „public relations“, v českém překladu „vztahy s veřejností“.
[86] Avast uzavře svoji dceřinou společnost Jumpshot. *Avast* [online]. 30.1.2020. [cit. 27.11.2021]. Dostupné z: https://press.avast.com/cs-cz/avast-uzavre-svoji-dcerinou-spolecnost-jumpshot
[87] Nařízení evropského parlamentu a rady EU 2016/679, *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)*, čl. 4.

zařízení, které stopu zanechalo a podle toho pak identifikovat jeho majitele. Například Soudní dvůr EU ve svém rozhodnutí ze dne 29. 1. 2008, sp zn. C 275/06, *Productores de Música de Espana (Promusicae) vs. Telefónica de Espana SAU*, považoval IP adresu v kontextu daného případu (Promusicae požadovala po Telefonice odhalení identit osob, kterým poskytovala připojení k internetu a u nichž byla známá jejich IP adresa a datum a čas připojení) za osobní údaj ve smyslu předpisů na ochranu osobních údajů.[88]

Zpracování osobních údajů je v GDPR definováno jako: *„jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení“.*[89]

Z toho vyplývá že jakékoli nakládání s osobními údaji, byť jen jejich shromažďování bez dalšího zpracování je podřízeno těmto předpisům.

Jako subjekt, který osobní údaje zpracovává rozlišuje legislativa na:

- **Správce** – správce je subjekt, který odpovídá za dodržování povinností kladených legislativou, především za dodržení zásad zpracování, které provádí. Správce musí disponovat řádným právním důvodem pro zpracování osobních údajů a určuje účel i prostředky pro jejich zpracování. Taktéž odpovídá za zabezpečení zpracovávaných osobních údajů. Každého správce se legislativa dotýká jiným způsobem, a to v závislosti na aspektech zpracování, které provádí[90]. Správcem může být jakýkoli subjekt, i fyzická osoba, pokud nezpracovává osobní údaje způsobem, který jí vylučuje z uplatnění výjimky osobní či domácí činnosti.[91]

[88] KOLOUCH, Jan. *Cybercrime*. 1. vyd. Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8, str. 76-77.
[89] *tamtéž*
[90] Správce, zpracovatel. *Úřad pro ochranu osobních údajů* [online]. 25.4.2019. [cit. 12.5.2021]. Dostupné z: https://www.uoou.cz/7-spravce-zpracovatel/d-27278
[91] Základní pojmy v GDPR. *Ministerstvo vnitra ČR* [online]. [cit. 12.5.2021]. Dostupné z: https://www.mvcr.cz/gdpr/clanek/zakladni-pojmy-v-gdpr.aspx

- **Zpracovatele** – zpracovatelem je jakýkoli subjekt, kterého si správce najímá, aby pro něj zpracovával osobní údaje. Od správce se zpracovatel liší tím, že může v rámci zpracování osobních údajů provádět pouze to, čím ho správce pověřil.[92]

Aby správce mohl zpracovávat osobní údaje určité osoby, musí mu tato osoba ke zpracování udělit souhlas. V případě internetových služeb, nebo softwaru je uživatel před prvním použitím dané platformy vyzván k udělení souhlasu se smluvními podmínkami (Terms of service – ToS), nebo s licenčním ujednáním koncového uživatele (End User License Agreement – EULA), kde se ve výčtu ustanovení typicky daná klauzule ohledně zpracování osobních údajů nachází. Souhlasem s ToS nebo EULA uživatel rovněž stvrzuje souhlas se zpracováním svých osobních údajů. V některým ze zákona daných případech lze zpracovávat osobní údaje i bez souhlasu. Tyto podmínky jsou uvedeny v § 43 zákona č. 110/2019 o zpracování osobních údajů.

Udělením souhlasu nabývá subjekt údajů (fyzická osoba) určitých práv, jejichž účelem je vybalancovat vztah mezi správcem a subjektem údajů. Výčet práv je uveden v zákoně č. 110/2019 Sb. (zákon o zpracování osobních údajů).

Mezi tato práva patří:[93]

- **Právo na přístup k osobním údajům** – správce je povinen na žádost subjektu údajů sdělit, zdali zpracovává jeho osobní údaje. Pokud je skutečně zpracovává, má povinnost předat je subjektu společně s informacemi o účelu zpracování osobních údajů, o právních předpisech na jejichž základě údaje zpracovává, o příjemcích zpracovávaných údajů, předpokládané době a způsobu uchování údajů, a o zdroji těchto údajů. Plné znění právní normy se nachází v § 28.
- **Právo na opravu a výmaz osobních údajů** – Správce je povinen na žádost subjektu údajů provést opravu nebo doplnění osobních údajů vztahujících se k jeho osobě. Správce je dále povinen provést na žádost

[92] Základní pojmy v GDPR. *Ministerstvo vnitra ČR* [online]. [cit. 12.5.2021]. Dostupné z: https://www.mvcr.cz/gdpr/clanek/zakladni-pojmy-v-gdpr.aspx
[93] Zákon č. 110/2019 Sb., *zákon o zpracování osobních údajů* v posledním znění.

subjektu výmaz jeho osobních údajů, pokud správce porušil zásady zpracování osobních údajů, nebo pokud má povinnost tyto údaje vymazat. Plné znění právní normy se nachází v § 29.

Jak již bylo uvedeno, správce má povinnost zajistit zabezpečení uchovávaných osobních záznamů. Toto může zajistit například jejich pseudonymizací nebo zašifrováním. Pokud jsou data zabezpečena tak, že jsou nečitelná nebo nekonkrétní, pak správci při případném úniku dat nemusí vzniknout povinnost únik dat ohlašovat dozorovému úřadu (úřadu pro ochranu osobních údajů) a dotčeným subjektům údajů. Správce však i v tomto případě musí vždy posoudit, zdali únik dat představuje riziko pro práva a svobody fyzických osob, a podle tohoto úsudku únik dat nahlásit.[94]

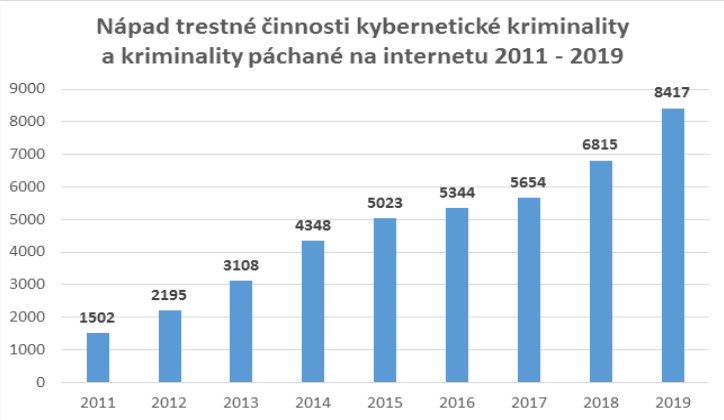
4.4 Zneužití digitální stopy

Způsoby užití digitálních stop uvedené v předešlých kapitolách jsou legální při splnění zákonem daných podmínek. Vzhledem k tomu, že digitální stopy mohou obsahovat osobní či jiné citlivé údaje, jsou v nepovolaných rukou dobrým zdrojem informací, a často jsou zneužívány při útocích v kyberprostoru.[95] Cílem těchto útoků může být získání dalších citlivých údajů, krádež identity, sledování, vydírání, případně jiné poškozování osob jako kyberšikana, nebo kyberstalking.

Zneužívání digitálních stop bude především doménou kybernetické trestné činnosti, kvůli samotné podstaty digitálních stop (jedná se o data uchovaná v kyberprostoru, pro práci s nimi je třeba využít zařízení ICT). Kybernetickou trestnou činnost, též kyberkriminalitu, nebo cybercrime chápejme jako *„trestnou činnost, která je páchána v prostředí informačních a komunikačních technologií včetně počítačových sítí. Samotná oblast informačních a komunikačních technologií je buď předmětem útoku, nebo je páchána trestná činnost za*

[94] Zabezpečení osobních údajů. *Úřad pro ochranu osobních údajů* [online]. 25.4.2019. [cit. 12.5.2021]. Dostupné z: https://www.uoou.cz/8-zabezpe-eni-osobnich-udaj/d-27282
[95] KOVÁŘOVÁ, Pavla. *Informační bezpečnost žáků základních škol*. 1. vyd. [Brno]: Masarykova univerzita, 2019. ISBN 978-80-210-9270-9, str. 30.

výrazného využití informačních a komunikačních technologií jakožto významného prostředku k jejímu páchání“.[96]



Graf 1 - Narůstající trend kybernetické kriminality

Na grafu 1[97] můžeme vidět statistiku spáchaných kybernetických trestných činů vedenou Policií ČR, jenž je od doby svého vzniku v roce 2011 na vzestupném trendu stejně tak jako v celém světě.[98]

Nejedná se však o nový druh kriminality, jelikož velká část kybernetických trestných činů je obdobou již dobře známých druhů protiprávního jednání (např. podvody, porušování autorských práv, krádeže aj.) s tím rozdílem, že jsou páchány v digitálním prostředí, ve kterém je to pro pachatele výhodnější.[99] Výhodnější proto, že objasňování kyberkriminality je kvůli vlastnostem prostředí, ve kterém se odehrává, značně obtížné, a navíc v kyberprostoru lze v dnešní době kvůli závislosti společnosti na ICT napáchat daleko větší škody, což znamená i vyšší zisk pro kyberzločince. V neposlední řadě kyberprostor rovněž umožnuje cílit útoky nikoli pouze na jednotlivce, ale i na masy potencionálních obětí.

Dalo by se tedy říct, že jde o evoluci kriminality, jelikož pachatelé, co se nepřizpůsobí novým trendům riskují daleko vyšší riziko dopadení a menší zisk než pachatelé, co se přesunuli do kyberprostoru. Níže přiložená tabulka 2[100] ilustruje srovnání průměrného ozbrojeného přepadení a průměrného kybernetického útoku.

---

[96] Kyberkriminalita. *Policie ČR* [online]. [cit. 12.12.2021]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx
[97] Kyberkriminalita. *Policie ČR* [online]. [cit. 12.12.2021]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx
[98] Kyberkriminalita na vzestupu. *Eurozprávy* [online]. 10.2.2020. [cit. 12.12.2021]. Dostupné z: https://eurozpravy.cz/domaci/zivot/kyberkriminalita-na-vzestupu-obetmi-jsou-stale-casteji-deti-udelejte-si-test.d47c0d49/
[99] KOLOUCH, Jan. *Cybercrime*. 1. vyd. Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8, str. 181.
[100] JIROVSKÝ, Václav. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, ISBN 978-80-247-1561-2, str. 30.

Tabulka 2 - Srovnání ozbrojeného přepadení a kybernetického útoku

Parametr	Průměrné ozbrojené přepadení	Průměrný kybernetický útok
Riziko	Pachatel riskuje, že bude zraněn či zabit.	Bez rizika fyzické újmy
Zisk	Průměrně 3–5 tisíc USD.	Průměrně 50–500 tisíc USD.
Pravděpodobnost dopadení	Dopadeno 50–60 % útočníků.	Dopadeno cca 10 % útočníků.
Pravděpodobnost odsouzení	Odsouzeno 95 % dopadených útočníků.	Z dopadených útočníků dojde k soudnímu projednávaní pouze u 15 % útočníků a z nich je odsouzeno jen 50 %.
Trest	Průměrně 5–6 let, pokud pachatel při loupeži nikoho nezranil.	Průměrně 2–4 roky.

Digitální stopy ale nejsou zneužívány pouze v rámci kybernetické trestné činnosti. Odcizené osobní údaje se zneužívají i pro klasické trestné činy jako například podvody. Na získání digitálních stop od obětí používají útočníci různé metody, přičemž u některých využívají i techniky sociálního inženýrství.

Jako nejčastější kybernetické útoky, které bývají spojovány se zneužitím digitálních stop jsou uváděny: **krádež identity**, **phishing**, **kyberšikana** a **kyberstalking**. Samotnou kapitolu zde věnuji i **sniffingu**, kterým se budu dále zabývat v praktické části práce.

4.4.1 Krádež identity

Krádež identity je podvodné jednání, kdy se někdo vydává za jiného člověka s cílem získat finanční prostředky, důležité informace nebo jiné výhody.[101] V praxi to znamená zmocnění se přístupových údajů k uživatelskému účtu oběti (email, internetové bankovnictví, profil na sociální síti atd.), nebo citlivých údajů oběti

[101] SOUČKOVÁ, Tereza. Krádež identity. *Policie ČR* [online]. 25.5.2010. [cit. 2.1.2022]. Dostupné z: https://www.policie.cz/clanek/ztrata-identity.aspx

(občanský průkaz, údaje platební karty), útočníkem, který se následně vydává za oběť.[102]

Obětem v takovém případě hrozí, že přijdou o peníze nebo jiné prostředky na svých účtech a budou zodpovídat za nezaplacené výdaje, škody, půjčky, dokonce i trestné činy, které útočník napáchal pod jejich identitou. O to horší je potom fakt, že je pro oběti velmi těžké dokazovat, že takto jednali útočníci, kteří se zmocnili jejich identit.[103]

Ukradené virtuální identity bývají nejčastěji zneužívány k:[104]

- Provádění phishingových či malwarových útoků v rámci seznamu uživatelů, které má osoba s odcizenou identitou v seznamu kontaktů.
- Rozesílání spamu.[105]
- Zisku informací, které nejsou veřejně dostupné.
- Získávání přístupu do dalších služeb. Řada online služeb umožňuje, pouze na základě zadání emailové adresy, změnu hesla. Pokud se tedy útočník zmocní emailové schránky napadeného, může jednoduše získat přístup k dalším službám, které jsou na napadenou emailovou schránku navázány.

Pod krádež identity patří i jednání, kdy útočník využije nasbíraná data pro to, aby založil duplicitní profil oběti na sociální síti a vydával se zde za ní. Cílem takového jednání může být kyberšikana, podvod, nebo může jít o způsob, jak se dostat k dalším citlivým údajům.[106]

Finanční ztráty spojené s krádeží identity za rok 2016 USA dosáhly výše 16 miliard dolarů. Jedná se tedy o velmi výnosný druh počítačové kriminality.[107]

---

[102] Krádež identity. *Internetem bezpečně* [online]. [cit. 2.1.2022]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybersikana/kradez-identity/

[103] SOUČKOVÁ, Tereza. Krádež identity. *Policie ČR* [online]. 25.5.2010. [cit. 2.1.2022]. Dostupné z: https://www.policie.cz/clanek/ztrata-identity.aspx

[104] KOLOUCH, Jan. *Cybercrime*. 1. vyd. Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8, str. 319.

[105] *„Spam“* – nevyžádané sdělení masově šířené internetem.

[106] Krádež identity. *Internetem bezpečně* [online]. [cit. 2.1.2022]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybersikana/kradez-identity/

[107] Krádež identity. *Eset* [online]. [cit. 2.1.2022]. Dostupné z: https://www.eset.com/cz/kradez-identity/

Dopuštění se krádeže identity může dojít k naplnění skutkové podstaty některého z těchto trestných činů:[108]

- § 182 TZK[109] – porušení tajemství dopravovaných zpráv.
- § 209 TZK – podvod.
- § 230 TZK – neoprávněný přístup k počítačovému systému a nosiči informací.
- § 231 TZK – opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat.

4.4.2 Sociální inženýrství

Sociální inženýrství je ve své podstatě způsob manipulace s lidmi, za účelem získání informací nebo nenápadnému donucení k určitému jednání, která využívá lidské naivity, neobezřetnosti a hlouposti. Útočník tak uvádí oběť do omylu, aby od ní získal, co potřebuje.[110]

Hlavní myšlenkou sociálního inženýrství je nevyužívat složité technické postupy jako například prolomení hesla, když je mnohem jednoduší oklamat oběť, která ho dobrovolně prozradí.[111]

Úspěch této manipulace spočívá v důvěřivosti a neuvědomělosti oběti, nejzranitelnější jsou proto masy nezkušeních a neznalých lidí, kteří nemají přehled o nebezpečích ICT.[112] Typickým útokem cílícím na tuto skupinu, využívající metod sociálního inženýrství, za účelem získání osobních údajů, je phishing.

4.4.3 Phishing

Phishing je podvodnou technikou, která využívá ICT technologie a techniky sociálního inženýrství k získávání citlivých údajů.

---

[108] Krádež identity. *Internetem bezpečně* [online]. [cit. 2.1.2022]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybersikana/kradez-identity/
[109] „TZK“ – Zákon č. 40/2009 Sb., *zákon trestní zákoník* v posledním znění.
[110] Sociální inženýrství. *Internetem bezpečně* [online]. [cit. 19.12.2021]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/podvodne-praktiky/socialni-inzenyrstvi/
[111] KOLOUCH, Jan. *Cybercrime*. 1. vyd. Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8, str. 186.
[112] KOLOUCH, Jan. *Cybercrime*. 1. vyd. Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8, str. 192.

V **užším slova smyslu** je to jednání, které po uživateli vyžaduje navštívení podvržené webové stránky (zobrazující např. stránku internetového bankovnictví, online obchodu aj.) a následné zadání přihlašovacích údajů, případně jsou tyto informace vyžadovány přímo (např. formou vyplnění formuláře aj.).[113]

Princip typického phishingového útoku spočívá v zaslání na první pohled věrohodné žádosti, která uživatele vybízí k nějaké akci (přechod na podvrženou stránku a vyplnění údajů, otevření přiloženého souboru s malware),[114] a k tomu ho i nějakým způsobem motivuje (pokud uživatel neuposlechne výzvu, bude mu automaticky smazán/zablokován účet atd.).

Phishing se původně šířil emailem jako spam, ale v dnešní době se s ním lze setkat i na sociálních sítích, internetových fórech nebo chatovacích platformách jako telegram, messenger atd. Tento typ útoku je cílen na masy, je navržen tak aby zasáhl co nejvíce lidí. Autor Jan Kolouch ho přirovnává ke *„kobercovému bombardování“*, jelikož stejně jako při bombardování cílí phishing na neurčené množství cílů, aby měl útočník vyšší naději na úspěch.[115]

V **širším slova smyslu** se jako phishing dá označit jakékoli podvodné jednání, které má v uživateli vzbudit důvěru, snížit jeho ostražitost či jej jinak donutit akceptovat scénář předem připravený útočníkem.[116]

Speciálními formami phishingu jsou jednání, které označujeme jako pharming, spear phishing, vishing a smishing.

Pharning – jedná se o sofistikovanější a nebezpečnější formu phishingu. Jde o útok na DNS[117] server, na kterém útočníci změní IP adresu původní stránky na svojí podvrženou stránku. V momentě, kdy uživatel zadá v internetovém prohlížeči webovou adresu, dojde k překladu zadané URL na IP adresu podvržené stránky a na tu je uživatel následně přepojen. Takto podvržené stránky bývají zpravidla

[113] KOLOUCH, Jan. *Cybercrime*. 1. vyd. Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8, str. 246.
[114] *„Malware“* – označení pro škodlivý software. Souhrnně se tak označují počítačové viry, trojské koně, adware, spyware apod.
[115] *tamtéž*
[116] *tamtéž*
[117] *„DNS“* – anglicky *„Domain Name System“*, v českém překladu *„systém doménových jmen“*. Jedná se o systém, který překládá názvy domén webových stránek na IP adresy.

k nerozeznání od originálních. Pokud na těchto stránkách uživatel zadá své citlivé údaje, získávají je útočníci.[118]

Spear phishing – jde o formu phishingu, která cílí na konkrétní skupinu, organizaci, nebo jednotlivce, tedy na data, které tyto subjekty vlastní. Útočníci nejčastěji přes podvodnou zprávu navážou kontakt s někým z organizace, a přes něj pak získávají informace a šíří další zprávy dovnitř.[119]

Vishing – vishing je telefonickým phishingem, při kterém se útočník za pomoci technik sociálního inženýrství snaží od oběti získat citlivé informace. Útočníci se zpravidla vydávají za důvěryhodnou osobu (zástupce banky, známe instituce atd.) a oběti oslovují kvůli nějaké fiktivní naléhavé záležitosti.[120]

Smishing – jedná se o phishing šířený přes SMS zprávy.[121]

Jednání, které má povahu phishingu lze postihnout dle § 209 TZK – podvod. V případech, kdy je součástí phishingového útoku malware lze jednání postihnout i dle § 230 TZK – neoprávněný přístup k počítačovému systému a nosiči informací). Ve specifických případech lze využít i ustanovení § 234 TZK – neoprávněné opatření, padělání a pozměnění platebního prostředku.[122]

4.4.4 Sniffing

Sniffing (česky čmuchání) je jednou z metod, jak se bez interakce s uživatelem dostat k jeho digitálním stopám, ze kterých lze extraktovat citlivé údaje.

Jedná se o odposlech dat – přesněji TCP paketů, procházejících počítačovou sítí pomocí tzv. snifferu, což je program, který slouží k monitorování sítě. Útočník s jeho pomocí může získat jak informace ohledně provozu v síti, tak i samotný obsahu komunikace, která v ní probíhá. Z bezpečnostního hlediska je sniffing

[118] KOLOUCH, Jan. *Cybercrime*. 1. vyd. Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8, str. 263.
[119] KOLOUCH, Jan. *Cybercrime*. 1. vyd. Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8, str. 264.
[120] Vishing. *Eset* [online]. 25.8.2021. [cit. 2.1.2022]. Dostupné z: https://www.eset.com/cz/blog/hrozby/vishing-jak-ho-rozeznat-a-vyhnout-se-mu/
[121] Smishing. *Kaspersky* [online]. [cit. 2.1.2022]. Dostupné z: https://www.kaspersky.com/resource-center/threats/what-is-smishing-and-how-to-defend-against-it
[122] KOLOUCH, Jan. *Cybercrime*. 1. vyd. Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8, str. 263.

možné označit rovněž za monitorování provozu sítě a jde o standartní prostředek pro diagnostiku sítě používaný síťovými správci.[123]

Vlastní činnost správců není nelegální, neboť pomáhá k analyzování problémů a správě v počítačové síti. Nelegálním se sniffing stává v případě, že je monitorování sítě prováděno bez souhlasu či vědomí majitele sítě, popřípadě jejího uživatele.

Obzvláště nebezpečné je navštěvování webových serverů, využívajících síťových protokolů, které nešifrují komunikaci (například weby využívající HTTP protokol), jelikož ji sniffer může bez obtíží přečíst. Bezpečné weby využívají HTTPS protokol, který komunikaci mezi uživatelem a serverem šifruje a pro útočníka je tedy nečitelná, pokud nedisponuje znalostmi k prolomení šifrovacího algoritmu. Weby fungující na HTTP protokolu jsou v dnešních webových prohlížečích typicky označovány jako nezabezpečené a bývají vizuálně označeny.

Právě kvůli sniffingu je třeba dávat si velký pozor, pokud zadáváme citlivé údaje na stránku využívající HTTP protokol a jsme připojeni k veřejné síti (např. v restauraci, hotelu atd.), jelikož ty jsou pro odposlouchávání ideálním místem.[124]

Z hlediska trestního práva by bylo možné takové jednání označit jako nelegální odposlech a záznam telekomunikačního provozu a postihnout jako § 182 TZK – Porušení tajemství dopravovaných zprav.[125]

4.4.5 Kyberšikana

Informace z digitálních stop jsou rovněž zneužívány ke kyberšikaně, a to zejména náctiletými.[126]

[123] KOLOUCH, Jan. Cybercrime. 1. vyd. Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8, str. 294.
[124] ROMAJZL, Lukáš. Jak hacknout wifi síť. *Dotyk* [online]. 16.1.2015. [cit. 23.1.2022]. Dostupné z: https://www.dotyk.cz/publicistika/jak-hacknout-wi-fi-sit.html
[125] KOLOUCH, Jan. *Cybercrime*. 1. vyd. Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8, str. 294.
[126] Digitální stopa. *Internetem bezpečně* [online]. [cit.8.1.2022]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/dobre-vedet/digitalni-stopa/

Kyberšikana je druh šikany využívající zařízení ICT k ublížení druhým (vydírání, ubližování, ztrapňování, zastrašování apod.), přičemž jejími aktéry jsou stejně jako u klasické šikany agresor – oběť – přihlížející.[127]

Narozdíl od klasické šikany, u kyberšikany útočníci vystupují zpravidla pod anonymními profily, což jim dodává odvahu k agresivnějším formám útoku. V kyberprostoru rovněž nezáleží na věku, pohlaví, fyzické síle, nebo na sociálním postavení útočníka, hlavní roli hrají znalosti a dovednosti ve využívání ICT. Útoky v kyberprostoru mohou přijít kdykoli a odkudkoli (myšleno z libovolného kanálu jako SMS, chat, sociální síť atd.), těžko tedy odhadnout kdy a kde k dalšímu útoku dojde. Dalším rozdílem je, že u kyberšikany přihlížející aktivně pomáhají agresorovi v šíření závadného obsahu, což se značně podepisuje na negativním psychickém dopadu na oběť.[128]

Jelikož kyberšikana probíhá primárně v rovině psychické, je těžké odhalit její dopady na oběti, nebo oběť samotnou. Oběť se často uzavře do sebe a přestane komunikovat se svým okolím. Úskalím kyberšikany je, že díky možnostem ICT nemusí teoreticky nikdy skončit. Vymazaný závadný obsah, nebo zablokované profily útočníků nejsou překážkou k tomu, aby byl závadný obsah znovu nahrán, nebo aby byly vytvořeny nové profily.[129]

Mezi formy kyberšikany patří:[130]

- **Publikace záznamu** – zveřejnění videa, audia, online komunikace, který oběť zesměšňuje, narušuje její soukromí, nebo ji zachycuje při páchaném aktu šikany či násilí.
- **Falšování identity** – vytváření falešných profilů útočníků a obětí na sociálních sítích za účelem zesměšňování, ztrapňování oběti.
- **Krádeže identity** – útočníci zjistí nebo prolomí heslo oběti k jejímu účtu na sociální síti a prostřednictvím ukradené identity oběť poškozují.
- **Ponižování a pomlouvání.**

[127] Kyberšikana. *Internetem bezpečně* [online]. [cit. 8.1.2022]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybersikana/
[128] *tamtéž*
[129] *tamtéž*
[130] PAPEŽOVÁ, Zdeňka. PREVENCE – Kyberšikana. *Policie ČR* [online]. [cit. 8.1.2022]. Dostupné z: https://www.policie.cz/clanek/prevence-kybersikana.aspx

- **Provokování a napadání uživatelů v online komunikaci.**
- **Zveřejňování cizích tajemství s úmyslem poškodit oběť.**
- **Obtěžování.**

Kyberšikana je společně s kybergroomingem, sextingem a kyberstalkingem řazena do kategorie kybernetických útoků páchaných na sociálních sítích. Sociální sítě jsou totiž prostředím, které na kterých se tento druh kyberkriminality primárně odehrává.[131]

Kyberšikana není sama o sobě trestným činem ani přestupkem, proto je vždy třeba posuzovat, zdali agresorovo jednání nenabylo skutkové podstaty nějakého trestného činu nebo přestupku uvedeného v zákonech. Pokud má například kyberšikana podobu vydírání, zastrašování či pomluvy, pak je možno na agresorovo jednání aplikovat § 175 TZK – Vydírání, § 353 – nebezpečné pronásledování, či § 184 TZK – pomluva.[132] Postihy za krádež identity jsou popsány v kapitole *„krádež identity“*.

4.4.6 Kyberstalking

Poslední kategorií kybernetických útoků, zneužívajících digitální stopy, kterou budu v toto práci rozebírat, je kyberstalking. U kyberstalkingu stejně jako u kyberšikany existuje ekvivalent stejného jednání v reálném světě namísto v kyberprostoru, a sice stalking.

Stalking je termín, který označuje opakované, dlouhodobé, systematické a stupňované obtěžování, které může mít řadu různých forem a různou intenzitu. Pronásledovatel svou oběť například dlouhodobě sleduje, bombarduje SMS zprávami, e-maily, telefonáty či nechtěnými pozornostmi (dárky). Útočník u oběti vyvolává pocity strachu.[133]

[131] KOLOUCH, Jan. *Cybercrime*. 1. vyd. Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8, str. 309.
[132] KOLOUCH, Jan. *Cybercrime*. 1. vyd. Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8, str. 312.
[133] KOPECKÝ, Kamil a Veronika KREJČÍ. *Rizika virtuální komunikace* [online]. Olomouc: NET UNIVERSITY, 2010. [cit. 12.1.2022]. ISBN 978-80-254-7737-3. Dostupné z: http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=9%3Astudie-o-stalkingu-a-kyberstalkingu

Až ve spojení s využitím ICT u útočníka hovoříme o kyberstalkingu. V tomto případě stalker pro komunikaci s obětí využívá instant messengerů, chatů, VoIP[134] technologií, sociálních sítí apod. Ryzí kyberstalkeři, kteří k pronásledování využívají pouze informační a komunikační technologie, se na rozdíl od klasických stalkerů nikdy neuchylují k fyzickému útoku. Kyberstalking však může být pouze doprovodný jev stalkingu, takže každý stalker může být zároveň kyberstalkerem.[135]

Pro kyberstalkery je typická jejich vytrvalost a systematičnost při pronásledování jejich oběti, a obvykle mají pro tento účel vytvořenou řadu falešných identit které používají pro komunikaci s obětí.[136]

Z hlediska digitálních stop je u kyberstalkingu zajímavé, že někteří kyberstalkeři sbírají na internetu, popřípadě od ostatních uživatelů na internetu informace o své oběti, které pak mohou oběti servírovat, aby demonstrovali svojí moc (typu vím kde jsi, co děláš, vidím tě apod.) a vyvolali v ní pocity strachu. Stejně tak se někteří kyberstalkeři uchylují ke kyberšikaně oběti a tyto informace (které mohou být citlivé) zveřejňují na sociálních sítích, kradou oběti její virtuální identity a zneužívají je v její neprospěch, šíří o oběti pomluvy, technicky zdatní kyberstalkeři se mohou uchýlit i k nasazení malwaru a sledovat oběti přes speciální programy (spyware).[137]

Pokud se podíváme na profil agresorů, nejčastěji jsou to bývalí partneři obětí a z 87 % celkového počtu stalkerů jsou útočníky muži. Ovšem z pohledu závažnosti stalkingu jsou problematičtějšími útočníky ženy – kvůli jejich cílevědomosti a systematičnosti.[138]

---

[134] *„VoIP“* – anglicky *„voice over internet protocol“*, v českém překladu *„protokol přenosu hlasu internetem“*.
[135] KOPECKÝ, Kamil a Veronika KREJČÍ. *Rizika virtuální komunikace* [online]. Olomouc: NET UNIVERSITY, 2010. [cit. 12.1.2022]. ISBN 978-80-254-7737-3. Dostupné z: http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=9%3Astudie-o-stalkingu-a-kyberstalkingu
[136] KOLOUCH, Jan. *Cybercrime*. 1. vyd. Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8, str. 318.
[137] KOPECKÝ, Kamil a Veronika KREJČÍ. *Rizika virtuální komunikace* [online]. Olomouc: NET UNIVERSITY, 2010. [cit. 12.1.2022]. ISBN 978-80-254-7737-3. Dostupné z: http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=9%3Astudie-o-stalkingu-a-kyberstalkingu
[138] *tamtéž*

Stalking a kyberstalking je trestněprávně postižitelné jednání, které lze subsumovat pod § 354 TZK – nebezpečné pronásledování, a v některých případech i pod § 353 TZK – nebezpečné vyhrožování.[139]

[139] KOPECKÝ, Kamil a Veronika KREJČÍ. *Rizika virtuální komunikace* [online]. Olomouc: NET UNIVERSITY, 2010. [cit. 12.1.2022]. ISBN 978-80-254-7737-3. Dostupné z: http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=9%3Astudie-o-stalkingu-a-kyberstalkingu

Praktická část

5 Vymezení cílů a metodologie

V praktické části této práce bych chtěl na názorném příkladu ukázat, jaká data lze získat odposlechem nezabezpečené HTTP komunikace. Tato data, odeslaná ze smartphonu, ukořistím z lokální bezdrátové sítě (WLAN), ke které je smartphone připojen.

Hlavním cílem praktické části této práce je analyzovat odchycenou síťovou komunikaci a digitální stopy v ní obsažené za pomoci open source softwaru. Vedlejším cílem je vysvětlení postupu pro odposlouchávání lokální bezdrátové sítě.

Pro vysvětlení postupu odposlouchávání bezdrátové sítě byla použita deskriptivní metoda (popis). Na rozbor digitálních stop v odchycených datech, pak analytická metoda.

Předpoklady:

- Odposlouchávající zařízení bude odposlouchávat sledované zařízení. Celkem zde tedy budou figurovat dvě zařízení.
- Odposlech bude proveden v lokální bezdrátové síti (WLAN), do které se sledované zařízení připojí.
- Bezdrátová síť, na které bude odposlech proveden bude zabezpečena WPA2 šifrováním s PSK autentizací.
- Heslo k bezdrátové síti je známo.
- Sledovaným zařízením bude smartphone.
- Sledovaný smartphone bude komunikovat skrze webový prohlížeč s webovým serverem prostřednictvím HTTP protokolu.
- Ze sledovaného smartphonu bude odeslán HTTP POST požadavek obsahující osobní údaje.

6 Použité nástroje

6.1 Použitý software

Odposlech jsem prováděl v Kali Linuxu virtualizovaném přes VirtualBox ve Windows 10, nicméně virtualizace není nutným předpokladem a odposlech lze provádět z pevně nainstalovaného, nebo live boot Kali OS.[140] Tento operační systém jsem si vybral proto, že v něm (a v ostatních Linuxových distribucích) na rozdíl od Windows lze jednoduše přepnout bezdrátový síťový adaptér do monitorovacího módu, což je nezbytný předpoklad pro sledování bezdrátové sítě. Ve Windows není tato funkce u většiny síťových adaptérů podporována kvůli limitům jejich ovladačů.[141]

- **Odposlouchávající zařízení**
  - **VirtualBox** (verze 6.1.32) – je volně dostupný open-source virtualizační software od společnosti Oracle, distribuovaný pro všechny velké operační systémy jako Windows, Mac, Linux atd. Slouží k virtualizaci operačních systémů.[142]
  - **Kali** (verze 2022.1) – je open-source Linuxová distribuce odvozená od Debian Linuxu, vybavená nástroji a sloužící zejména k penetračnímu testování, počítačové forenzní analýze, reverzní inženýrství a obecně k etickému i neetickému hackování.[143]
  - **Wireshark** (verze 3.6.0) – je open-source software sloužící k analýze síťových protokolů, distribuovaný pro všechny velké operační systémy jako Windows, Mac, Linux atd. Umožňuje podrobné sledování provozu v počítačových sítích, a mimo monitorování se využívá k vyhledávání, diagnostice a odstraňování problémů v sítích. Mimo jiné podporuje

[140] OS – operační systém
[141] Ovladač – anglicky *„Driver“* je označení pro software, pomocí kterého pracuje operační systém s připojeným hardware.
[142] VirtualBox. *VirtualBox* [online]. [cit. 22.2.2022]. Dostupné z: https://www.virtualbox.org/
[143] Kali. *Kali* [online]. [cit. 22.2.2022]. Dostupné z: https://www.kali.org/

i zachytávání dat z Wi-Fi sítí. Může být zneužit k nelegálnímu sniffingu.[144]

- **Sledovaný smartphone**
  - **EMUI** (verze 11.0.0) – je proprietární nástavba mobilního open-source operačního systému Android 10, vyvíjený společností Huawei, která jím vybavuje svoje produkty.[145]
  - **Brave** (verze 1.35.103) – je open-source webový prohlížeč vyvíjený společností Brave software, založený na webovém prohlížeči chromium (Chrome).[146]

6.2 Použitý hardware

U odposlouchávajícího zařízení má cenu zmínit pouze použitý síťový adaptér, jelikož ne všechny Wi-Fi adaptéry podporují, nebo jsou vhodné pro monitorovací režim, který je pro odposlech bezdrátových sítí nezbytný. Ostatní komponenty v použitém zařízení nemají na tuto činnost jakýkoliv významný vliv.

- **Odposlouchávající zařízení**
  - **TP-LINK Archer T9UH** (verze 1) – je Wi-Fi síťový adaptér připojovaný přes rozhraní USB. Adaptér využívá čipovou sadu Realtek RTL8814AU, která v Linuxu umožňuje režim monitorování sítě. Tento adaptér jsem zvolil, jelikož je označován jako jeden z nejlepších pro síťové odposlechy.[147]
- **Sledovaný smartphone**
  - **Huawei Mate 20 pro** – je smartphone od společnosti Huawei. Podrobnosti o konfiguraci zařízení lze najít například na webu „*www.gsmarena.com*“.

[144] Wireshark. *Wireshark* [online]. [cit. 22.2.2022]. Dostupné z: https://www.wireshark.org/
[145] EMUI. *Wikipedia* [online]. 8.2.2022. [cit. 22.2.2022]. Dostupné z: https://en.wikipedia.org/wiki/EMUI
[146] Brave. Wikipedia [online]. 12.7.2021. [cit. 22.2.2022]. https://cs.wikipedia.org/wiki/Brave_(webový_prohlížeč)
[147] Archer T9UH. *tp-link* [online]. [cit. 22.2.2022]. https://www.tp-link.com/cz/home-networking/adapter/archer-t9uh/

7 Odposlech a analýza dat

7.1 Konfigurace Kali

V první řadě je třeba říci, že pokud chceme ke sledování bezdrátové sítě využít virtualizovaný Linux nebo jiný OS, je třeba pro záchyt dat použít bezdrátový USB síťový adaptér, a ten poté přes virtualizační software připojit virtuálního OS. Síťová karta připojená do základní desky nebude ve virtuálním OS pro účely monitorování sítě fungovat, jelikož s ní bude vždy fyzicky pracovat pouze nativní OS. Pokud tedy chceme pro odposlech využít síťovou kartu, musíme si OS, na kterém budeme provádět odposlech, nainstalovat napevno.

Kali OS je volně dostupný a lze si ho stáhnout v několika různých variantách z „*https://www.kali.org/get-kali/*“. Po provedení instalace OS je potřeba připojit se k internetu, abychom mohli stáhnout potřebné ovladače pro síťový adaptér. U fyzicky nainstalovaného OS toho docílíme připojením ethernetového kabelu do sítě, u virtuálního OS je potřeba přidat síťovou kartu v nastavení virtualizačního softwaru.

Uživatelské rozhraní Kali (viz obrázek 5 níže) je intuitivní a velmi podobné Windows. V horní části plochy se nachází lišta, jejíž funkce jsou zleva doprava: start menu, panel oblíbených aplikací, panel pro přepínání ploch, panel otevřených aplikací, panel správce úloh a systémový panel. Stejně jako ve Windows se na ploše nacházejí ikony souborů, a průzkumník souborů je zde rovněž velmi podobný.

Obrázek 5 - Uživatelské rozhraní Kali

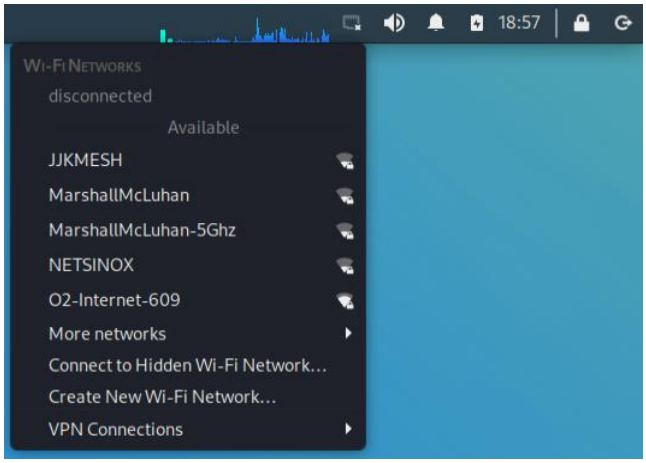
Po seznámení s uživatelským rozhraním Kali je potřeba zjistit čipovou sadu síťového adaptéru, který chceme pro odposlech využít. Tu můžeme zjistit přes Terminal, což je Linuxové CLI.[148] Doporučuji používat Root Terminal, jelikož ten se spouští s nejvyššími (Root) oprávněními, a tak nemusíme každý příkaz uvádět příkazem *„sudo“*, pro elevaci uživatelských oprávnění.

Pokud máme připojenou bezdrátovou síťovou kartu k základní desce, můžeme v Terminalu použít příkaz *„sudo lspci“*, který vyjede seznam připojených zařízení přes PCI,[149] ze kterého lze vyčíst čipovou sadu síťové karty. V případě připojeného USB síťového adaptéru můžeme použít příkaz *„sudo lsusb“*, který vyjede seznam připojených zařízení přes USB port. Na obrázku 6 níže můžeme vidět, že se v seznamu nachází USB síťový adaptér *„TP-Link Archer T9UH v1“* a čipová sada *„Realtek RTL8814AU“* je uvedena vedle v závorkách.

[148] CLI – anglicky *„Command Line Interface“*, v českém překladu *„příkazová řádka“*. Jedná se o uživatelské rozhraní, ve kterém uživatel komunikuje s programy nebo OS prostřednictvím příkazů, které zapisuje do řádky.
[149] PCI – anglicky *„Peripheral Component Interconnect“* je označení sběrnice základní desky pro připojení rozšiřujících počítačových komponent.

Obrázek 6 - Seznam připojených USB zařízení.

Přes získané označení čipové sady si lze na internetu vyhledat potřebný ovladač. Například *„googlením“* dotazu *„Realtek RTL8814AU Linux driver download*“ je mi hned jako první výsledek nabídnut odkaz na stránku *„https://github.com/morrownr/8814au“*, která obsahuje podrobný návod, jak ovladač nainstalovat. Postup, jak ovladač stáhnout a nainstalovat zde uvádět nebudu, jelikož ho lze najít na internetu. Po nainstalování ovladače je třeba restartovat systém.

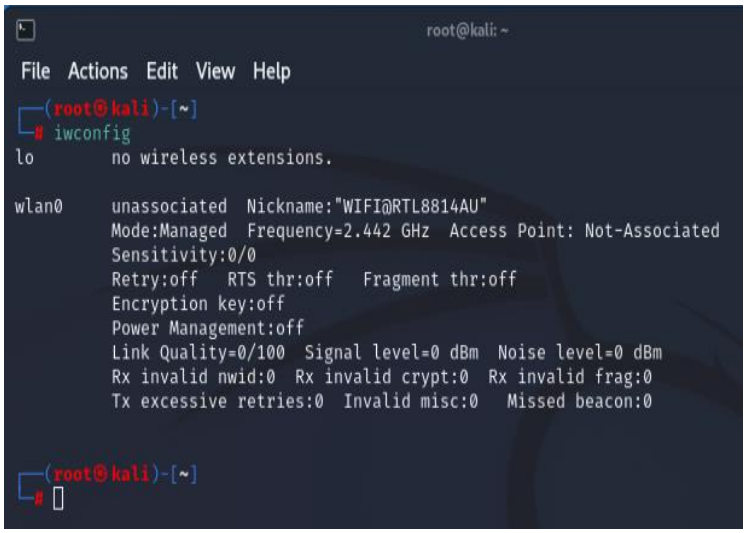


Obrázek 7 - Detekované Wi-Fi sítě

Pokud se instalace ovladačů podařila, tak by se v nabídce dostupných sítí (ikonka se nachází na liště v systémovém panelu) měly zobrazovat detekované Wi-Fi sítě z okolí, jako na obrázku 7. K sítím by se mělo jít bez problému připojit.

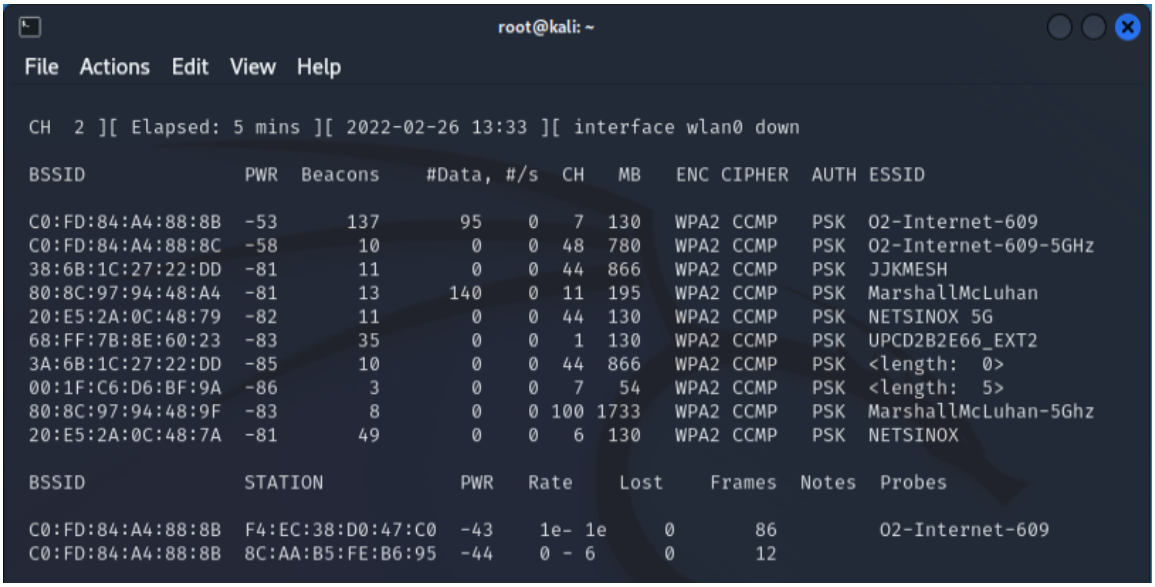
Pro zahájení odposlechu sítě je nyní třeba udělat ještě pár věcí – zjistit v jakém kanálu operuje Wi-Fi sít, kterou chceme odposlouchávat, dále ukončit procesy které, by mohli narušovat odposlech, a nakonec přepnout síťový adaptér do monitorovacího módu a nastavit mu kanál, v jakém operuje bezdrátová síť, kterou chceme odposlouchávat.

Pro zjištění kanálu sítě nejdřív potřebujeme zjistit název síťového rozhraní, které má náš bezdrátový síťový adaptér. Ten zjistíme zadání příkazu *„sudo iwconfig“* do Terminalu. Jak je vidět na obrázku 8, v mém případě se bezdrátové rozhraní jmenuje *„wlan0“*.



Obrázek 8 - Síťová rozhraní

Nyní můžeme zjistit na jakých kanálech operují dostupné Wi-Fi sítě. Zadáním příkazu „*sudo airodump-ng wlan0“*, kdy *„wlan0“* je názvem síťového rozhraní, se spustí utilita pro skenování bezdrátových sítí *„airodump“.*



Obrázek 9 - Airodump

Na obrázku 9 můžeme vidět, jaké informace nám utilita airodump poskytuje. Nejzajímavějšími jsou sloupce:

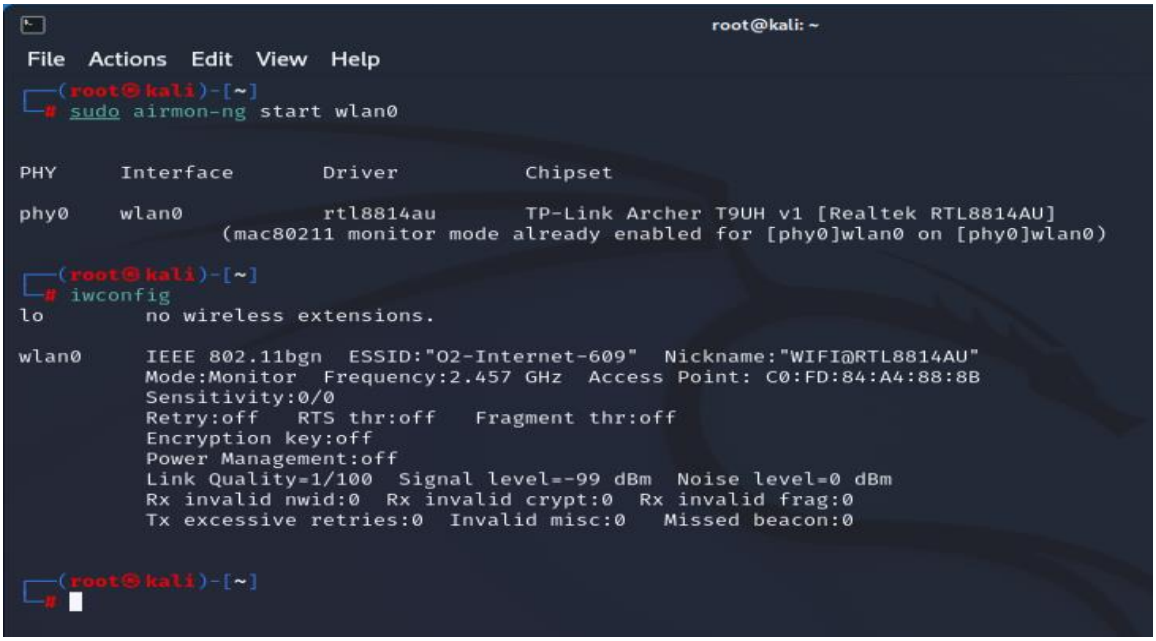
- **BSSID** – udává mac adresu AP.[150]

[150] AP – anglicky *„Access point“*, v českém překladu *„vstupní bod“*. Jde o zařízení, které Wi-Fi síť vysílá, nejčastěji router.

- **CH** – udává na jakém kanálu Wi-Fi síť operuje. Kanály udávají, na jaké frekvenci AP Wi-Fi síť vysílá. Kanál 1 například vysílá na frekvenci 2412 MHz, kanál 2 na 2417 MHz atd.
- **ENC** – udává jaký druh šifrování AP využívá.
- **AUTH** – udává jaký druh autentizace AP využívá.
- **ESSID** – udává název Wi-Fi sítě.

Síť, kterou chci sledovat, se jmenuje *„O2-Internet-609“* a podle informací, které poskytl airodump operuje na kanálu 7. Po získání potřebných dat, doporučuji restartovat systém, jelikož airodump zapíná pro své potřeby monitorovací mód, který narušuje sledování sítě ve Wiresharku, a na to, jak ho vypnout jiným způsobem, jsem nepřišel.

Dále je třeba spustit monitorovací mód a nastavit kanál síťového adaptéru. Zadáním příkazu *„sudo airmon-ng check“* do Terminálu se zobrazí procesy, které mohou zasahovat do fungování síťového adaptéru. Ty doporučuji příkazem *„sudo airmon-ng check kill“* ukončit, aby neměnily nastavení adaptéru, což může mít za následek problémy s odposlechem sítě. Zadáním příkazu *„sudo airmon-ng start wlan0“*, se spustí monitorovací mód síťového adaptéru. Zadáním příkazu *„sudo iwconfig“* si pak lze ověřit v jakém módu se síťový adaptér nachází (viz obrázek 10).



Obrázek 10 - Ověření monitorovacího módu

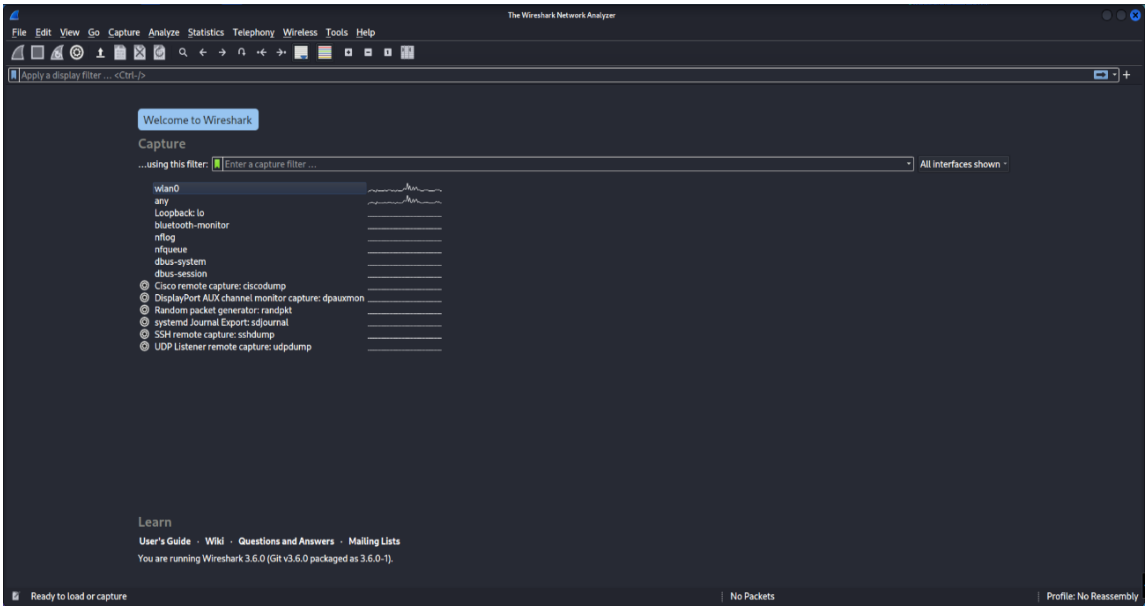
Zapnutím monitorovacího módu dojde k odpojení od připojených bezdrátových sítí, přičemž síťový adaptér začne ze vzduchu sbírat komunikaci ze všech bezdrátových sítí v dosahu, jež operují na stejné frekvenci.

Přepnutí kanálu lze provést příkazem *„sudo iwconfig wlan0 channel x“*, kdy za x dosadíme číslo kanálu, v mém případě tedy 7. Příkazem *„sudo iwlist wlan0 channel“* lze zkontrolovat na jaký kanál je síťový adaptér naladěn. V případě, že ve Wiresharku bude podezřele málo zachycených paketů ze sledované sítě, doporučuji zkontrolovat, zdali se nezměnil kanál, na který je nalazen síťový adaptér.

7.2 Odposlech sítě

Po úspěšném nastavení monitorovacího módu a nalazení správného kanálu lze začít s odposlechem sítě. Pro vizualizaci zachycené komunikace jsem se rozhodl použít program Wireshark, jelikož je nejpoužívanějším softwarem pro tyto účely a existuje na něj celá řada návodů a školících materiálů.

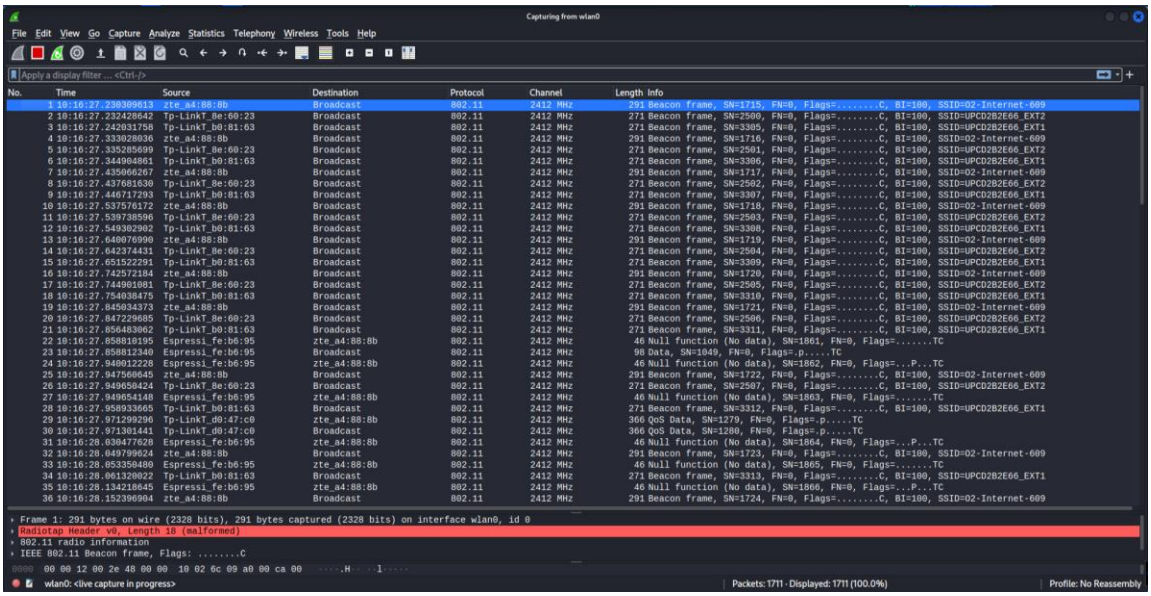
Wireshark bývá standardně dodáván jako základní softwarové vybavení Kali, tažе by se měl nacházet již nainstalovaný v systému. Pokud v systému nainstalováný není, na URL *„https://www.kali.org/tools/wireshark/“* lze najít návod jak ho nainstalovat do Kali.



Obrázek 11 - Úvodní obrazovka Wiresharku

Po spuštění Wiresharku se načte obrazovka se seznamem rozhraní zachytávajících síťový provoz doprovozených grafem aktivity – viz obrázek 11 výše.

Po výběru rozhraní, na kterém chceme sledovat síťový provoz (v mém případě *„wlan0“*), by mělo dojít k načtení obrazovky zobrazující seznam zachycených paketů z bezdrátových sítí, operujících na odposlouchávaném kanálu, který se neustále aktualizuje o nová data (viz obrázek 12). Pokud je síťový kanál hodně vytížený, nově zachycená data přibývají do seznamu opravdu rychle, a bez použití filtrů je seznam velmi nepřehledný.



Obrázek 12 - Zachycené pakety

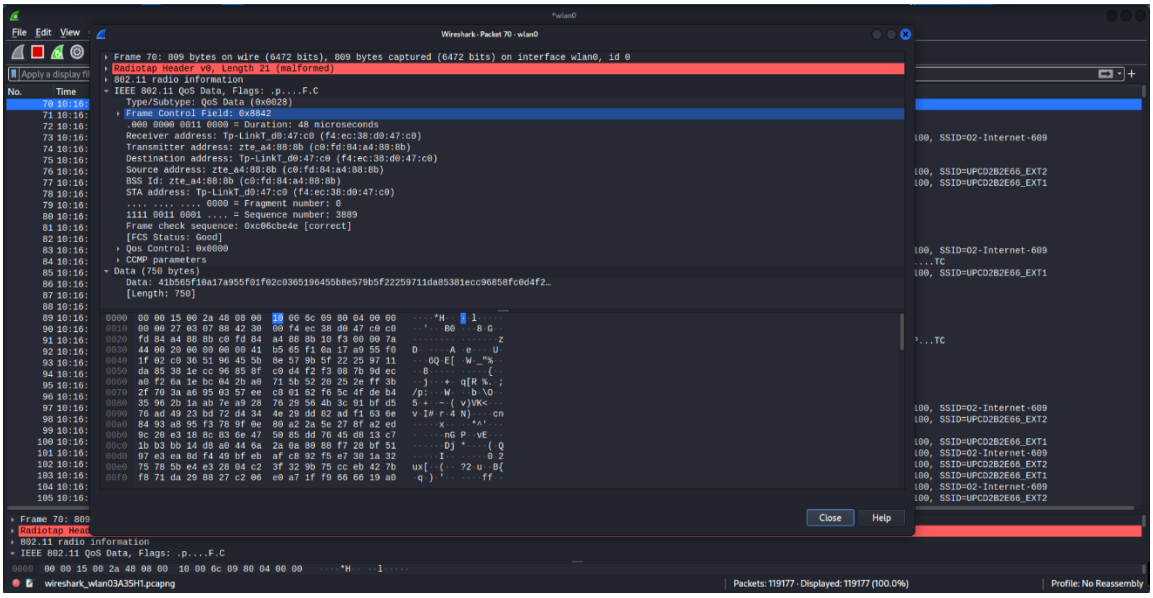
Sloupce zleva doprava udávají:

- **Time** – čas zachycení paketu.
- **Source** – zdroj, který paket vyslal.
- **Destination** – cíl, kam má paket dorazit.
- **Protocol** – síťový protokol komunikace.
- **Length** – bitová délka paketu.
- **Info** – dodatečné informace o paketu. Lze z něj například vyčíst SSID (název bezdrátové sítě).

Jelikož je odchycená komunikace zašifrovaná (síť používá WPA2 šifrování s PSK autentizací), tak se u všech zachycených paketů zobrazuje komunikační

protokol 802.11, čímž Wireshark obecně popisuje, že jde o bezdrátový přenos dat podle standardu IEEE 802.11.[151] Stejně tak zdroj vysílání i cíl kam má paket dorazit jsou označeny názvem síťového adaptéru nebo MAC adresou, namísto IP adresy, jelikož s těmito údaji pracuje protokol IEEE 802.11, na rozdíl od IP adresy, kterou využívá protokol IP.

Po rozkliknutí libovolného odchyceného paketu v seznamu se otevře okno obsahující detailní informace, včetně samotných dat, které paket obsahuje (viz obrázek 13).



Obrázek 13 - Detail paketu

Aby byl obsah zachycených paketů z bezdrátové sítě srozumitelný, je potřeba je dešifrovat. K tomu musíme v první řadě znát heslo k bezdrátové síti, a s jeho pomocí přidat do Wiresharku dešifrovací klíče. Podrobný návod, jak toho docílit lze nalézt na této URL: *„https://wiki.wireshark.org/HowToDecrypt802.11“*.

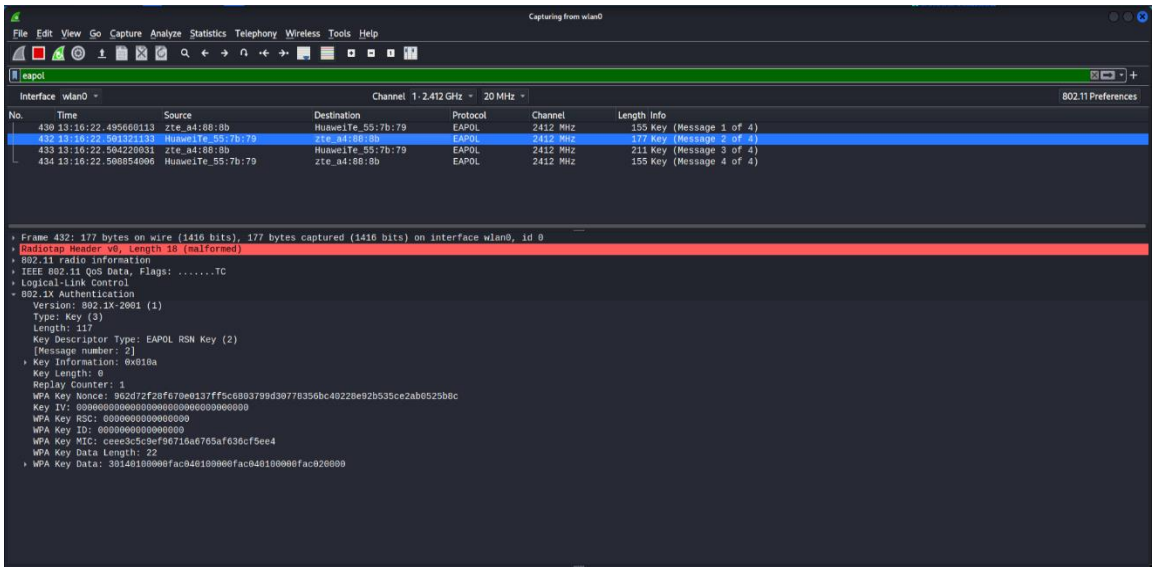
Samotné vytvoření dešifrovacích klíčů však pro PSK autentizaci nestačí. Ještě je třeba odchytit „*handshaky*“[152] mezi AP a novým zařízením, které se připojuje do bezdrátové sítě. AP s PSK autentizací totiž šifrují komunikaci s každým připojeným zařízením podle vygenerovaných šifrovacích klíčů, které si navzájem předají během autentizace, která probíhá při prvním připojení do sítě (pokud zařízení síť

[151] IEEE 802.2. *Wikipedia* [online]. 15.1.2022. [cit. 28.2.2022]. Dostupné z: https://cs.wikipedia.org/wiki/IEEE_802.2

[152] Handshake – v českém překladu *„potřesení rukou“* je v IT označení pro automatizované vyjednávání mezi zařízeními.

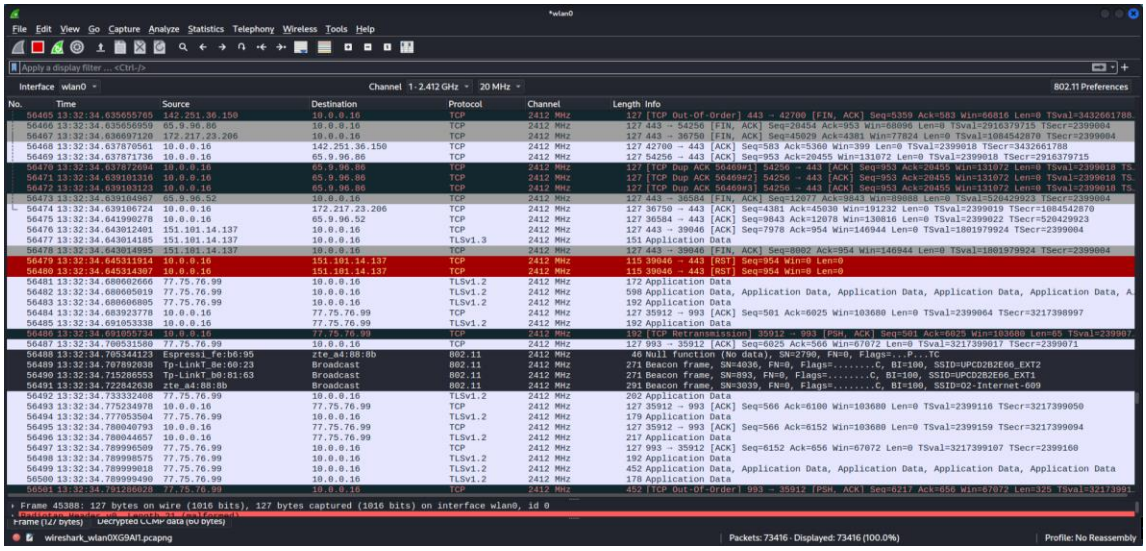
opustí a následně se opět připojí, proces se opakuje). Handshake probíhá formou čtyř navzájem vyměněných zpráv mezi AP a připojujícím se zařízení, a pro výměnu se používá síťový protokol EAPOL. Aby byl proces dešifrování úspěšný, je potřeba odchytit všechny čtyři zprávy.

Další postup je tedy takový, že smartphone, které chci sledovat, připojím do bezdrátové sítě. Abych se ujistil, že jsem odchytil všechny čtyři zprávy, vyfiltroval jsem si výsledky skenování tak, aby se mi zobrazila pouze komunikace protokolu EAPOL. V detailech odchycených zpráv pak mohou vidět i šifrovací klíče (viz. obrázek 14).

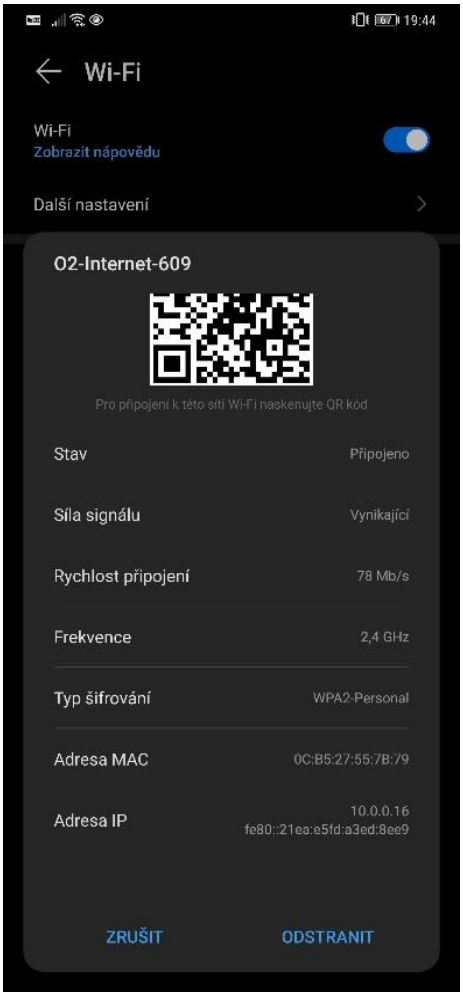


Obrázek 14 - Zachycené handshaky

Odchycení všech čtyř vyměněných EAPOL zpráv by mělo spustit automatické dešifrování komunikace mezi AP a sledovaným smartphonem. Po vyčištění filtru ve Wiresharku a přechodu na libovolný web ve sledovaném smartphonu je vidět zachycená komunikace standardních protokolů, používaných pro komunikaci v internetu (viz obrázek 15).



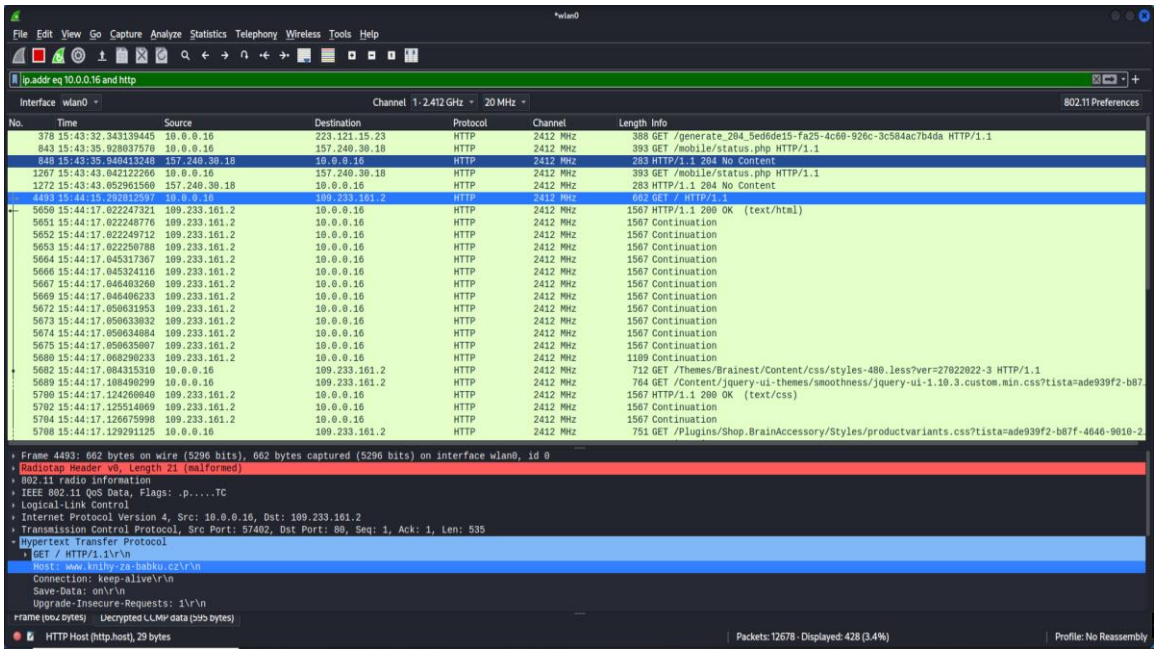
Obrázek 16 - Dešifrovaná komunikace



Obrázek 15 - IP adresa sledovaného smartphonu

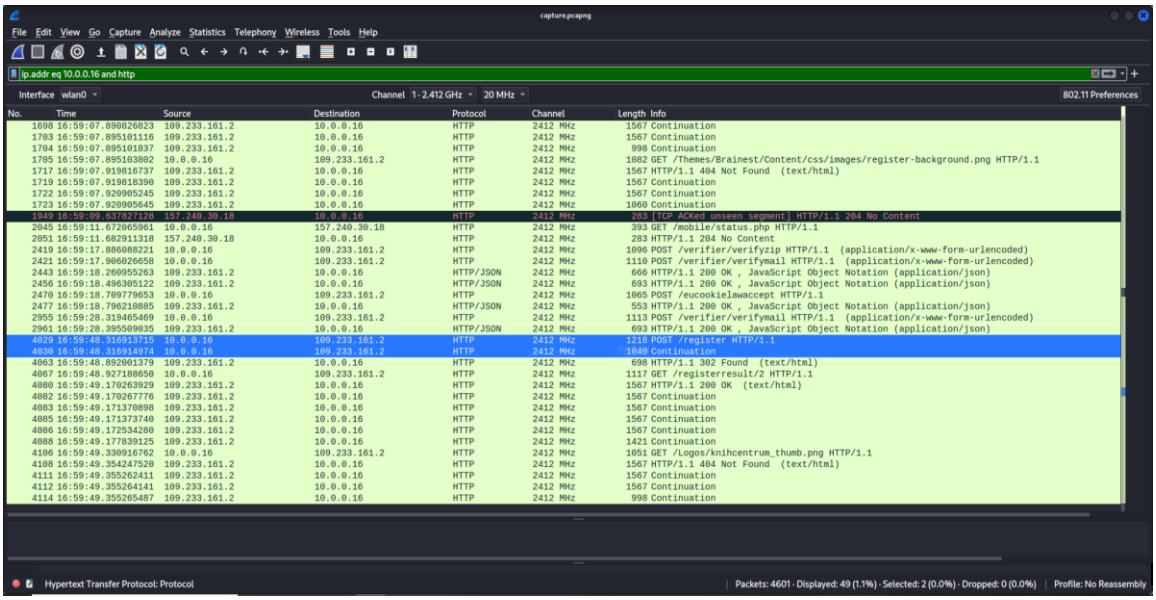
Nyní už můžu přejít na samotnou podstatu praktické části této práce, a tou je odchyt a analýza HTTP POST požadavku, který obsahuje digitální stopy. Abych se nemusel probírat zbytečně moc odchycenými pakety, mohu filtr upřesnit ještě tak, aby zobrazoval pouze výsledky z IP adresy sledovaného smartphonu (obrázek 16) a HTTP protokolu, příkazem: *„ip.addr eq 10.0.0.16 and http“*.

Nezabezpečeným webem, na který budu posílat HTTP POST požadavek obsahující citlivé údaje je: *„http://www.knihy-zababku.cz“*. Po přechodu na tento web sledovaným smartphonem došlo k naskakování zachycených HTTP zpráv ve Wiresharku. Jak je vidět na obrázku 17, zachycen byl HTTP GET požadavek o zaslání obsahu webové stránky s odpovědí od webového serveru.



Obrázek 18 - HTTP zprávy načteného webu

Na adrese *„http://www.knihy-za-babku.cz/register“* tohoto webu se nachází formulář registrace, který jsem na sledovaném smartphonu vyplnil a potvrdil. Odeslaná data byla vzápětí odchycena ve Wiresharku. Jak je vidět na obrázku 18, objem dat byl tak veliký, že se POST požadavek rozdělil do dvou paketů, přičemž údaje vyplněné do formuláře se skrývají v tom druhém. Pro snadnější analýzu jsem si tyto dva pakety uložil do JSON souboru, který rozeberu v následující kapitole.



Obrázek 17 - Zachycené HTTP POST pakety

7.3 Analýza digitálních stop

Data ze zachycených paketů HTTP POST požadavku, které budu v této kapitole analyzovat, lze najít v příloze 1 této práce, uložené ve formátu JSON, což je značkovací jazyk určený pro zápis dat do formy čitelné jak člověkem, tak strojem. Obsahem jsou data z vybraných paketů zachycených Wiresharkem, uložená do textových řetězců, na které se budu odkazovat číslem řádku.

První paket se nachází na řádcích 2–347, druhý paket na řádcích 348-642. Data v obou paketech jsou rozdělena do několika sekcí, přičemž každá obsahuje parametry s hodnotami, které danou sekci popisují.

- Řádky 3–27 u prvního paketu a 349–373 u druhého paketu obsahují obecné informace o paketech.
- Řádky 29–108 u prvního paketu a 375–454 u druhého paketu obsahují data *„Radiotap headeru“*, což jsou technické informace o bezdrátovém síťovém adaptéru, který paket zachytil.[153]
- Řádky 110–115 u prvního paketu a 456–461 u druhého paketu obsahují data o bezdrátové síti, ze které byly pakety zachyceny.
- Řádky 117–173 u prvního paketu a 463–519 u druhého paketu obsahují data protokolu IEEE 802.11.
- Řádky 176–193 u prvního paketu a 522–539 u druhého paketu obsahují data *„Logical link control“*, což je podvrstva linkové vrstvy protokolu IEEE 802.11, která zajišťuje součinnost různých síťových protokolů.[154]
- Řádky 195–223 u prvního paketu a 541–569 u druhého paketu obsahují data IP protokolu.
- Řádky 225–285 u prvního paketu a 571–631 u druhého paketu obsahují data TCP protokolu.
- Řádky 287–343 u prvního paketu a 633–637 u druhého paketu obsahují data aplikačního protokolu (v tomto případě HTTP).

[153] What are RadioTap Headers? *WiFiNigel* [online]. [cit. 28.2.2022]. https://wifinigel.blogspot.com/2013/11/what-are-radiotap-headers.html
154 Logical Link Control. *Wikipedia* [online]. 8. 8. 2021. [cit. 28.2.2022]. https://cs.wikipedia.org/wiki/Logical_Link_Control

Nyní k samotným digitálním stopám. Při analýze souboru jsem postupoval odshora dolu a vypsal čísla řádků, které obsahují digitální stopy, jež by mohli být potencionálně zneužity. Nutno podotknout, že veškerá data ze zachycených paketů jsou digitálními stopami proběhlé komunikace mezi odposlouchávaným smartphonem a webovým serverem.

Jelikož se většina dat mezi zachyceným pakety shoduje, vypíšu pouze ta, která se nachází v prvním paketu. Data, jež se mezi pakety neshodují se nacházejí v sekci aplikačního protokolu, a ta popíšu pro každý paket zvlášť.

- Řádek 14, parametr:[155] ***„frame.time“***, hodnota: ***„Feb 27, 2022 16:59:48.316913715 EST“*** – timestamp zachycení paketu ze sítě.
- Řádek 140, parametr: ***„wlan.addr“***, hodnota: ***„c0:fd:84:a4:88:8b“*** – MAC adresa AP.
- Řádek 141, parametr: ***„wlanaddr_resolved“***, hodnota: ***„zte_a4:88:8b“*** – název síťového adaptéru AP.
- Řádek 144, parametr: ***„wlan.addr“***, hodnota: ***„0c:b5:27:55:7b:79“*** – MAC adresa odposlouchávaného smartphonu.
- Řádek 145, parametr: ***„wlanaddr_resolved“***, hodnota: ***„HuaweiTe_55:7b:79“*** – název síťového adaptéru odposlouchávaného smartphonu.
- Řádek 172, parametr: ***„wlan.analysis.tk“***, hodnota: ***„a5b6467bdac9c09c4f938e5d824bc3e7“*** – TK klíč určený k šifrování/dešifrování přenášeného datového obsahu v paketech.[156]
- Řádek 173, parametr: ***„wlan.analysis.pmk“***, hodnota: ***„428b50abf84f6a78fc90af72f5121be8bc37e5159ea607a55cd97b2c6b67ece8“*** – PMK klíč určený k šifrování/dešifrování komunikace mezi zařízením a AP.[157]

[155] Parametr – pomocná proměnná pro ukládání vstupních hodnot.
[156] 4-WAY HANDSHAKE. *WiFi-professionals* [online]. 24.1.2019. [cit. 3.2.2022]. https://www.wifi-professionals.com/2019/01/4-way-handshake
[157] *tamtéž*

- Řádek 216, parametr: ***„ip.src“***, hodnota: ***„10.0.0.16“*** – IP adresa sledovaného smartphonu v lokální síti.
- Řádek 220, parametr: ***„ip.dst“***, hodnota: ***„109.233.161.2“*** – veřejná IP adresa cílového webového serveru, kam má být paket odeslán.

- **Data aplikačního protokolu prvního paketu** – zde se nacházejí informace o hlavičce HTTP POST požadavku, která obsahuje doplňující informace k samotným přenášeným datům.
  - Řádek 287, parametr: ***„http“***– informace o použití HTTP protokolu.
  - Řádek 295, parametr: ***„http.request.method“***, hodnota: ***„POST“*** – použitá metoda HTTP protokolu.
  - Řádek 299, parametr: ***„http.host“***, hodnota: ***„www.knihy-za-babku.cz“*** – webová adresa cílového webového serveru (host).
  - Řádek 314, parametr: ***„http.user_agent“***, hodnota: ***„Mozilla/5.0 (Linux; Android 10) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102 Mobile Safari/537.36“*** – user-agent header,[158] který obsahuje informace o zařízení, ze kterého byl HTTP požadavek odeslán.
  - Řádek 338, parametr: ***„http.request.full_uri“***, hodnota: ***„http://www.knihy-za-babku.cz/register“*** – plná URL adresa stránky, ze které požadavek odchází.

Veškeré digitální stopy, které byly dosud zmíněny, jsou digitálními stopami neovlivnitelnými. Vytvářejí je síťové protokoly, aby zařízení mohlo komunikovat v síti. Běžný uživatel obvykle ani netuší, že tyto informace o sobě a svém zařízení předává dál.

- **Data aplikačního protokolu druhého paketu** – zde se nacházejí samotná data z registračního formuláře. Jelikož se jedná o data, které

[158] User-Agent. Mozilla [online]. 18.2.2022. [cit. 1.3.2022]. https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/User-Agent

uživatel sám vytvořil a dobrovolně odeslal dál, tak jde o digitální stopy ovlivnitelné.

- Řádek 634, parametr: ***„http.file_data“***, hodnota: ***„__RequestVerificationToken=0XNsUCqfRpHgwNmQ9U3WifplWbmKsaJpKwmhTCVvVXSqMupCsDLmw-GqYiRZjV3jeukim8B9BPzZt6jIYlVEYicUPl41&Gender=M&FirstName=Max&LastName=Lagron&Company=Firma+1&StreetAddress=Ulice+123&City=Praha&ZipPostalCode=19000&Phone=%2B420123456789&Phone_mask=%2B420+123+456+789&Email=Email111%40test.cz&Password=abc123&ConfirmPassword=abc123&hpinput=&accept-privacy-policy=on&g-recaptcha-response=03AGdBq27mV9tHj4s_JCfy1f8UzG6Zl2LSafnCc-UBR6_dW-fO5YrZYO4Ejjxh_P_4ZvdsSxB1d70lHjDgN5F7fk570RZM-qubqqJAfeeRaKKbURbZva08Ctl8O0p-XSbCqkVS4eO7FMzmtP6FFlPiKZDk3g1eVhh2hmizJ7iUaEh2iMheZfylzKgdMf9GaqMxrlq6jPW4167alUxV-vNv8FDoDYva6WlYJTiuwYbvGNrkXQavOpaNNOXfFPL-_90HNugVlcqRThDXKzdiYSBcjeCjmn63KEqqZN9wBDhNITOEF8OGboeTUK2XEcrVsfPguqHwQUelccNPAmVOzuRh5-Q2oTarflCr5r8AUwH1e163THjpYkvfK8Wa_DR6zGEMtWJ4ILuyqvX5e56XtqCuhFPjXaZEmRBYoTEZhWbDeOTeYly0YNkM8PZqL5GWBZ-X7ltpXQZR1PocSdy1qqchmHyvTSoRcMAvCA&register-button=Registrovat“*** – informace z vyplněného formuláře. Data jsou spojena do jednoho řetězce, přičemž jednotlivé parametry s jejich hodnotami jsou zapsány ve formátu *„parametr1=hodnota1“*, a tyto dvojice jsou dále propojeny znakem *„&“* s následující dvojicí v pořadí, tedy ve formátu *„parametr1=hodnota1&parametr2=hodnota2“*. Celý řetězec je dále zakódován procentním kódováním (URL kódováním), které převádí speciální znaky na alfanumerické, před které vkládá jako

vodící znak procento.[159] Po rozkódování řetězce dekodérem[160] a selekcí nejdůležitějších informací jsem dostal tyto výsledky:

- Parametr: ***„Gender“***, hodnota: ***„M“*** – hodnota z vyplněného formuláře, která udává, že pohlaví je *„M“* jako muž.
- Parametr: ***„FirstName“***, hodnota: ***„Max“*** – hodnota z vyplněného formuláře, která udává, že křestní jméno je *„Max“*.
- Parametr: ***„LastName“***, hodnota: ***„Lagron“*** – hodnota z vyplněného formuláře, která udává, že příjmení je *„Lagron“*.
- Parametr: ***„Company“***, hodnota: ***„Firma 1“*** – hodnota z vyplněného formuláře, která udává, že název firmy je *„Firma 1“*.
- Parametr: ***„StreetAddress“***, hodnota: ***„Ulice 123“*** – hodnota z vyplněného formuláře, která udává, že adresa je *„Ulice 123“*.
- Parametr: ***„City“***, hodnota: ***„Praha“*** – hodnota z vyplněného formuláře, která udává, že město je *„Praha“*.
- Parametr: ***„ZipPostalCode“***, hodnota: ***„19000“*** – hodnota z vyplněného formuláře, která udává, že PSČ je *„19000“*.
- Parametr: ***„Phone“***, hodnota: ***„+420123456789“*** – hodnota z vyplněného formuláře, která udává, že telefonní číslo je *„+420123456789“*.
- Parametr: ***„Phone_mask“***, hodnota: ***„+420 123 456 789“*** – hodnota z vyplněného formuláře, která udává, že telefonní číslo s oddělovači je *„+420 123 456 789“*.
- Parametr: ***„Email“***, hodnota: ***„Email111@test.cz“*** – hodnota z vyplněného formuláře, která udává, že email je *„Email111@test.cz“*.

[159] POST. Mozilla [online]. 13.8.2022. [cit. 1.3.2022]. https://developer.mozilla.org/en-US/docs/Web/HTTP/Methods/POST
[160] Například na adrese: „https://www.url-encode-decode.com/“

- Parametr: ***„Password“***, hodnota: ***„abc123“*** – hodnota z vyplněného formuláře, která udává, že heslo je *„abc123“*.
- Parametr: ***„ConfirmPassword“***, hodnota: ***„abc123“*** – Hodnota z vyplněného formuláře, která udává, že potvrzení hesla je *„abc123“*.

Obrázek 19 - Vyplněný formulář

Jak je vidět na obrázku 19 níže, který je zachycením obrazovky vyplněného formuláře ze sledovaném smartphonu, zadané údaje se shodují s daty z ukořistěných paketů, včetně hesla, které je bohužel na formuláři zamaskované hvězdičkami.

Tato data, ukořistěná z vyplněného formuláře, mohou být zneužita ke krádeži identity, spáchání podvodu, nebo k dalším útokům, například na emailovou schránku oběti, ke které nyní útočník zná adresu.

Informace o OS a použitém softwaru, které HTTP protokol poskytuje, mohou být rovněž zneužity k dalším útokům, kdy útočník může využít různých vulnerabilit v napadeném zařízení, aby k němu získal přístup.

IP adresy a MAC adresy mohou být zase zneužity k útokům v síti, typicky k rušení komunikace mezi napadeným zařízením a AP.

Závěr

Smyslem této bakalářské práce bylo vysvětlit čtenáři, co jsou digitální stopy, jaká data po sobě zanecháváme v kyberprostoru svojí činností, jak probíhá přenos dat v internetu, a jak ho lze poměrně jednoduše sledovat, pokud jsou použity zastaralé nezabezpečené technologie jako HTTP protokol. Tohoto cíle bylo dosaženo, především v praktické části práce, ve které byly aplikovány poznatky z teoretické části do praxe, a na popisovaném příkladu bylo předvedeno, jaká data lze získat odposlouchávání bezdrátové sítě. Data obsahující citlivé údaje byla úspěšně zachycena z odposlouchávané sítě, a po provedené analýze byla potvrzena jejich autenticita. Mimo to byl v praktické části práce rovněž vysvětlen postup pro odposlouchávání bezdrátové sítě.

Přínos této práce spatřuji především ve vysvětlení rizik, která se pojí s digitálními stopami, což souvisí s šířením povědomí o bezpečném používání internetu, o kterém jsem psal v úvodu.

Jak jsem již v práci uvedl, kybernetická kriminalita je na vzestupném trendu, tudíž je třeba používat sofistikovanějších, bezpečnějších technologií, abychom zabránili zneužití našich dat. Dobrou zprávou je, že HTTP protokol, kterým jsem se zabýval v této práci, v dnešní době využívá minimum webových serverů a nenajdeme ho prakticky na žádném významnějším webu, jelikož je nahrazován bezpečným HTTPS protokolem.

Ani to však není stoprocentní záruka bezpečnosti, a už vůbec ne toho, že se v budoucnosti s příchodem nových technologií nestane současné zabezpečení přenosu dat obsoletní. Kyberprostor nejspíše nikdy nebude bezpečným místem, proto je třeba znát jeho rizika a umět si chránit svoje data.

Seznam použité literatury

Monografie

[1] HORÁK, Jaroslav. *Bezpečnost malých počítačových sítí*. 1. vyd. [Praha]: Grada, 2003. ISBN 80-247-0663-6.

[2] KOLOUCH, Jan. *Cybercrime*. 1. vyd. Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8.

[3] ČÍŽEK, František a kol. *Filosofie, metodologie, věda*. 1. vyd. Praha: Svoboda, 1969.

[4] KOVÁŘOVÁ, Pavla. *Informační bezpečnost žáků základních škol*. 1. vyd. [Brno]: Masarykova univerzita, 2019. ISBN 978-80-210-9270-9.

[5] JIROVSKÝ, Václav. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, ISBN 978-80-247-1561-2.

[6] STRAUS, Jiří a kol. *Úvod do kriminalistiky*. 3. vyd. Plzeň: Aleš Čeněk, 2012. ISBN 978-80-7380-367-4.

Zákonná úprava a IAŘ (interní akty řízení)

[7] Nařízení evropského parlamentu a rady EU 2016/679, *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)*.

[8] Zákon č. 181/2014 Sb., *zákon o kybernetické bezpečnosti* v posledním znění.

[9] Zákon č. 141/1961 Sb., *zákon o trestním řízení soudním (trestní řád)* posledním znění.

[10] Zákon č. 40/2009 Sb., *zákon trestní zákoník* v posledním znění.

[11] Zákon č. 110/2019 Sb., *zákon o zpracování osobních údajů* v posledním znění.

Webové stránky a elektronické zdroje

[12] DANEL, Roman. *Analýza projektování systémů* [online]. Ostrava, 2014. E-learningová podpora. Vysoká škola báňská – Technická univerzita Ostrava, Hornicko-geologická fakulta [cit. 16.1.2022]. Dostupné z: https://homel.vsb.cz/~dan11/aps/texty/INOHGF_EL_APS_DANEL.pdf

[13] RAK, Roman a Viktor PORADA. *Digitální stopy v kriminalistice a forenzních vědách*. Soudní inženýrství [online]. 2006, roč. 17. [cit. 2.8.2021]. Dostupné z: http://www.sinz.cz/archiv/docs/si-2005-01-3-23.pdf

[14] Internet [online]. [cit. 30.1.2022]. Dostupné z: https://www.ssph.cz/vyuka/wp-content/uploads/2020/03/psi-internet.pdf

[15] BOHÁČ, Leoš. *IP protokol* [online]. 2016. [cit. 7.2.2022]. Dostupné z: https://docplayer.cz/1694986-Ip-protokol-leos-bohac.html

[16] DOLEŽALOVÁ, Stanislava. *Metodologie vědy, vědecké metody a metodika práce* [online]. [cit. 16.1.2022]. Dostupné z: https://docplayer.cz/7963823-2-metodologie-vedy-vedecke-metody-a-metodika-prace.html

[17] KOPECKÝ, Kamil a Veronika KREJČÍ. *Rizika virtuální komunikace* [online]. Olomouc: NET UNIVERSITY, 2010. [cit. 21.1.2022]. ISBN 978-80-254-7737-3. Dostupné z: http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=9%3Astudie-o-stalkingu-a-kyberstalkingu

[18] RAK, Roman a Viktor PORADA. *Vlastnosti digitálních stop a jejich dopady na forenzní šetření*. Soudní inženýrství [online]. 2005, roč. 16. [cit. 16.10.2021]. http://www.sinz.cz/archiv/docs/si-2005-04-183-192.pdf

[19] Avast uzavře svoji dceřinou společnost Jumpshot. *Avast* [online]. 30.1.2020. [cit. 27.11.2021]. Dostupné z: https://press.avast.com/cs-cz/avast-uzavre-svoji-dcerinou-spolecnost-jumpshot

[20] ROMAJZL, Lukáš. Jak hacknout wifi síť. *Dotyk* [online]. 16.1.2015. [cit. 23.1.2022]. Dostupné z: https://www.dotyk.cz/publicistika/jak-hacknout-wi-fi-sit.html

[21] Krádež identity. *Eset* [online]. [cit. 2.1.2022]. Dostupné z: https://www.eset.com/cz/kradez-identity/

[22] Vishing. *Eset* [online]. 25.8.2021. [cit. 2.1.2022]. Dostupné z: https://www.eset.com/cz/blog/hrozby/vishing-jak-ho-rozeznat-a-vyhnout-se-mu/

[23] Kyberkriminalita na vzestupu. *Eurozprávy* [online]. 10.2.2020. [cit. 12.12.2021]. Dostupné z: https://eurozpravy.cz/domaci/zivot/kyberkriminalita-na-vzestupu-obetmi-jsou-stale-casteji-deti-udelejte-si-test.d47c0d49/

[24] PASTUCHOVÁ, Markéta. Open source přebírá v oblasti softwaru klíčovou roli. *ICT manažer* [online]. 5.11.2011. [cit. 30.1.2022]. Dostupné z archivu: https://web.archive.org/web/20120111073224/http://www.ictmanazer.cz/2011/11/open-source-prebira-v-oblasti-softwaru-klicovou-roli/

[25] Digitální stopa. *Internetem bezpečně* [online]. [cit. 14.3.2021]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/dobre-vedet/digitalni-stopa/

[26] Krádež identity. *Internetem bezpečně* [online]. [cit. 2.1.2022]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybersikana/kradez-identity/

[27] Kyberšikana. *Internetem bezpečně* [online]. [cit. 8.1.2022]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybersikana/

[28] Sociální inženýrství. *Internetem bezpečně* [online]. [cit. 19.12.2021]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/podvodne-praktiky/socialni-inzenyrstvi/

[29] JOHNSTON, Matthew. How Facebook (Meta) Makes Money. *Investopedia* [online]. 4.2.2022. [cit. 8.2.2022]. Dostupné z: https://www.investopedia.com/ask/answers/120114/how-does-facebook-fb-make-money.asp

[30] Metadata. *IT slovník* [online]. [cit. 4.2.2021]. Dostupné z: https://it-slovnik.cz/pojem/metadata

[31] Cookies. *IT slovník* [online]. [cit. 4.2.2021]. Dostupné z: https://it-slovnik.cz/pojem/cookies

[32] Log. *IT slovník* [online]. [cit. 4.2.2021]. Dostupné z: https://it-slovnik.cz/pojem/log

[33] Kali. *Kali* [online]. [cit. 22.2.2022]. Dostupné z: https://www.kali.org/

[34] Smishing. *Kaspersky* [online]. [cit. 2.1.2022]. Dostupné z: https://www.kaspersky.com/resource-center/threats/what-is-smishing-and-how-to-defend-against-it

[35] What is a digital footprint? And how to protect it from hackers. *Kaspersky* [online]. [cit. 27.11.2021]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/what-is-a-digital-footprint

[36] Behaviorální marketing. *Mediaguru* [online]. [cit. 24.10.2021]. Dostupné z: https://www.mediaguru.cz/slovnik-a-mediatypy/slovnik/klicova-slova/behavioralni-marketing/

[37] POST. *Mozilla* [online]. 13.8.2022. [cit. 3.1.2022]. https://developer.mozilla.org/en-US/docs/Web/HTTP/Methods/POST

[38] User-Agent. *Mozilla* [online]. 18.2.2022. [cit. 3.1.2022]. https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/User-Agent

[39] Základní pojmy v GDPR. *Ministerstvo vnitra ČR* [online]. [cit. 5.12.2021]. Dostupné z: https://www.mvcr.cz/gdpr/clanek/zakladni-pojmy-v-gdpr.aspx

[40] The Open Source Definition. *Opensource* [online]. 22.3.2007. [cit. 22.1.2022]. Dostupné z: https://opensource.org/osd

[41] KAN, Michael. The Cost of Avast's Free Antivirus: Companies Can Spy on Your Clicks. *PCmag* [online]. 27.1.2020. [cit. 27.11.2021]. Dostupné z: https://www.pcmag.com/news/the-cost-of-avasts-free-antivirus-companies-can-spy-on-your-clicks

[42] SOUČKOVÁ, Tereza. Krádež identity. *Policie ČR* [online]. 25.5.2010. [cit. 2.1.2022]. Dostupné z: https://www.policie.cz/clanek/ztrata-identity.aspx

[43] Kyberkriminalita. *Policie ČR* [online]. [cit. 12.12.2021]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx

[44] PAPEŽOVÁ, Zdeňka. PREVENCE – Kyberšikana. *Policie ČR* [online]. [cit. 8.1.2022]. Dostupné z: https://www.policie.cz/clanek/prevence-kybersikana.aspx

[45] Archer T9UH. *tp-link* [online]. [cit. 22.2.2022]. https://www.tp-link.com/cz/home-networking/adapter/archer-t9uh/

[46] Správce, zpracovatel. *Úřad pro ochranu osobních údajů* [online]. 25.4.2019. [cit. 5.12.2021]. Dostupné z: https://www.uoou.cz/7-spravce-zpracovatel/d-27278

[47] Zabezpečení osobních údajů. *Úřad pro ochranu osobních údajů* [online]. 25.4.2019. [cit. 5.12.2021]. Dostupné z: https://www.uoou.cz/8-zabezpe-eni-osobnich-udaj/d-27282

[48] VirtualBox. *VirtualBox* [online]. [cit. 22.2.2022]. Dostupné z: https://www.virtualbox.org/

[49] What are RadioTap Headers? *WiFiNigel* [online]. [cit. 28.2.2022]. https://wifinigel.blogspot.com/2013/11/what-are-radiotap-headers.html

[50] 4-WAY HANDSHAKE. *WiFi-professionals* [online]. 24.1.2019. [cit. 3.1.2022]. https://www.wifi-professionals.com/2019/01/4-way-handshake

[51] Brave. *Wikipedia* [online]. 12. 7. 2021. [cit. 22.2.2022]. https://cs.wikipedia.org/wiki/Brave_(webový_prohlížeč)

[52] EMUI. *Wikipedia* [online]. 8.2.2022. [cit. 22.2.2022]. Dostupné z: https://en.wikipedia.org/wiki/EMUI

[53] Hypertext Transfer Protocol. *Wikipedia* [online]. 14.12.2021. [cit. 6.2.2022]. Dostupné z: https://cs.wikipedia.org/wiki/Hypertext_Transfer_Protocol

[54] IEEE 802.2. *Wikipedia* [online]. 15.1.2022. [cit. 28.2.2022]. Dostupné z: https://cs.wikipedia.org/wiki/IEEE_802.2

[55] IPv6. *Wikipedia* [online]. 15.1.2022. [cit. 5.2.2022]. Dostupné z: https://cs.wikipedia.org/wiki/IPv6

[56] Logical Link Control. *Wikipedia* [online]. 8. 8. 2021. [cit. 28.2.2022]. https://cs.wikipedia.org/wiki/Logical_Link_Control

[57] Otevřený software. *Wikipedia* [online]. 6.2.2022. [cit. 22.1.2022]. Dostupné z: https://cs.wikipedia.org/wiki/Otev%C5%99en%C3%BD_software

[58] Síťový port. *Wikipedia* [online]. 8.8.2021. [cit. 6.2.2022]. Dostupné z: https://cs.wikipedia.org/wiki/S%C3%AD%C5%A5ov%C3%BD_port

[59] Wireshark. *Wireshark* [online]. [cit. 22.2.2022]. Dostupné z: https://www.wireshark.org/

Seznam použitých zkratek a symbolů

- **AP** – anglicky *„Access point“*, v českém překladu *„vstupní bod“*.
- **CLI** – anglicky *„Command Line Interface“*, v českém překladu *„příkazová řádka“*.
- **DNS** – anglicky *„Domain Name System“*, v českém překladu *„systém doménových jmen“*.
- **EULA** – anglicky *„End user licence agreement“*, v českém překladu *„licenční smlouva s koncovým uživatelem“*.
- **GAN** - *„Global Area Network“*, v českém překladu *„Globální síť“*.
- **HTTP** – anglicky *„Hypertext transfer protocol“*, v českém překladu *„hypertextový přenosový protokol“*.
- **ICT** – anglicky *„Information and Communication Technologies“*, v českém překladu *„informační a komunikační technologie“*.
- **IP** – anglicky *„Internet protocol“*, v českém překladu *„Internetový protokol“*.
- **ISP** – anglicky *„Internet service provider“*, v českém překladu *„poskytovatel internetových služeb“*.
- **IT** – anglicky *„information technology“*, v českém překladu *„informační technologie“*.
- **LAN** – anglicky *„Local Area Network“*, v českém překladu *„místní počítačová síť“*.
- **MAC** – anglicky *„Media Access Control“*, v českém doslovném překladu *„řízení přístupu k médiím“*.
- **MAN** – anglicky *„Metropolitan Area Network“*, v českém překladu *„metropolitní počítačová síť“*.
- **OS** – Operační systém.
- **PCI** – anglicky *„Peripheral Component Interconnect“*.
- **PR** – anglicky *„public relations“*, v českém překladu *„vztahy s veřejností“*.
- **TCP** – anglicky *„Transmition control protocol“*, v českém překladu *„protokol řízení přenosu“*.

- **TŘ** – Zákon č. 141/1961 Sb., *zákon o trestním řízení soudním (trestní řád)* v posledním znění.
- **TZK** – Zákon č. 40/2009 Sb., *zákon trestní zákoník* v posledním znění.
- **UDP** – anglicky *„User datagram protocol“*, v českém překladu *„uživatelský protokol pro přenost datagramů“*.
- **URL** – anglicky *„Uniform Resource Locator“*, v českém překladu *„jednotný lokátor zdroje“*.
- **VoIP** – anglicky *„voice over internet protocol“*, v českém překladu *„protokol přenosu hlasu internetem“*.
- **WAN** – anglicky *„Wide Area Network“*, v českém překladu *„rozlehlá počítačová síť“*.
- **WLAN** – anglicky *„Wireless Local Area Network“*, v českém překladu *„bezdrátová místní počítačová síť“*.
- **WWW** – anglicky *„World Wide Web“*, v českém překladu *„celosvětová síť“*.

Seznam obrázků, tabulek a grafů

Seznam příloh

Příloha 1 – Data ze zachycených paketů ve formátu JSON.


```
[
{
"_index": "packets-2022-02-27",
"_type": "doc",
"_score": null,
"_source": {
"layers": {
"frame": {
"frame.interface_id": "0",
"frame.interface_id_tree": {
"frame.interface_name": "wlan0"
},
"frame.encap_type": "23",
"frame.time": "Feb 27, 2022 16:59:48.316913715 EST",
"frame.offset_shift": "0.000000000",
"frame.time_epoch": "1645999188.316913715",
"frame.time_delta": "0.007229285",
"frame.time_delta_displayed": "19.921404680",
"frame.time_relative": "35.353283117",
"frame.number": "4029",
"frame.len": "1218",
"frame.cap_len": "1218",
"frame.marked": "0",
"frame.ignored": "0",
"frame.protocols": "radiotap:wlan_radio:wlan:llc:ip:tcp:http",
"frame.coloring_rule.name": "HTTP",
"frame.coloring_rule.string": "http || tcp.port == 80 || http2"
},
"radiotap": {
"radiotap.version": "0",
"radiotap.pad": "0",
"radiotap.length": "21",
"radiotap.present": {
"radiotap.present.word": "0x0008482a",
"radiotap.present.word_tree": {
"radiotap.present.tsft": "0",
"radiotap.present.flags": "1",
"radiotap.present.rate": "0",
"radiotap.present.channel": "1",
"radiotap.present.fhss": "0",
"radiotap.present.dbm_antsignal": "1",
"radiotap.present.dbm_antnoise": "0",
"radiotap.present.lock_quality": "0",
```

```
44.         "radiotap.present.tx_attenuation": "0",
45.         "radiotap.present.db_tx_attenuation": "0",
46.         "radiotap.present.dbm_tx_power": "0",
47.         "radiotap.present.antenna": "1",
48.         "radiotap.present.db_antsignal": "0",
49.         "radiotap.present.db_antnoise": "0",
50.         "radiotap.present.fcs": "1",
51.         "radiotap.present.txflags": "0",
52.         "radiotap.present.data_retries": "0",
53.         "radiotap.present.xchannel": "0",
54.         "radiotap.present.mcs": "1",
55.         "radiotap.present.ampdu": "0",
56.         "radiotap.present.vht": "0",
57.         "radiotap.present.timestamp": "0",
58.         "radiotap.present.he": "0",
59.         "radiotap.present.he_mu": "0",
60.         "radiotap.present.0_length.psdu": "0",
61.         "radiotap.present.l_sig": "0",
62.         "radiotap.present.tlv": "0",
63.         "radiotap.present.rtap_ns": "0",
64.         "radiotap.present.vendor_ns": "0",
65.         "radiotap.present.ext": "0"
66.         },
67.         "_ws.expert": {
68.         "radiotap.data_past_header": "",
69.         "_ws.expert.message": "Radiotap data goes past the end of the
            radiotap header",
70.         "_ws.expert.severity": "8388608",
71.         "_ws.expert.group": "117440512"
72.         },
73.         "_ws.malformed": "Malformed Packet"
74.         },
75.         "radiotap.flags": "0x10",
76.         "radiotap.flags_tree": {
77.         "radiotap.flags.cfp": "0",
78.         "radiotap.flags.preamble": "0",
79.         "radiotap.flags.wep": "0",
80.         "radiotap.flags.frag": "0",
81.         "radiotap.flags.fcs": "1",
82.         "radiotap.flags.datapad": "0",
83.         "radiotap.flags.badfcs": "0",
84.         "radiotap.flags.shortgi": "0"
85.         },
86.         "radiotap.channel.freq": "2412",
87.         "radiotap.channel.flags": "0x0480",
88.         "radiotap.channel.flags_tree": {
89.         "radiotap.channel.flags.700mhz": "0",
90.         "radiotap.channel.flags.800mhz": "0",
91.         "radiotap.channel.flags.900mhz": "0",
```

```
92.       "radiotap.channel.flags.turbo": "0",
93.       "radiotap.channel.flags.cck": "0",
94.       "radiotap.channel.flags.ofdm": "0",
95.       "radiotap.channel.flags.2ghz": "1",
96.       "radiotap.channel.flags.5ghz": "0",
97.       "radiotap.channel.flags.passive": "0",
98.       "radiotap.channel.flags.dynamic": "1",
99.       "radiotap.channel.flags.gfsk": "0",
100.      "radiotap.channel.flags.gsm": "0",
101.      "radiotap.channel.flags.sturbo": "0",
102.      "radiotap.channel.flags.half": "0",
103.      "radiotap.channel.flags.quarter": "0"
104.      },
105.      "radiotap.dbm_antsignal": "-38",
106.      "radiotap.antenna": "0",
107.      "radiotap.fcs": "0x00002700",
108.      "radiotap.fcs_bad": "1"
109.      },
110.      "wlan_radio": {
111.      "wlan_radio.phy": "6",
112.      "wlan_radio.11g.mode": "0",
113.      "wlan_radio.channel": "1",
114.      "wlan_radio.frequency": "2412",
115.      "wlan_radio.signal_dbm": "-38"
116.      },
117.      "wlan": {
118.      "wlan.fc.type_subtype": "0x0028",
119.      "wlan.fc": "0x8841",
120.      "wlan.fc_tree": {
121.      "wlan.fc.version": "0",
122.      "wlan.fc.type": "2",
123.      "wlan.fc.subtype": "8",
124.      "wlan.flags": "0x41",
125.      "wlan.flags_tree": {
126.      "wlan.fc.ds": "0x01",
127.      "wlan.fc.tods": "1",
128.      "wlan.fc.fromds": "0",
129.      "wlan.fc.frag": "0",
130.      "wlan.fc.retry": "0",
131.      "wlan.fc.pwrmgt": "0",
132.      "wlan.fc.moredata": "0",
133.      "wlan.fc.protected": "1",
134.      "wlan.fc.order": "0"
135.      }
136.      },
137.      "wlan.duration": "148",
138.      "wlan.ra": "c0:fd:84:a4:88:8b",
139.      "wlan.ra_resolved": "zte_a4:88:8b",
140.      "wlan.addr": "c0:fd:84:a4:88:8b",
```

```
141.  "wlan.addr_resolved": "zte_a4:88:8b",
142.  "wlan.ta": "0c:b5:27:55:7b:79",
143.  "wlan.ta_resolved": "HuaweiTe_55:7b:79",
144.  "wlan.addr": "0c:b5:27:55:7b:79",
145.  "wlan.addr_resolved": "HuaweiTe_55:7b:79",
146.  "wlan.da": "c0:fd:84:a4:88:8b",
147.  "wlan.da_resolved": "zte_a4:88:8b",
148.  "wlan.sa": "0c:b5:27:55:7b:79",
149.  "wlan.sa_resolved": "HuaweiTe_55:7b:79",
150.  "wlan.bssid": "c0:fd:84:a4:88:8b",
151.  "wlan.bssid_resolved": "zte_a4:88:8b",
152.  "wlan.staa": "0c:b5:27:55:7b:79",
153.  "wlan.staa_resolved": "HuaweiTe_55:7b:79",
154.  "wlan.frag": "0",
155.  "wlan.seq": "221",
156.  "wlan.addr": "c0:fd:84:a4:88:8b",
157.  "wlan.addr_resolved": "zte_a4:88:8b",
158.  "wlan.fcs": "0x2aac6500",
159.  "wlan.fcs.status": "1",
160.  "wlan.qos": "0x0000",
161.  "wlan.qos_tree": {
162.  "wlan.qos.tid": "0",
163.  "wlan.qos.priority": "0",
164.  "wlan.qos.bit4": "0",
165.  "wlan.qos.ack": "0x0000",
166.  "wlan.qos.amsdupresent": "0",
167.  "wlan.qos.txop_dur_req": "0"
168.  },
169.  "CCMP parameters": {
170.  "wlan.ccmp.extiv": "0x0000000000E0",
171.  "wlan.wep.key": "0",
172.  "wlan.analysis.tk": "a5b6467bdac9c09c4f938e5d824bc3e7",
173.  "wlan.analysis.pmk":
      "428b50abf84f6a78fc90af72f5121be8bc37e5159ea607a55cd97b2c6
      b67ece8"
174.  }
175.  },
176.  "llc": {
177.  "llc.dsap": "0xaa",
178.  "llc.dsap_tree": {
179.  "llc.dsap.sap": "85",
180.  "llc.dsap.ig": "0"
181.  },
182.  "llc.ssap": "0xaa",
183.  "llc.ssap_tree": {
184.  "llc.ssap.sap": "85",
185.  "llc.ssap.cr": "0"
186.  },
187.  "llc.control": "0x0003",
```

```
188.      "llc.control_tree": {
189.      "llc.control.u_modifier_cmd": "0x00",
190.      "llc.control.ftype": "0x03"
191.      },
192.      "llc.oui": "0",
193.      "llc.type": "0x0800"
194.      },
195.      "ip": {
196.      "ip.version": "4",
197.      "ip.hdr_len": "20",
198.      "ip.dsfield": "0x00",
199.      "ip.dsfield_tree": {
200.      "ip.dsfield.dscp": "0",
201.      "ip.dsfield.ecn": "0"
202.      },
203.      "ip.len": "1143",
204.      "ip.id": "0x3b7f",
205.      "ip.flags": "0x40",
206.      "ip.flags_tree": {
207.      "ip.flags.rb": "0",
208.      "ip.flags.df": "1",
209.      "ip.flags.mf": "0"
210.      },
211.      "ip.frag_offset": "0",
212.      "ip.ttl": "64",
213.      "ip.proto": "6",
214.      "ip.checksum": "0xe206",
215.      "ip.checksum.status": "2",
216.      "ip.src": "10.0.0.16",
217.      "ip.addr": "10.0.0.16",
218.      "ip.src_host": "10.0.0.16",
219.      "ip.host": "10.0.0.16",
220.      "ip.dst": "109.233.161.2",
221.      "ip.addr": "109.233.161.2",
222.      "ip.dst_host": "109.233.161.2",
223.      "ip.host": "109.233.161.2"
224.      },
225.      "tcp": {
226.      "tcp.srcport": "58314",
227.      "tcp.dstport": "80",
228.      "tcp.port": "58314",
229.      "tcp.port": "80",
230.      "tcp.stream": "16",
231.      "tcp.completeness": "14",
232.      "tcp.len": "1091",
233.      "tcp.seq": "4796",
234.      "tcp.seq_raw": "1299091444",
235.      "tcp.nxtseq": "5887",
236.      "tcp.ack": "18870",
```

```
237.  "tcp.ack_raw": "2446880971",
238.  "tcp.hdr_len": "32",
239.  "tcp.flags": "0x0018",
240.  "tcp.flags_tree": {
241.  "tcp.flags.res": "0",
242.  "tcp.flags.ns": "0",
243.  "tcp.flags.cwr": "0",
244.  "tcp.flags.ecn": "0",
245.  "tcp.flags.urg": "0",
246.  "tcp.flags.ack": "1",
247.  "tcp.flags.push": "1",
248.  "tcp.flags.reset": "0",
249.  "tcp.flags.syn": "0",
250.  "tcp.flags.fin": "0",
251.  "tcp.flags.str": "·····AP···"
252.  },
253.  "tcp.window_size_value": "523",
254.  "tcp.window_size": "523",
255.  "tcp.window_size_scalefactor": "-1",
256.  "tcp.checksum": "0x74cb",
257.  "tcp.checksum.status": "2",
258.  "tcp.urgent_pointer": "0",
259.  "tcp.options": "01:01:08:0a:00:91:10:43:07:b4:09:8d",
260.  "tcp.options_tree": {
261.  "tcp.options.nop": "01",
262.  "tcp.options.nop_tree": {
263.  "tcp.option_kind": "1"
264.  },
265.  "tcp.options.nop": "01",
266.  "tcp.options.nop_tree": {
267.  "tcp.option_kind": "1"
268.  },
269.  "tcp.options.timestamp": "08:0a:00:91:10:43:07:b4:09:8d",
270.  "tcp.options.timestamp_tree": {
271.  "tcp.option_kind": "8",
272.  "tcp.option_len": "10",
273.  "tcp.options.timestamp.tsval": "9506883",
274.  "tcp.options.timestamp.tsecr": "129239437"
275.  }
276.  },
277.  "Timestamps": {
278.  "tcp.time_relative": "40.977760948",
279.  "tcp.time_delta": "19.917538056"
280.  },
281.  "tcp.analysis": {
282.  "tcp.analysis.bytes_in_flight": "1091",
283.  "tcp.analysis.push_bytes_sent": "1091"
284.  },
```

285. "tcp.payload":
"50:4f:53:54:20:2f:72:65:67:69:73:74:65:72:20:48:54:54:50:2f:31:2e:
31:0d:0a:48:6f:73:74:3a:20:77:77:77:2e:6b:6e:69:68:79:2d:7a:61:2d:
62:61:62:6b:75:2e:63:7a:0d:0a:43:6f:6e:6e:65:63:74:69:6f:6e:3a:20:6
b:65:65:70:2d:61:6c:69:76:65:0d:0a:43:6f:6e:74:65:6e:74:2d:4c:65:6
e:67:74:68:3a:20:39:31:33:0d:0a:43:61:63:68:65:2d:43:6f:6e:74:72:6f
:6c:3a:20:6d:61:78:2d:61:67:65:3d:30:0d:0a:55:70:67:72:61:64:65:2d
:49:6e:73:65:63:75:72:65:2d:52:65:71:75:65:73:74:73:3a:20:31:0d:0a
:4f:72:69:67:69:6e:3a:20:68:74:74:70:3a:2f:2f:77:77:77:2e:6b:6e:69:6
8:79:2d:7a:61:2d:62:61:62:6b:75:2e:63:7a:0d:0a:43:6f:6e:74:65:6e:7
4:2d:54:79:70:65:3a:20:61:70:70:6c:69:63:61:74:69:6f:6e:2f:78:2d:77
:77:77:2d:66:6f:72:6d:2d:75:72:6c:65:6e:63:6f:64:65:64:0d:0a:55:73:
65:72:2d:41:67:65:6e:74:3a:20:4d:6f:7a:69:6c:6c:61:2f:35:2e:30:20:2
8:4c:69:6e:75:78:3b:20:41:6e:64:72:6f:69:64:20:31:30:29:20:41:70:7
0:6c:65:57:65:62:4b:69:74:2f:35:33:37:2e:33:36:20:28:4b:48:54:4d:4
c:2c:20:6c:69:6b:65:20:47:65:63:6b:6f:29:20:43:68:72:6f:6d:65:2f:39:
38:2e:30:2e:34:37:35:38:2e:31:30:32:20:4d:6f:62:69:6c:65:20:53:61:
66:61:72:69:2f:35:33:37:2e:33:36:0d:0a:41:63:63:65:70:74:3a:20:74:
65:78:74:2f:68:74:6d:6c:2c:61:70:70:6c:69:63:61:74:69:6f:6e:2f:78:6
8:74:6d:6c:2b:78:6d:6c:2c:61:70:70:6c:69:63:61:74:69:6f:6e:2f:78:6d
:6c:3b:71:3d:30:2e:39:2c:69:6d:61:67:65:2f:61:76:69:66:2c:69:6d:61:
67:65:2f:77:65:62:70:2c:69:6d:61:67:65:2f:61:70:6e:67:2c:2a:2f:2a:3
b:71:3d:30:2e:38:2c:61:70:70:6c:69:63:61:74:69:6f:6e:2f:73:69:67:6e
:65:64:2d:65:78:63:68:61:6e:67:65:3b:76:3d:62:33:3b:71:3d:30:2e:39
:0d:0a:53:65:63:2d:47:50:43:3a:20:31:0d:0a:52:65:66:65:72:65:72:3a
:20:68:74:74:70:3a:2f:2f:77:77:77:2e:6b:6e:69:68:79:2d:7a:61:2d:62:
61:62:6b:75:2e:63:7a:2f:72:65:67:69:73:74:65:72:0d:0a:41:63:63:65:
70:74:2d:45:6e:63:6f:64:69:6e:67:3a:20:67:7a:69:70:2c:20:64:65:66:
6c:61:74:65:0d:0a:41:63:63:65:70:74:2d:4c:61:6e:67:75:61:67:65:3a:
20:63:73:2d:43:5a:2c:63:73:3b:71:3d:30:2e:39:2c:65:6e:2d:43:5a:3b:
71:3d:30:2e:38:2c:65:6e:3b:71:3d:30:2e:37:0d:0a:43:6f:6f:6b:69:65:3
a:20:5f:5f:75:74:6d:61:3d:32:35:37:39:34:32:32:32:35:2e:31:34:31:34
:35:39:35:39:35:33:2e:31:36:34:35:39:39:37:32:34:38:2e:31:36:34:35
:39:39:37:32:34:38:2e:31:36:34:35:39:39:37:32:34:38:2e:31:3b:20:5f:
5f:75:74:6d:7a:3d:32:35:37:39:34:32:32:32:35:2e:31:36:34:35:39:39:
37:32:34:38:2e:31:2e:31:2e:75:74:6d:63:73:72:3d:28:64:69:72:65:63:
74:29:7c:75:74:6d:63:63:6e:3d:28:64:69:72:65:63:74:29:7c:75:74:6d:
63:6d:64:3d:28:6e:6f:6e:65:29:3b:20:5f:5f:75:74:6d:63:3d:32:35:37:3
9:34:32:32:32:35:3b:20:41:53:50:2e:4e:45:54:5f:53:65:73:73:69:6f:6e
:49:64:3d:62:35:79:33:72:69:70:62:71:6b:6f:77:77:6e:65:72:74:76:68:
6e:77:61:64:6f:3b:20:5f:5f:52:65:71:75:65:73:74:56:65:72:69:66:69:6
3:61:74:69:6f:6e:54:6f:6b:65:6e:3d:76:33:7a:47:46:48:33:55:69:75:6e
:64:77:4f:55:79:4d:52:6b:54:77:72:4c:57:4c:5f:2d:7a:34:6f:46:79:6a:6
f:4e:7a:43:4f:77:74:33:50:62:63:79:46:62:5f:48:5f:49:71:64:32:6d:73:
6e:62:51:58:70:73:33:39:76:79:77:51:76:66:76:47:4d:4e:55:77:66:33:
75:69:47:55:58:52:79:44:61:72:5f:38:30:31:3b:20:5f:5f:75:74:6d:74:3
d:31:3b:20:4e:6f:70:2e:63:75:73:74:6f:6d:65:72:3d:30:61:33:61:35:36
:37:66:2d:31:66:32:65:2d:34:35:34:36:2d:61:35:33:37:2d:64:30:64:63
:36:66:64:62:39:64:64:34:3b:20:5f:5f:75:74:6d:62:3d:32:35:37:39:34:

```
32:32:32:35:2e:31:38:2e:31:30:2e:31:36:34:35:39:39:37:32:34:38:0d:
0a:0d:0a"
},
"http": {
"POST /register HTTP/1.1\\r\\n": {
"_ws.expert": {
"http.chat": "",
"_ws.expert.message": "POST /register HTTP/1.1\\r\\n",
"_ws.expert.severity": "2097152",
"_ws.expert.group": "33554432"
},
"http.request.method": "POST",
"http.request.uri": "/register",
"http.request.version": "HTTP/1.1"
},
"http.host": "www.knihy-za-babku.cz",
"http.request.line": "Host: www.knihy-za-babku.cz\r\n",
"http.connection": "keep-alive",
"http.request.line": "Connection: keep-alive\r\n",
"http.content_length_header": "913",
"http.content_length_header_tree": {
"http.content_length": "913"
},
"http.request.line": "Content-Length: 913\r\n",
"http.cache_control": "max-age=0",
"http.request.line": "Cache-Control: max-age=0\r\n",
"http.request.line": "Upgrade-Insecure-Requests: 1\r\n",
"http.request.line": "Origin: http://www.knihy-za-babku.cz\r\n",
"http.content_type": "application/x-www-form-urlencoded",
"http.request.line": "Content-Type: application/x-www-form-
urlencoded\r\n",
"http.user_agent": "Mozilla/5.0 (Linux; Android 10)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102
Mobile Safari/537.36",
"http.request.line": "User-Agent: Mozilla/5.0 (Linux; Android 10)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102
Mobile Safari/537.36\r\n",
"http.accept":
"text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,ima
ge/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9",
"http.request.line": "Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,ima
ge/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9\r\n",
"http.request.line": "Sec-GPC: 1\r\n",
"http.referer": "http://www.knihy-za-babku.cz/register",
"http.request.line": "Referer: http://www.knihy-za-
babku.cz/register\r\n",
```

```
321.    "http.accept_encoding": "gzip, deflate",
322.    "http.request.line": "Accept-Encoding: gzip, deflate\r\n",
323.    "http.accept_language": "cs-CZ,cs;q=0.9,en-CZ;q=0.8,en;q=0.7",
324.    "http.request.line": "Accept-Language: cs-CZ,cs;q=0.9,en-
        CZ;q=0.8,en;q=0.7\r\n",
325.    "http.cookie":
        "__utma=257942225.1414595953.1645997248.1645997248.164599
        7248.1;
        __utmz=257942225.1645997248.1.1.utmcsr=(direct)|utmccn=(direct)
        |utmcmd=(none); __utmc=257942225;
        ASP.NET_SessionId=b5y3ripbqkowwnertvhnwado;
        __RequestVerificationToken=v3zGFH3UiundwOUyMRkTwrLWL_-
        z4oFyjoNzCOwt3PbcyFb_H_Iqd2msnbQXps39vywQvfvGMNUwf3ui
        GUXRyDar_801; __utmt=1; Nop.customer=0a3a567f-1f2e-4546-
        a537-d0dc6fdb9dd4; __utmb=257942225.18.10.1645997248",
326.    "http.cookie_tree": {
327.    "http.cookie_pair":
        "__utma=257942225.1414595953.1645997248.1645997248.164599
        7248.1",
328.    "http.cookie_pair":
        "__utmz=257942225.1645997248.1.1.utmcsr=(direct)|utmccn=(direct
        )|utmcmd=(none)",
329.    "http.cookie_pair": "__utmc=257942225",
330.    "http.cookie_pair":
        "ASP.NET_SessionId=b5y3ripbqkowwnertvhnwado",
331.    "http.cookie_pair":
        "__RequestVerificationToken=v3zGFH3UiundwOUyMRkTwrLWL_-
        z4oFyjoNzCOwt3PbcyFb_H_Iqd2msnbQXps39vywQvfvGMNUwf3ui
        GUXRyDar_801",
332.    "http.cookie_pair": "__utmt=1",
333.    "http.cookie_pair": "Nop.customer=0a3a567f-1f2e-4546-a537-
        d0dc6fdb9dd4",
334.    "http.cookie_pair": "__utmb=257942225.18.10.1645997248"
335.    },
336.    "http.request.line": "Cookie:
        __utma=257942225.1414595953.1645997248.1645997248.164599
        7248.1;
        __utmz=257942225.1645997248.1.1.utmcsr=(direct)|utmccn=(direct)
        |utmcmd=(none); __utmc=257942225;
        ASP.NET_SessionId=b5y3ripbqkowwnertvhnwado;
        __RequestVerificationToken=v3zGFH3UiundwOUyMRkTwrLWL_-
        z4oFyjoNzCOwt3PbcyFb_H_Iqd2msnbQXps39vywQvfvGMNUwf3ui
        GUXRyDar_801; __utmt=1; Nop.customer=0a3a567f-1f2e-4546-
        a537-d0dc6fdb9dd4; __utmb=257942225.18.10.1645997248\r\n",
337.    "\\r\\n": "",
338.    "http.request.full_uri": "http://www.knihy-za-babku.cz/register",
339.    "http.request": "1",
340.    "http.request_number": "6",
341.    "http.prev_request_in": "2955",
```

```
"http.response_in": "4063",
"http.next_request_in": "4067"
}
}
}
},
{
"_index": "packets-2022-02-27",
"_type": "doc",
"_score": null,
"_source": {
"layers": {
"frame": {
"frame.interface_id": "0",
"frame.interface_id_tree": {
"frame.interface_name": "wlan0"
},
"frame.encap_type": "23",
"frame.time": "Feb 27, 2022 16:59:48.316914974 EST",
"frame.offset_shift": "0.000000000",
"frame.time_epoch": "1645999188.316914974",
"frame.time_delta": "0.000001259",
"frame.time_delta_displayed": "0.000001259",
"frame.time_relative": "35.353284376",
"frame.number": "4030",
"frame.len": "1040",
"frame.cap_len": "1040",
"frame.marked": "0",
"frame.ignored": "0",
"frame.protocols": "radiotap:wlan_radio:wlan:llc:ip:tcp:http:data",
"frame.coloring_rule.name": "HTTP",
"frame.coloring_rule.string": "http || tcp.port == 80 || http2"
},
"radiotap": {
"radiotap.version": "0",
"radiotap.pad": "0",
"radiotap.length": "21",
"radiotap.present": {
"radiotap.present.word": "0x0008482a",
"radiotap.present.word_tree": {
"radiotap.present.tsft": "0",
"radiotap.present.flags": "1",
"radiotap.present.rate": "0",
"radiotap.present.channel": "1",
"radiotap.present.fhss": "0",
"radiotap.present.dbm_antsignal": "1",
"radiotap.present.dbm_antnoise": "0",
"radiotap.present.lock_quality": "0",
"radiotap.present.tx_attenuation": "0",
```

```
391.      "radiotap.present.db_tx_attenuation": "0",
392.      "radiotap.present.dbm_tx_power": "0",
393.      "radiotap.present.antenna": "1",
394.      "radiotap.present.db_antsignal": "0",
395.      "radiotap.present.db_antnoise": "0",
396.      "radiotap.present.fcs": "1",
397.      "radiotap.present.txflags": "0",
398.      "radiotap.present.data_retries": "0",
399.      "radiotap.present.xchannel": "0",
400.      "radiotap.present.mcs": "1",
401.      "radiotap.present.ampdu": "0",
402.      "radiotap.present.vht": "0",
403.      "radiotap.present.timestamp": "0",
404.      "radiotap.present.he": "0",
405.      "radiotap.present.he_mu": "0",
406.      "radiotap.present.0_length.psdu": "0",
407.      "radiotap.present.l_sig": "0",
408.      "radiotap.present.tlv": "0",
409.      "radiotap.present.rtap_ns": "0",
410.      "radiotap.present.vendor_ns": "0",
411.      "radiotap.present.ext": "0"
412.      },
413.      "_ws.expert": {
414.      "radiotap.data_past_header": "",
415.      "_ws.expert.message": "Radiotap data goes past the end of the
          radiotap header",
416.      "_ws.expert.severity": "8388608",
417.      "_ws.expert.group": "117440512"
418.      },
419.      "_ws.malformed": "Malformed Packet"
420.      },
421.      "radiotap.flags": "0x10",
422.      "radiotap.flags_tree": {
423.      "radiotap.flags.cfp": "0",
424.      "radiotap.flags.preamble": "0",
425.      "radiotap.flags.wep": "0",
426.      "radiotap.flags.frag": "0",
427.      "radiotap.flags.fcs": "1",
428.      "radiotap.flags.datapad": "0",
429.      "radiotap.flags.badfcs": "0",
430.      "radiotap.flags.shortgi": "0"
431.      },
432.      "radiotap.channel.freq": "2412",
433.      "radiotap.channel.flags": "0x0480",
434.      "radiotap.channel.flags_tree": {
435.      "radiotap.channel.flags.700mhz": "0",
436.      "radiotap.channel.flags.800mhz": "0",
437.      "radiotap.channel.flags.900mhz": "0",
438.      "radiotap.channel.flags.turbo": "0",
```

```
439.      "radiotap.channel.flags.cck": "0",
440.      "radiotap.channel.flags.ofdm": "0",
441.      "radiotap.channel.flags.2ghz": "1",
442.      "radiotap.channel.flags.5ghz": "0",
443.      "radiotap.channel.flags.passive": "0",
444.      "radiotap.channel.flags.dynamic": "1",
445.      "radiotap.channel.flags.gfsk": "0",
446.      "radiotap.channel.flags.gsm": "0",
447.      "radiotap.channel.flags.sturbo": "0",
448.      "radiotap.channel.flags.half": "0",
449.      "radiotap.channel.flags.quarter": "0"
450.      },
451.      "radiotap.dbm_antsignal": "-39",
452.      "radiotap.antenna": "0",
453.      "radiotap.fcs": "0x00002700",
454.      "radiotap.fcs_bad": "1"
455.      },
456.      "wlan_radio": {
457.      "wlan_radio.phy": "6",
458.      "wlan_radio.11g.mode": "0",
459.      "wlan_radio.channel": "1",
460.      "wlan_radio.frequency": "2412",
461.      "wlan_radio.signal_dbm": "-39"
462.      },
463.      "wlan": {
464.      "wlan.fc.type_subtype": "0x0028",
465.      "wlan.fc": "0x8841",
466.      "wlan.fc_tree": {
467.      "wlan.fc.version": "0",
468.      "wlan.fc.type": "2",
469.      "wlan.fc.subtype": "8",
470.      "wlan.flags": "0x41",
471.      "wlan.flags_tree": {
472.      "wlan.fc.ds": "0x01",
473.      "wlan.fc.tods": "1",
474.      "wlan.fc.fromds": "0",
475.      "wlan.fc.frag": "0",
476.      "wlan.fc.retry": "0",
477.      "wlan.fc.pwrmgt": "0",
478.      "wlan.fc.moredata": "0",
479.      "wlan.fc.protected": "1",
480.      "wlan.fc.order": "0"
481.      }
482.      },
483.      "wlan.duration": "148",
484.      "wlan.ra": "c0:fd:84:a4:88:8b",
485.      "wlan.ra_resolved": "zte_a4:88:8b",
486.      "wlan.addr": "c0:fd:84:a4:88:8b",
487.      "wlan.addr_resolved": "zte_a4:88:8b",
```

```
488.  "wlan.ta": "0c:b5:27:55:7b:79",
489.  "wlan.ta_resolved": "HuaweiTe_55:7b:79",
490.  "wlan.addr": "0c:b5:27:55:7b:79",
491.  "wlan.addr_resolved": "HuaweiTe_55:7b:79",
492.  "wlan.da": "c0:fd:84:a4:88:8b",
493.  "wlan.da_resolved": "zte_a4:88:8b",
494.  "wlan.sa": "0c:b5:27:55:7b:79",
495.  "wlan.sa_resolved": "HuaweiTe_55:7b:79",
496.  "wlan.bssid": "c0:fd:84:a4:88:8b",
497.  "wlan.bssid_resolved": "zte_a4:88:8b",
498.  "wlan.staa": "0c:b5:27:55:7b:79",
499.  "wlan.staa_resolved": "HuaweiTe_55:7b:79",
500.  "wlan.frag": "0",
501.  "wlan.seq": "222",
502.  "wlan.addr": "c0:fd:84:a4:88:8b",
503.  "wlan.addr_resolved": "zte_a4:88:8b",
504.  "wlan.fcs": "0x774df808",
505.  "wlan.fcs.status": "1",
506.  "wlan.qos": "0x0000",
507.  "wlan.qos_tree": {
508.  "wlan.qos.tid": "0",
509.  "wlan.qos.priority": "0",
510.  "wlan.qos.bit4": "0",
511.  "wlan.qos.ack": "0x0000",
512.  "wlan.qos.amsdupresent": "0",
513.  "wlan.qos.txop_dur_req": "0"
514.  },
515.  "CCMP parameters": {
516.  "wlan.ccmp.extiv": "0x0000000000E1",
517.  "wlan.wep.key": "0",
518.  "wlan.analysis.tk": "a5b6467bdac9c09c4f938e5d824bc3e7",
519.  "wlan.analysis.pmk":
      "428b50abf84f6a78fc90af72f5121be8bc37e5159ea607a55cd97b2c6
      b67ece8"
520.  }
521.  },
522.  "llc": {
523.  "llc.dsap": "0xaa",
524.  "llc.dsap_tree": {
525.  "llc.dsap.sap": "85",
526.  "llc.dsap.ig": "0"
527.  },
528.  "llc.ssap": "0xaa",
529.  "llc.ssap_tree": {
530.  "llc.ssap.sap": "85",
531.  "llc.ssap.cr": "0"
532.  },
533.  "llc.control": "0x0003",
534.  "llc.control_tree": {
```

```
535.      "llc.control.u_modifier_cmd": "0x00",
536.      "llc.control.ftype": "0x03"
537.      },
538.      "llc.oui": "0",
539.      "llc.type": "0x0800"
540.      },
541.      "ip": {
542.      "ip.version": "4",
543.      "ip.hdr_len": "20",
544.      "ip.dsfield": "0x00",
545.      "ip.dsfield_tree": {
546.      "ip.dsfield.dscp": "0",
547.      "ip.dsfield.ecn": "0"
548.      },
549.      "ip.len": "965",
550.      "ip.id": "0x3b80",
551.      "ip.flags": "0x40",
552.      "ip.flags_tree": {
553.      "ip.flags.rb": "0",
554.      "ip.flags.df": "1",
555.      "ip.flags.mf": "0"
556.      },
557.      "ip.frag_offset": "0",
558.      "ip.ttl": "64",
559.      "ip.proto": "6",
560.      "ip.checksum": "0xe2b7",
561.      "ip.checksum.status": "2",
562.      "ip.src": "10.0.0.16",
563.      "ip.addr": "10.0.0.16",
564.      "ip.src_host": "10.0.0.16",
565.      "ip.host": "10.0.0.16",
566.      "ip.dst": "109.233.161.2",
567.      "ip.addr": "109.233.161.2",
568.      "ip.dst_host": "109.233.161.2",
569.      "ip.host": "109.233.161.2"
570.      },
571.      "tcp": {
572.      "tcp.srcport": "58314",
573.      "tcp.dstport": "80",
574.      "tcp.port": "58314",
575.      "tcp.port": "80",
576.      "tcp.stream": "16",
577.      "tcp.completeness": "14",
578.      "tcp.len": "913",
579.      "tcp.seq": "5887",
580.      "tcp.seq_raw": "1299092535",
581.      "tcp.nxtseq": "6800",
582.      "tcp.ack": "18870",
583.      "tcp.ack_raw": "2446880971",
```

```
584.  "tcp.hdr_len": "32",
585.  "tcp.flags": "0x0018",
586.  "tcp.flags_tree": {
587.  "tcp.flags.res": "0",
588.  "tcp.flags.ns": "0",
589.  "tcp.flags.cwr": "0",
590.  "tcp.flags.ecn": "0",
591.  "tcp.flags.urg": "0",
592.  "tcp.flags.ack": "1",
593.  "tcp.flags.push": "1",
594.  "tcp.flags.reset": "0",
595.  "tcp.flags.syn": "0",
596.  "tcp.flags.fin": "0",
597.  "tcp.flags.str": "·····AP···"
598.  },
599.  "tcp.window_size_value": "523",
600.  "tcp.window_size": "523",
601.  "tcp.window_size_scalefactor": "-1",
602.  "tcp.checksum": "0x8e3f",
603.  "tcp.checksum.status": "2",
604.  "tcp.urgent_pointer": "0",
605.  "tcp.options": "01:01:08:0a:00:91:10:43:07:b4:09:8d",
606.  "tcp.options_tree": {
607.  "tcp.options.nop": "01",
608.  "tcp.options.nop_tree": {
609.  "tcp.option_kind": "1"
610.  },
611.  "tcp.options.nop": "01",
612.  "tcp.options.nop_tree": {
613.  "tcp.option_kind": "1"
614.  },
615.  "tcp.options.timestamp": "08:0a:00:91:10:43:07:b4:09:8d",
616.  "tcp.options.timestamp_tree": {
617.  "tcp.option_kind": "8",
618.  "tcp.option_len": "10",
619.  "tcp.options.timestamp.tsval": "9506883",
620.  "tcp.options.timestamp.tsecr": "129239437"
621.  }
622.  },
623.  "Timestamps": {
624.  "tcp.time_relative": "40.977762207",
625.  "tcp.time_delta": "0.000001259"
626.  },
627.  "tcp.analysis": {
628.  "tcp.analysis.bytes_in_flight": "2004",
629.  "tcp.analysis.push_bytes_sent": "913"
630.  },
631.  "tcp.payload":
      "5f:5f:52:65:71:75:65:73:74:56:65:72:69:66:69:63:61:74:69:6f:6e:54:
```

6f:6b:65:6e:3d:30:58:4e:73:55:43:71:66:52:70:48:67:77:4e:6d:51:39:
55:33:57:69:66:70:49:57:62:6d:4b:73:61:4a:70:4b:77:6d:68:54:43:56:
76:56:58:53:71:4d:75:70:43:73:44:4c:6d:77:2d:47:71:59:69:52:5a:6a:
56:33:6a:65:75:6b:69:6d:38:42:39:42:50:7a:5a:74:36:6a:49:59:6c:56:
45:59:69:63:55:50:49:34:31:26:47:65:6e:64:65:72:3d:4d:26:46:69:72:
73:74:4e:61:6d:65:3d:4d:61:78:26:4c:61:73:74:4e:61:6d:65:3d:4c:61:
67:72:6f:6e:26:43:6f:6d:70:61:6e:79:3d:46:69:72:6d:61:2b:31:26:53:7
4:72:65:65:74:41:64:64:72:65:73:73:3d:55:6c:69:63:65:2b:31:32:33:2
6:43:69:74:79:3d:50:72:61:68:61:26:5a:69:70:50:6f:73:74:61:6c:43:6f
:64:65:3d:31:39:30:30:30:26:50:68:6f:6e:65:3d:25:32:42:34:32:30:31:
32:33:34:35:36:37:38:39:26:50:68:6f:6e:65:5f:6d:61:73:6b:3d:25:32:4
2:34:32:30:2b:31:32:33:2b:34:35:36:2b:37:38:39:26:45:6d:61:69:6c:3
d:45:6d:61:69:6c:31:31:31:25:34:30:74:65:73:74:2e:63:7a:26:50:61:7
3:73:77:6f:72:64:3d:61:62:63:31:32:33:26:43:6f:6e:66:69:72:6d:50:61
:73:73:77:6f:72:64:3d:61:62:63:31:32:33:26:68:70:69:6e:70:75:74:3d:
26:61:63:63:65:70:74:2d:70:72:69:76:61:63:79:2d:70:6f:6c:69:63:79:
3d:6f:6e:26:67:2d:72:65:63:61:70:74:63:68:61:2d:72:65:73:70:6f:6e:7
3:65:3d:30:33:41:47:64:42:71:32:37:6d:56:39:74:48:6a:34:73:5f:4a:4
3:66:79:31:66:38:55:7a:47:36:5a:49:32:4c:53:61:66:6e:43:63:2d:55:4
2:52:36:5f:64:57:2d:66:4f:35:59:72:5a:59:4f:34:45:6a:6a:78:68:5f:50:
5f:34:5a:76:64:73:53:78:42:31:64:37:30:49:48:6a:44:67:4e:35:46:37:
66:6b:35:37:30:52:5a:4d:2d:71:75:62:71:71:4a:41:66:65:65:52:61:4b:
4b:62:55:52:62:5a:76:61:30:38:43:74:6c:38:4f:30:70:2d:58:53:62:43:
71:6b:56:53:34:65:4f:37:46:4d:7a:6d:74:50:36:46:46:49:50:69:4b:5a:
44:6b:33:67:31:65:56:68:68:32:68:6d:69:7a:4a:37:69:55:61:45:68:32:
69:4d:68:65:5a:66:79:6c:7a:4b:67:64:4d:66:39:47:61:71:4d:78:72:6c:
71:36:6a:50:57:34:31:36:37:61:6c:55:78:56:2d:76:4e:76:38:46:44:6f:
44:59:76:61:36:57:6c:59:4a:54:69:75:77:59:62:76:47:4e:72:6b:58:51:
61:76:4f:70:61:4e:4e:4f:58:66:46:50:4c:2d:5f:39:30:48:4e:75:67:56:4
9:63:71:52:54:68:44:58:4b:7a:64:69:59:53:42:63:6a:65:43:6a:6d:6e:3
6:33:4b:45:71:71:5a:4e:39:77:42:44:68:4e:49:54:4f:45:46:38:4f:47:62
:6f:65:54:55:4b:32:58:45:63:72:56:73:66:50:67:75:71:48:77:51:55:65:
6c:63:63:4e:50:41:6d:56:4f:7a:75:52:68:35:2d:51:32:6f:54:61:72:66:6
c:43:72:35:72:38:41:55:77:48:31:65:31:36:33:54:48:6a:70:59:6b:76:6
6:4b:38:57:61:5f:44:52:36:7a:47:45:4d:74:57:4a:34:49:4c:75:79:71:7
6:58:35:65:35:36:58:74:71:43:75:68:46:50:6a:58:61:5a:45:6d:52:42:5
9:6f:54:45:5a:68:57:62:44:65:4f:54:65:59:49:79:30:59:4e:6b:4d:38:50
:5a:71:4c:35:47:57:42:5a:2d:58:37:6c:74:70:58:51:5a:52:31:50:6f:63:
53:64:79:31:71:71:63:68:6d:48:79:76:54:53:6f:52:63:4d:41:76:43:41:
26:72:65:67:69:73:74:65:72:2d:62:75:74:74:6f:6e:3d:52:65:67:69:73:
74:72:6f:76:61:74"
632. },
633. "http": {
634. "http.file_data":
"__RequestVerificationToken=0XNsUCqfRpHgwNmQ9U3WifpIWbm
KsaJpKwmhTCVvVXSqMupCsDLmw-
GqYiRZjV3jeukim8B9BPzZt6jIYlVEYicUPI41&Gender=M&FirstName
=Max&LastName=Lagron&Company=Firma+1&StreetAddress=Ulice
+123&City=Praha&ZipPostalCode=19000&Phone=%2B4201234567

89&Phone_mask=%2B420+123+456+789&Email=Email111%40test.cz&Password=abc123&ConfirmPassword=abc123&hpinput=&accept-privacy-policy=on&g-recaptcha-response=03AGdBq27mV9tHj4s_JCfy1f8UzG6ZI2LSafnCc-UBR6_dW-fO5YrZYO4Ejjxh_P_4ZvdsSxB1d70IHjDgN5F7fk570RZM-qubqqJAfeeRaKKbURbZva08Ctl8O0p-XSbCqkVS4eO7FMzmtP6FFIPiKZDk3g1eVhh2hmizJ7iUaEh2iMheZfylzKgdMf9GaqMxrlq6jPW4167alUxV-vNv8FDoDYva6WlYJTiuwYbvGNrkXQavOpaNNOXfFPL-_90HNugVIcqRThDXKzdiYSBcjeCjmn63KEqqZN9wBDhNITOEF8OGboeTUK2XEcrVsfPguqHwQUelccNPAmVOzuRh5-Q2oTarflCr5r8AUwH1e163THjpYkvfK8Wa_DR6zGEMtWJ4ILuyqvX5e56XtqCuhFPjXaZEmRBYoTEZhWbDeOTeYIy0YNkM8PZqL5GWBZ-X7ltpXQZR1PocSdy1qqchmHyvTSoRcMAvCA&register-button=Registrovat",

635. "data": {

636. "data.data":
"5f:5f:52:65:71:75:65:73:74:56:65:72:69:66:69:63:61:74:69:6f:6e:54:6f:6b:65:6e:3d:30:58:4e:73:55:43:71:66:52:70:48:67:77:4e:6d:51:39:55:33:57:69:66:70:49:57:62:6d:4b:73:61:4a:70:4b:77:6d:68:54:43:56:76:56:58:53:71:4d:75:70:43:73:44:4c:6d:77:2d:47:71:59:69:52:5a:6a:56:33:6a:65:75:6b:69:6d:38:42:39:42:50:7a:5a:74:36:6a:49:59:6c:56:45:59:69:63:55:50:49:34:31:26:47:65:6e:64:65:72:3d:4d:26:46:69:72:73:74:4e:61:6d:65:3d:4d:61:78:26:4c:61:73:74:4e:61:6d:65:3d:4c:61:67:72:6f:6e:26:43:6f:6d:70:61:6e:79:3d:46:69:72:6d:61:2b:31:26:53:74:72:65:65:74:41:64:64:72:65:73:73:3d:55:6c:69:63:65:2b:31:32:33:26:43:69:74:79:3d:50:72:61:68:61:26:5a:69:70:50:6f:73:74:61:6c:43:6f:64:65:3d:31:39:30:30:30:26:50:68:6f:6e:65:3d:25:32:42:34:32:30:31:32:33:34:35:36:37:38:39:26:50:68:6f:6e:65:5f:6d:61:73:6b:3d:25:32:42:34:32:30:2b:31:32:33:2b:34:35:36:2b:37:38:39:26:45:6d:61:69:6c:3d:45:6d:61:69:6c:31:31:31:25:34:30:74:65:73:74:2e:63:7a:26:50:61:73:73:77:6f:72:64:3d:61:62:63:31:32:33:26:43:6f:6e:66:69:72:6d:50:61:73:73:77:6f:72:64:3d:61:62:63:31:32:33:26:68:70:69:6e:70:75:74:3d:26:61:63:63:65:70:74:2d:70:72:69:76:61:63:79:2d:70:6f:6c:69:63:79:3d:6f:6e:26:67:2d:72:65:63:61:70:74:63:68:61:2d:72:65:73:70:6f:6e:73:65:3d:30:33:41:47:64:42:71:32:37:6d:56:39:74:48:6a:34:73:5f:4a:43:66:79:31:66:38:55:7a:47:36:5a:49:32:4c:53:61:66:6e:43:63:2d:55:42:52:36:5f:64:57:2d:66:4f:35:59:72:5a:59:4f:34:45:6a:6a:78:68:5f:50:5f:34:5a:76:64:73:53:78:42:31:64:37:30:49:48:6a:44:67:4e:35:46:37:66:6b:35:37:30:52:5a:4d:2d:71:75:62:71:71:4a:41:66:65:65:52:61:4b:4b:62:55:52:62:5a:76:61:30:38:43:74:6c:38:4f:30:70:2d:58:53:62:43:71:6b:56:53:34:65:4f:37:46:4d:7a:6d:74:50:36:46:46:49:50:69:4b:5a:44:6b:33:67:31:65:56:68:68:32:68:6d:69:7a:4a:37:69:55:61:45:68:32:69:4d:68:65:5a:66:79:6c:7a:4b:67:64:4d:66:39:47:61:71:4d:78:72:6c:71:36:6a:50:57:34:31:36:37:61:6c:55:78:56:2d:76:4e:76:38:46:44:6f:44:59:76:61:36:57:6c:59:4a:54:69:75:77:59:62:76:47:4e:72:6b:58:51:61:76:4f:70:61:4e:4e:4f:58:66:46:50:4c:2d:5f:39:30:48:4e:75:67:56:49:63:71:52:54:68:44:58:4b:7a:64:69:59:53:42:63:6a:65:43:6a:6d:6e:3

6:33:4b:45:71:71:5a:4e:39:77:42:44:68:4e:49:54:4f:45:46:38:4f:47:62
:6f:65:54:55:4b:32:58:45:63:72:56:73:66:50:67:75:71:48:77:51:55:65:
6c:63:63:4e:50:41:6d:56:4f:7a:75:52:68:35:2d:51:32:6f:54:61:72:66:6
c:43:72:35:72:38:41:55:77:48:31:65:31:36:33:54:48:6a:70:59:6b:76:6
6:4b:38:57:61:5f:44:52:36:7a:47:45:4d:74:57:4a:34:49:4c:75:79:71:7
6:58:35:65:35:36:58:74:71:43:75:68:46:50:6a:58:61:5a:45:6d:52:42:5
9:6f:54:45:5a:68:57:62:44:65:4f:54:65:59:49:79:30:59:4e:6b:4d:38:50
:5a:71:4c:35:47:57:42:5a:2d:58:37:6c:74:70:58:51:5a:52:31:50:6f:63:
53:64:79:31:71:71:63:68:6d:48:79:76:54:53:6f:52:63:4d:41:76:43:41:
26:72:65:67:69:73:74:65:72:2d:62:75:74:74:6f:6e:3d:52:65:67:69:73:
74:72:6f:76:61:74",
"data.len": "913"
}
}
}
}
}
]