UNIVERZITA PARDUBICE

FAKULTA ELEKTROTECHNIKY A INFORMATIKY

BAKALÁŘSKÁ PRÁCE

2017 Ondřej Dušek

Univerzita Pardubice

Fakulta elektrotechniky a informatiky

Analýza paketů za využití nástroje Wireshark

Ondřej Dušek

Bakalářská práce

2017

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: **2016/2017**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Ondřej Dušek**
Osobní číslo:	**I14085**
Studijní program:	**B2646 Informační technologie**
Studijní obor:	**Informační technologie**
Název tématu:	**Analýza paketů za využití nástroje Wireshark**
Zadávající katedra:	**Katedra informačních technologií**

Zásady pro vypracování:

Cílem práce je podrobně představit možnosti využití nástroje Wireshark pro analýzu síťového provozu, síťové bezpečnosti a prakticky tyto možnosti ověřit. V teoretické části autor podrobně představí analyzátor síťového provozu Wireshark a jeho možnosti pro analýzu síťové komunikace.
V praktické části pak autor navrhne a realizuje minimálně deset základních a pokročilých úloh na analýzu síťového provozu za využití nástroje Wireshark.

Rozsah grafických prací:

Rozsah pracovní zprávy: **40 stran**

Forma zpracování bakalářské práce: **tištěná**

Seznam odborné literatury:

BAXTER, James H. Wireshark essentials: get up and running with Wireshark to analyze network packets and protocols effectively. Birmingham: Packt Publishing, 2014. ISBN 978-1-78355-464-5.

NATH, Anish. Packet Analysis with Wireshark. 1. Birmingham, United Kingdom: Packt Publishing Limited, 2015. ISBN 9781785887819.

VERMA, Piyush. Wireshark Network Security. 1. Birmingham, United Kingdom: Packt Publishing Limited, 2015. ISBN 9781784393335.

Vedoucí bakalářské práce: **Mgr. Josef Horálek, Ph.D.**
Katedra informačních technologií

Datum zadání bakalářské práce: **31. října 2016**

Termín odevzdání bakalářské práce: **12. května 2017**

Univerzita Pardubice -8- Česká republika

L.S.

Ing. Zdeněk Němec, Ph.D.
děkan

Mgr. Josef Horálek, Ph.D.
vedoucí katedry

V Pardubicích dne 31. března 2017

Prohlášení autora

Prohlašuji, že jsem tuto práci vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 20. 3. 2017

Ondřej Dušek

ANOTACE

Bakalářská práce se zaměřuje na diagnostický nástroj Wireshark a jeho využití v praxi. Nejprve je představen úvod do ISO/OSI modelu sítě, poté jsou rozebrány protokoly, se kterými se pracovalo v praktické části. Následuje kapitola obsahující manuál k použití programu. Druhou polovinou práce je praktická část, ve které jsou popsány situace z praxe a jejich zobrazení, případně řešení ve Wiresharku.

KLÍČOVÁ SLOVA

Wireshark, ISO/OSI, paket, analýza, počítačová síť

TITLE

Packet analysis using Wireshark

ANNOTATION

Bachelor thesis is focused on the Wireshark diagnostic tool and its use in practice. First there is an introduction to ISO/OSI model of the network then protocols used in practical part are discussed. Following chapter contains a program manual. The second half of the thesis is practical part, which describes practical situations, their representation, or solution in Wireshark.

KEYWORDS

Wireshark, ISO/OSI, packet, analysis, network

OBSAH

Úvod 12
1 Cíl práce 13
2 Model ISO/OSI 14
Obecný popis 14
Fyzická vrstva 14
Linková vrstva 15
Síťová vrstva 15
Transportní vrstva 15
Relační vrstva 15
Prezentační vrstva 15
Aplikační vrstva 15
3 Protokoly 16
3.1 ARP 16
3.2 ICMP 16
ICMPv6 16
3.3 DHCP 17
DHCPv6 17
3.4 DNS 17
3.5 HTTP 18
3.6 IPv4 18
IPv6 18
3.7 TCP 19
4 Bezpečnost 20
Monitorování a analýza 20
Software 20
Tcpdump 20

Netcat 20
Ettercap 20
Nmap 21
5 Wireshark 22
5.1 Popis 22
5.2 Historie 22
5.3 Systémové požadavky 22
5.4 Instalace (na operačním systému Windows) 23
5.5 Rozložení 23
5.6 Hlavní nabídka 25
File 25
Edit 26
View 26
Go 27
Capture 28
Analyze 28
Statistics 29
Telephony, Wireless 29
Help 30
5.7 Panel filtrů 30
5.8 Hlavní okno 31
5.9 Stavový panel 31
6 Praktická část 33
6.1 Problém s DNS překladem adres 33
6.2 Nefunkční komunikace kvůli chybě směrování 33
6.3 Duplikované IP adresy 34
6.4 Nedostatek přidělovaných adres DHCP 34

6.5 Broadcast storm 35
6.6 Ztráta fragmentů 35
6.7 Připojení k bezdrátové síti 36
6.8 Man-in-the-middle útok 37
6.9 DoS útok 37
6.10 Nalezení přihlašovacích údajů v HTTP paketu 38
6.11 Brute-force útok 39
6.12 Geolokace IP 39
7 Závěr 41
8 Použitá literatura 42
9 Přílohy 43

SEZNAM ILUSTRACÍ A TABULEK

Obrázek 1 – Porovnání modelů 14
Obrázek 2 – Úvodní obrazovka 24
Obrázek 3 – Nastavení generátoru paketů 25
Obrázek 4 – File 25
Obrázek 5 – Edit 26
Obrázek 6 – View 27
Obrázek 7 – Go 27
Obrázek 8 – Capture 28
Obrázek 9 – Analyze 28
Obrázek 10 – Statistics 29
Obrázek 11 – Wireless 30
Obrázek 12 – Expression 30
Obrázek 13 – Hlavní okno 31
Obrázek 14 – Vlastnosti souboru 32
Obrázek 15 – Chybná adresa DNS serveru 33
Obrázek 16 – Snižování hodnoty TTL 34
Obrázek 17 – DHCP požadavky 35
Obrázek 18 – Broadcast storm 36
Obrázek 19 – Přihlášení do bezdrátové sítě 37
Obrázek 20 – H.O.I.C 38
Obrázek 21 – Přihlášení přes HTTP protokol 38
Obrázek 22 – Brute-force útok 39
Obrázek 23 – GeoIP 40

SEZNAM ZKRATEK A ZNAČEK

ARP	Address Resolution Protocol
CRC	Cyclic Redundancy Check
DoS	Denial of Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
ISO	International Organization for Standardisation
MAC	Media Access Control
OSI	Open Systém Interconnection
SSID	Service Set Identifier
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
TTL	Time To Live
VoIP	Voice over Internet Protocol
Wi-Fi	Wireless Fidelity

ÚVOD

Počítačové sítě jsou dnes většinou velmi rozsáhlé a s vývojem technologií se zvyšuje jejich složitost a možnosti. Je proto důležité mít síť stabilní a spolehlivou. Monitorování a analýza se tak staly důležitou součástí realizace a údržby sítě. Díky množství a kvalitě monitorovacích nástrojů jsou odborníci na toto téma ceněni, protože se nejedná o jednoduché záležitosti.

Monitorovací nástroje jsou vhodné nejen pro testování, zda je realizovaná síť v pořádku, ale také pro průběžné kontroly, zjišťování výpadku prvků nebo třeba pro nelegální činnosti. Získané informace se dají vyžívat mnoha způsoby.

Na začátku práce je kapitola o síťovém modelu ISO/OSI. Model je zde popsán z důvodu lepšího přehledu o tom, jak funguje komunikace po síti. Rozdělení komunikace na vrstvy také zjednodušuje představu o funkcích a využití jednotlivých protokolů.

Následuje kapitola s rozepsanými podrobnostmi o protokolech. Z obrovského množství jsou vybrány ty protokoly, se kterými se pracuje v praktické části práce. Je zde popsána jejich funkčnost i jednotlivé bity, ze kterých se skládá jejich hlavička.

Čtvrtá kapitola je zaměřena na bezpečnost sítí a jsou zde popsány některé základní monitorovací nástroje.

Kapitola Wireshark představuje manuál pro práci s tímto programem. Kromě základních informací je zde vysvětlení většiny používaných funkcí. Informace jsou podloženy přiloženými obrázky pro lepší představu.

Druhou polovinou práce je kapitola Praktická část, kde jsou realizovány některé příklady znázorňující práci s programem. Příklady jsou vybrány z praxe se zaměřením na odhalení problému nebo jako ukázka složitějšího síťového provozu.

1 CÍL PRÁCE

Cílem je úvod do monitorování přenosu dat po síti. Tato práce slouží zároveň jako návod pro používání programu Wireshark, protože obsahuje jeho kompletní popis s vysvětlením funkcí a uvádí praktickou ukázku použití. Ukázky zobrazují základní provoz sítě s nejčastějšími protokoly, se kterými se lze běžně setkat. Jsou zde zobrazeny ukázky monitorování v případě problémů nefunkčnosti sítě nebo některé z útoků, které lze pomocí Wiresharku buď odhalit, nebo ukázat jejich možnosti.

2 MODEL ISO/OSI

Obecný popis

Model ISO/OSI je abstraktní model rozdělení sítě, kde se v každé vrstvě odesílaný paket zapouzdří spolu s informacemi dodávanými danou vrstvou. Celkově se jedná o sedm vrstev:

- fyzická vrstva,
- linková vrstva,
- síťová vrstva,
- transportní vrstva,
- relační vrstva,
- prezentační vrstva,
- aplikační vrstva.

Tento model je pouze doporučením organizace ISO a nemusí být striktně dodržován při vývoji jednotlivých protokolů. Existuje ještě model TCP/IP, jenž vychází z ISO/OSI. Ten je však více flexibilní, protože spojuje některé vrstvy do jedné. Více na následujícím obrázku:

<table>
<tr><th>ISO/OSI</th><th>TCP/IP</th></tr>
<tr><td>Aplikační</td><td rowspan="3">Aplikační</td></tr>
<tr><td>Prezentační</td></tr>
<tr><td>Relační</td></tr>
<tr><td>Transportní</td><td>Transportní</td></tr>
<tr><td>Síťová</td><td>Síťová</td></tr>
<tr><td>Linková</td><td rowspan="2">Síťové rozhraní</td></tr>
<tr><td>Fyzická</td></tr>
</table>

Obrázek 1 – Porovnání modelů

Fyzická vrstva

Nejnižší vrstvou ISO/OSI modelu je fyzická vrstva. Na této úrovni se řeší fyzický přenos dat přes přenosová média. Vrstva definuje typy použitých kabelů, bezdrátový přenos, ze zařízení to jsou především rozbočovače (hub), opakovače (repeater) nebo síťové adaptéry. Důležitou součástí vrstvy jsou i technologie konverze digitálního signálu na analogový a nazpět nebo

kódovaní. Nejsou zde používané protokoly, pouze standardy pro kabeláž, bezdrátový přenos, koncovky, atd.

Linková vrstva

Hlavním účelem vrstvy je adresování mezi fyzicky propojenými zařízeními pomocí MAC adres používaných jako identifikátory jednotlivých zařízení. K paketu jsou adresy připojené informacemi v hlavičce a v patičce je kontrolní součet (CRC) potřebný pro kontrolu správnosti přenesených dat. Linkovými zařízeními vrstvy jsou mosty (bridge) a přepínače (switch). Typickými protokoly jsou Ethernet, Token Ring, FDDI, AppleTalk, PPP.

Síťová vrstva

Síťová vrstva je zodpovědná za směrování dat mezi sítěmi a používá logické adresování mezi odesílateli a příjemci. Vrstva paketu přidává hlavičku obsahující adresy a další informace. Součástí vrstvy jsou i technologie rozdělování dat mezi jednotlivé pakety a detekce chyb. O tyto služby se starají směrovače (router). Typickými protokoly jsou IP, RIP, ICMP, ARP.

Transportní vrstva

Tato vrstva poskytuje přenosové služby nižším vrstvám tak, aby data mohla být spolehlivě přenesena příjemci. Spojení se navazuje mezi porty aplikací. Vrstva se dále stará o segmentaci dat, tedy rozdělení velkých paketů na menší. Přidává paketu hlavičku použitého přenosového protokolu. Na této vrstvě operují firewally nebo proxy servery. Transportními protokoly jsou UDP, TCP, SPX.

Relační vrstva

Protokoly na relační vrstvě nastavují a udržují spojení mezi počítači. To je důležité především při posílání většího množství dat najednou. Typickými protokoly jsou NetBIOS, SAP, SDP, NWLink.

Prezentační vrstva

Prezentační vrstva kóduje a dekóduje data, aby mohla být odeslána příjemci, a zároveň umožňuje šifrování. K datům přidává informaci o typu souboru a jeho velikosti. Mezi mnoha protokoly na prezentační vrstvě lze najít například ASCII, MPEG, JPEG nebo MIDI.

Aplikační vrstva

Nejvyšší vrstvou se rozumí aplikační vrstva, tedy rozhraní pro uživatele, jediná vrstva, kterou uživatel doopravdy vidí. Typickými protokoly jsou HTTP, SMTP, FTP, telnet.

3 PROTOKOLY

Protokol je standardizovaná forma dat posílaných po síti. Existuje mnoho variant, od jednoduchých po složité, každý však slouží svému účelu.

3.1 ARP

ARP (Address Resolution Protocol) je protokol linkové vrstvy. Používá se při nacházení MAC adres ostatních zařízení v podsíti. ARP dotaz s informacemi o odesílateli je posílán na broadcast a hledané zařízení mu odpovídá ARP odpovědí s informacemi o sobě.

Protokol obsahuje:

- 0-15. bit – hardwarový typ,
- 16-31. bit – protokolový typ,
- 32-39. bit – délka hardwarové adresy,
- 40-47. bit – délka protokolové adresy,
- 48-63. bit – typ operace (žádost/odpověď).
- 64-107. bit – MAC adresa odesílatele,
- 108-139. bit – protokolová adresa odesílatele,
- 140-187. bit – MAC adresa příjemce (v žádosti je ignorováno),
- 188-219. bit – protokolová adresa adresáta.

3.2 ICMP

ICMP (Internet Control Message Protocol) je protokol síťové vrstvy používaný především pro informování o problému chybovými zprávami nebo pro zjištění dostupnosti nástrojem ping. Je definovaný v RFC 792.

ICMP zpráva se zapouzdřuje IP paketem, který chybovou zprávu vyvolal.

Protokol obsahuje:

- 0-7. bit – typ ICMP zprávy,
- 8-15. bit – kód ICMP zprávy upřesňující typ problému,
- 16-31. bit – kontrolní součet.

ICMPv6

ICMPv6 (Internet Control Message Protocol for IPv6) je obdoba ICMP s několika rozdíly. Hlavním rozdílem je, že je využíván protokolem IPv6 oproti předchozímu.

Hlavička protokolu zůstává stejné jako u předchozí verze.

3.3 DHCP

DHCP (Dynamic Host Configuration Protocol) je protokol aplikační vrstvy používaný pro automatickou konfiguraci IP adres klientů z volných nabídek rozsahu DHCP serveru.

Protokol obsahuje:

- 0-7. bit – typ DHCP zprávy (požadavek/odpověď),
- 8-15. bit – typ hardwarového spojení,
- 16-23. bit – délka hardwarové adresy,
- 24-31. bit – bity pro relay agenty (uzly mezi dhpc serverem a klientem),
- 32-63. bit – identifikační číslo DHCP zprávy,
- 64-79. bit – doba žádosti klienta o adresu,
- 80-95. bit – příznaky,
- 96-223. bit – čtyři sekce pro adresy,
- 224-351. bit – hardwarová adresa klienta,
- 352-863. bit – název serveru,
- 864-1887. bit – název bootovacího souboru,
- nepovinné parametry.

DHCPv6

DHCPv6 (Dynamic Host Configuration Protocol for IPv6) je obdoba DHCP pro IPv6. Mezi rozdíly patří zasílání žádosti o adresu na multicast (více adresátů) místo broadcastu (všichni dostupní) nebo možnost více adres na jedno rozhraní.

3.4 DNS

DNS (Domain Name System) je protokol aplikační vrstvy využívaný pro výměnu informací mezi klientem a DNS serverem. Informacemi je myšlen překlad IP adres na jejich doménová jména a naopak.

Protokol obsahuje:

- 0-15. bit – identifikace,
- 16. bit – příznak určující, jestli se jedná o požadavek nebo odpověď,
- 17-20. bit – typ DNS zprávy,
- 21-27. bit – různé jedno-bitové příznaky,
- 28-31. bit – návratový kód,

- 32-95. bit – čtyři stejně velké sekce s počtem požadavků a odpovědí,
- další bity – čtyři sekce s daty požadavků a odpovědí.

3.5 HTTP

HTTP (Hypertext Transfer Protocol) je protokol aplikační vrstvy přenášející webová data ve formátu html. Vyšší verze umí přenášet jakákoliv data.

HTTP se dělí na dva typy a to HTTP request (požadavek) a HTTP response (odpověď). Klient odesílá požadavek s dotazovací metodou, která určuje, zda chce uživatel data stáhnout, nahrát smazat nebo něco jiného. Po obdržení požadavku odesílá server odpověď s kódem (např. 200 pro úspěch nebo chybový kód začínající číslem 4).

3.6 IPv4

IPv4 (Internet Protocol version 4) je protokol síťové vrstvy pro směrování paketů. Protokol se nestará o spolehlivé doručení, pouze o přiblížení dat svému cíli. Skládá se z hlavičky a odesílaných dat.

Protokol obsahuje:

- 0-3. bit – verze protokolu,
- 4-7. bit – délka hlavičky,
- 8-15. bit – typ služby,
- 16-31. bit – celková délka paketu,
- 32-47. bit – identifikační hodnota,
- 48-50. bit – fragmentační příznaky,
- 51-63. bit – pořadí fragmentu,
- 64-71. bit – TTL,
- 72-79. bit – typ následujícího vnitřního protokolu,
- 80-95. bit – kontrolní součet hlavičky,
- 96-127. bit – zdrojová adresa
- 128-159. bit – cílová adresa,
- nepovinné parametry.

IPv6

IPv6 (Internet Protocol version 6) je rozšíření IPv4. Rozdíl je především v rozšíření hlavičky v oblasti adres.

Protokol obsahuje:

- 0-3. bit – verze protokolu,
- 4-11. bit – třída provozu,
- 12-31. bit – tabulka toku,
- 32-47. bit – délka dat,
- 48-55. bit – typ následujícího vnitřního protokolu,
- 56-63. bit – limit skoků (TTL),
- 64-191. bit – zdrojová adresa,
- 192-319. bit – cílová adresa.

3.7 TCP

TCP (Transmission Control Protocol) je protokol transportní vrstvy. Tento protokol se používá na vytvoření spojení mezi dvěma zařízeními. Zároveň garantuje spolehlivý přenos a také doručení fragmentů ve správném pořadí.

Protokol obsahuje:

- 0-15. bit – zdrojový port,
- 16-31. bit – cílový port,
- 32-63. bit – číslo fragmentu,
- 64-95. bit – číslo následujícího fragmentu,
- 96-99. bit – počáteční bit dat v paketu,
- 100-105. bit – rezervováno,
- 106-111. bit – ovládací bity,
- 112-127. bit – okno,
- 128-145. bit – kontrolní součet,
- 146-161. bit – ukazatel na prioritní data,
- nepovinné parametry,
- data.

4 BEZPEČNOST

Bezpečnost počítačových sítí je dnes jedním z nejdůležitějších problémů, které řeší podstatná část uživatelů.

Monitorování a analýza

Základem kontroly bezpečnosti je monitorování sítě. Monitorováním a analýzou lze objevit většinu možných chyb a bezpečnostních děr.

Software

Pro kontrolu provozu na síti existuje mnoho nástrojů. Zde jsou uvedeny nejpoužívanější alternativy k Wiresharku.

Tcpdump

Tcpdump je nástroj běžící na příkazové řádce. Umožňuje zachytávání a zobrazování obsahu TCP/IP a jiných paketů podle zadaného filtru. Je funkční na operačních systémech UNIX i Windows (verze WinDump). Běžně se využívá pro analýzu počítačových sítí, jejich chování a výkon a také aplikací komunikujících po síti.

Netcat

Netcat čte a zapisuje data procházející skrz síťovou komunikaci, používající TCP/IP protokol. Jedná se o utilitu navrženou tak, aby mohla být využívána jinými programy a skripty. Nástroj dokáže vytvořit mnoho různých typů spojení, stačí jen nastavit požadované parametry. To je zajištěno použitím tunelového módu. Podporuje operační systémy UNIX.

Ettercap

Ettercap simuluje Man in the middle útok, což znamená, že se uvnitř sítě nachází zařízení, které zachytává, čte a přeposílá data správnému adresátovi. Toho lze dosáhnout promiskuitním režimem (vlastností síťové karty umožňující zachytávání cizí komunikace) a tzv. ARP poisoningem (technologie rozesílání ARP paketů a nastavení stejné MAC adresy jako má adresát a zachycení dat adresovaných jemu). Používá se buď na odposlouchávání komunikace po síti (např. přihlašovací údaje), nebo jako monitorovací nástroj (dokáže nacházet i další útočníky na síti). Lze jej rozšířit pomocí mnoha rozšíření pro odposlech, např. možnost zjištění přihlašovacích údajů z velkého množství protokolů, včetně přihlášení otiskem prstu nebo obsahu zobrazovaných webových stránek. Opět je podporován operačními systémy UNIX.

Nmap

Nmap je utilita pro zjišťování rozestavění sítě a bezpečnosti. Použitím vlastních IP paketů nachází zařízení připojené k síti, jejich zabezpečení (operační systém, paketové filtry, dostupné služby) a další. Nástroj byl vytvořen ve verzích pro Linux, Mac OS i Windows.

5 WIRESHARK

5.1 Popis

Wireshark je nejrozšířenější paketový analyzátor na světě (Wireshark · Go Deep., 2017). Umožňuje sledování přenosu dat na síti na úrovni jednotlivých paketů. Zároveň je jakýmsi standardem pro analýzu pro mnoho organizací, vládní agentury nebo vzdělávací instituce.

Jedná se o open source (licence zaručující dostupnost programu zdarma s otevřeným zdrojovým kódem) multiplatformní software, lze ho používat na UNIXových systémech, jako jsou Linux, Mac OS X, BSD, Solaris nebo na operačním systému Windows. Program lze stáhnout z oficiálního webu.

Wireshark je freeware (svobodný software) vydávaný pod licencí GNU General Public License (Všeobecná veřejná licence GNU), verze 2.

5.2 Historie

Program původně vznikl jako projekt Geralda Combse v roce 1998. Ten začal vyvíjet analytický program pro jednoho poskytovatele internetu, pro kterého pracoval, protože cena dostupných nástrojů byla příliš vysoká a nepodporovaly jimi používaný operační systém. Tak vznikl nástroj Ethereal.

Roku 2006 nastoupil Combs do nového zaměstnání ve společnosti CACE Technologies. Stále vlastnil většinu práv na zdrojový kód Etherealu, takže začal vyvíjet nástroj Wireshark. Poučil se z mnoha chyb předchozího programu a postupně dostal, za pomoci mnoha dalších vývojářů, Wireshark na pozici nejpoužívanějšího analytického nástroje. V průběhu času získal software několik ocenění, například InfoWorld, eWeek nebo PC Magazine – Editor's Choice.

5.3 Systémové požadavky

Uvedené požadavky jsou pro nejnovější verzi 2.2.5.

- Operační systém Windows Vista a vyšší, Windows Server 2008 a vyšší nebo linuxová distribuce (Apple macOS, Debian GNU/Linux, FreeBSD, Gentoo Linux, HP-UX, Mandriva Linux, NetBSD, OpenPKG, Red Hat Enterprise/Fedora Linux, Sun Solaris/i386, Sun Solaris/SPARC, Canonical Ubuntu).
- 64bitový AMD64/x86-64 nebo 32bitový x86 procesor.
- 400 MB RAM.
- 300 MB dostupné místo na pevném disku.

- 1024×768 px rozlišení obrazovky s alespoň 16bitovou barevnou hloubkou.
- Podporovaná síťová karta (Ethernet, 802.11, atd.).

Poslední verze podporující Windows XP byla 1.10 a Windows Server 2003 byla 1.12.

5.4 Instalace (na operačním systému Windows)

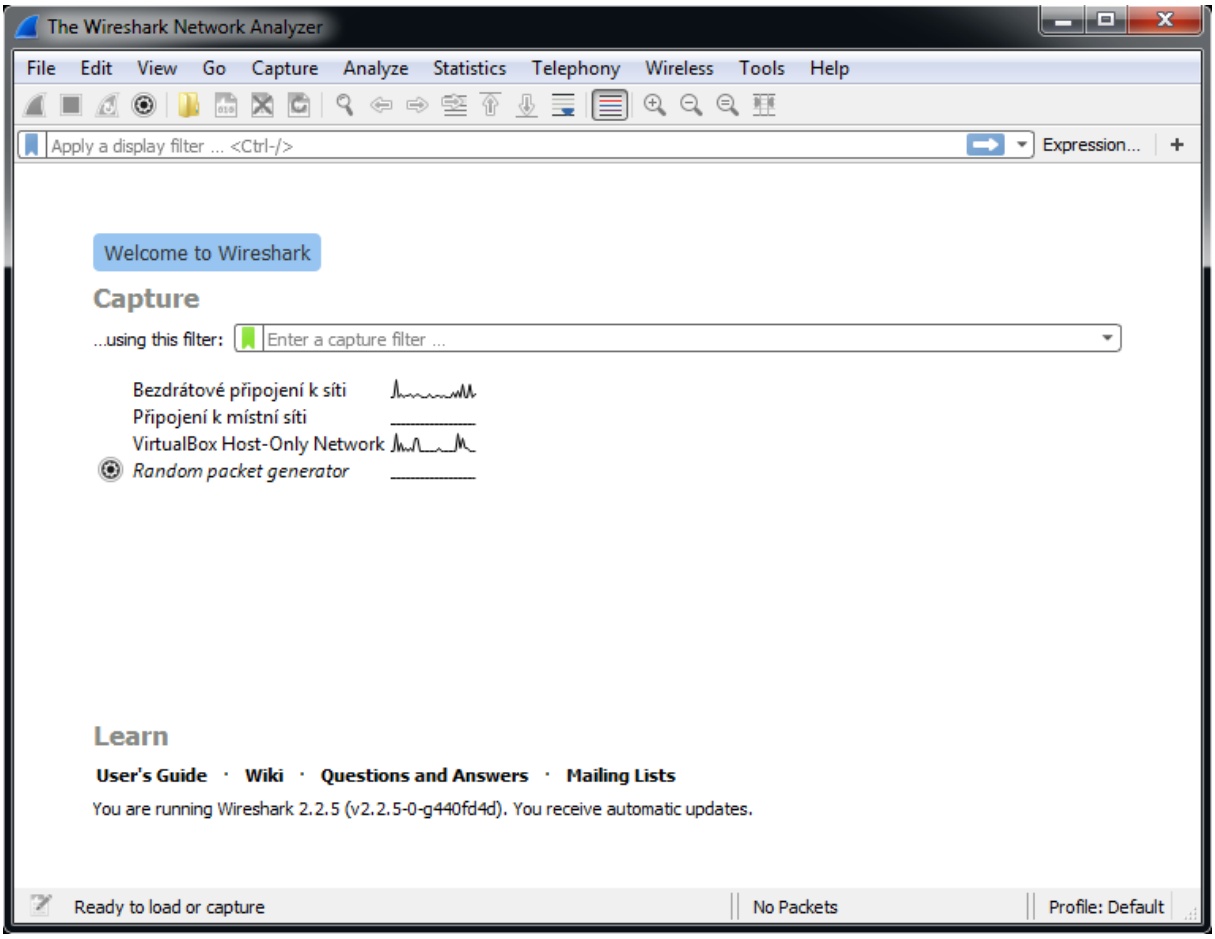
Po stažení programu z oficiálního webu spusťte stažený soubor s příponou exe. Během instalace je nabídnuto umístění instalace. Další nabídkou jsou rozšíření:

- Wireshark – hlavní program,
- TShark – hlavní program fungující přes příkazovou řádku,
- Wireshark 1 Legacy – starší uživatelské prostředí,
- Plugins & Extensions – rozšíření pro Wireshark a TShark,
    - Dissector Plugins,
    - Tree Statistics Plugins – rozšířené statistiky,
    - Mate (Meta Analysis and Tracing Engine) – uživatelem konfigurovatelné rozšíření pro zobrazovací filtry,
    - SNMP MIBs,
- Tools – přídavné nástroje příkazové řádky pro práci se soubory,
    - Editcap – úprava obsahu souborů a zápis dat do jiných,
    - Text2Pcap,
    - Reordercap – řazení dat v souboru podle času,
    - Mergecap – slučování více souborů do jednoho,
    - Capinfos – informace o souborech,
    - Rawshark – paketový filtr,
- User's Guide – uživatelská příručka.

Součástí instalace je i WinPcap nutný k monitorování přenosu po síti. Je to to nejdůležitější, co od Wiresharku čekáme, a bez něho lze pracovat pouze s daty z importovaných souborů.

5.5 Rozložení

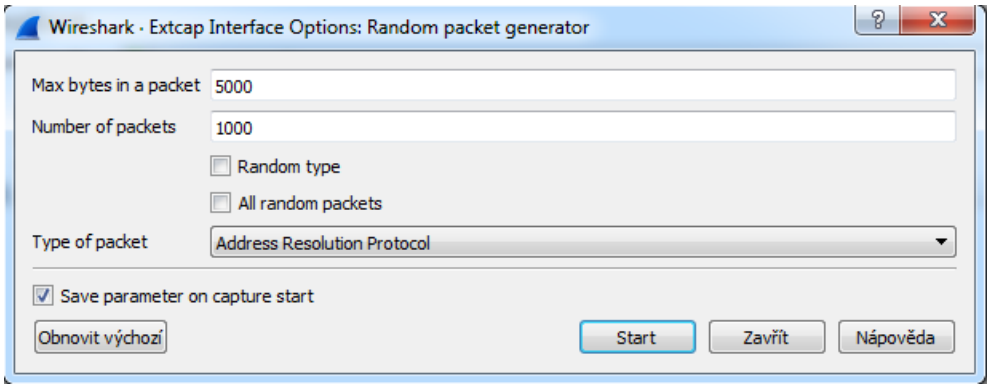
Po zapnutí programu je zobrazena úvodní obrazovka se zdroji, které je možné monitorovat. Podle měnících se grafů lze zjistit, které jsou aktivní a při instalaci rozšíření – nabízeného při instalaci – je zde navíc možnost generovat proud náhodných paketů.



Obrázek 2 – Úvodní obrazovka

V prvním řádku od shora je hlavní nabídka programu, pod ní výběr nejčastěji používaných nástrojů. Ten nemůže být upravován uživatelem, ale může být schován. Řádek se zadávacím polem je správa filtrů na zobrazování pouze požadovaných protokolů.

Hlavní okno obsahuje úvodní obrazovku s výběrem zdroje provozu. Random packet generator představuje náhodný generátor paketů. Vlevo před jeho názvem je ikona možností otevírající dialogové okno, kde lze tento nástroj nastavit. Zde lze zadat maximální velikost paketů, jejich počet nebo typ. Ovládací tlačítka jsou tady pro obnovení původního nastavení, spuštění generátoru, zavření dialogového okna a nápovědu.



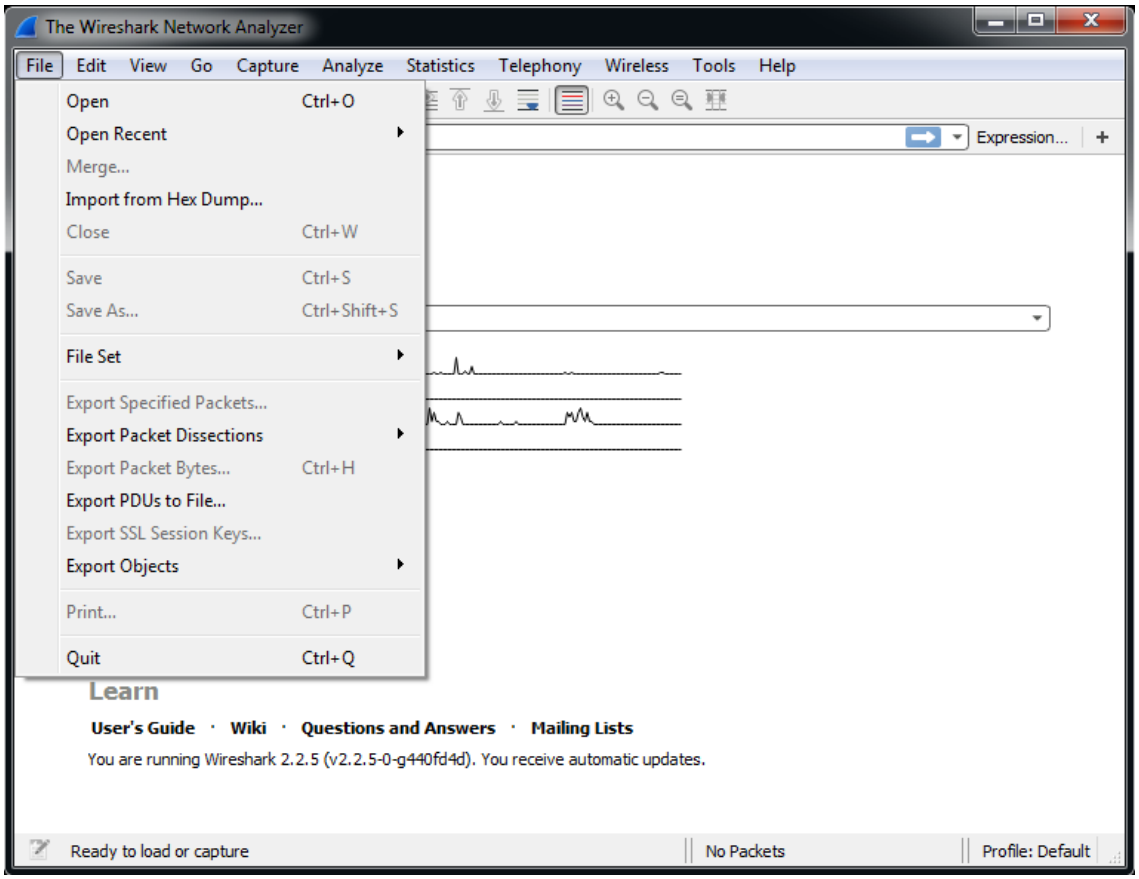
Obrázek 3 – Nastavení generátoru paketů

Ve spodní části je stavový řádek.

5.6 Hlavní nabídka

File

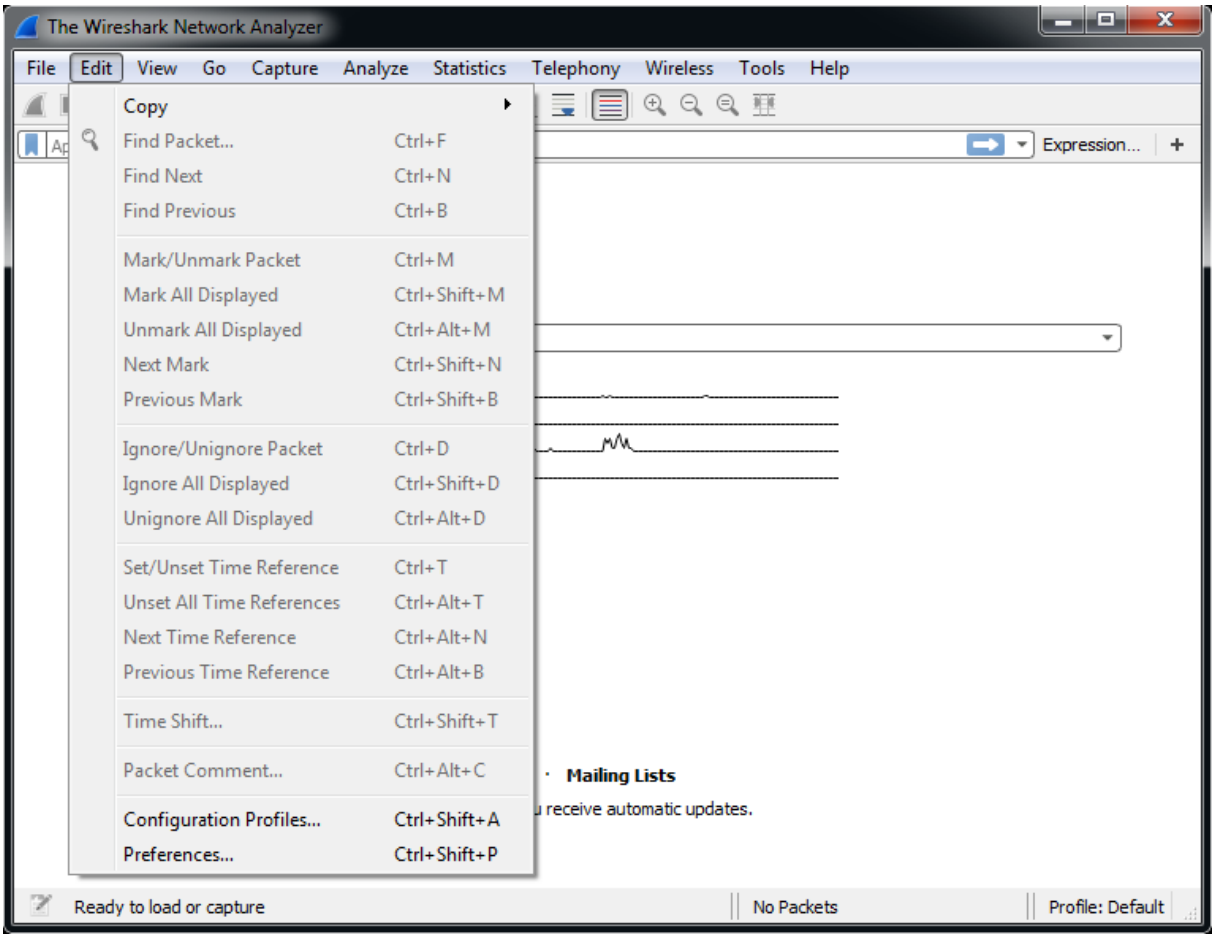
Ve File se pracuje se soubory a nastavením, kde lze například importovat nebo exportovat výpis z monitorování sítě. Pomocí nástroje Merge… se spojují získané pakety s jinými, již dříve odchycenými, do jednoho souboru (File Set). Exportovat se dají nejen seznamy paketů, různé analýzy, ale i jednotlivé soubory z http protokolů. Zároveň se zde i ukončuje program.



Obrázek 4 – File

Edit

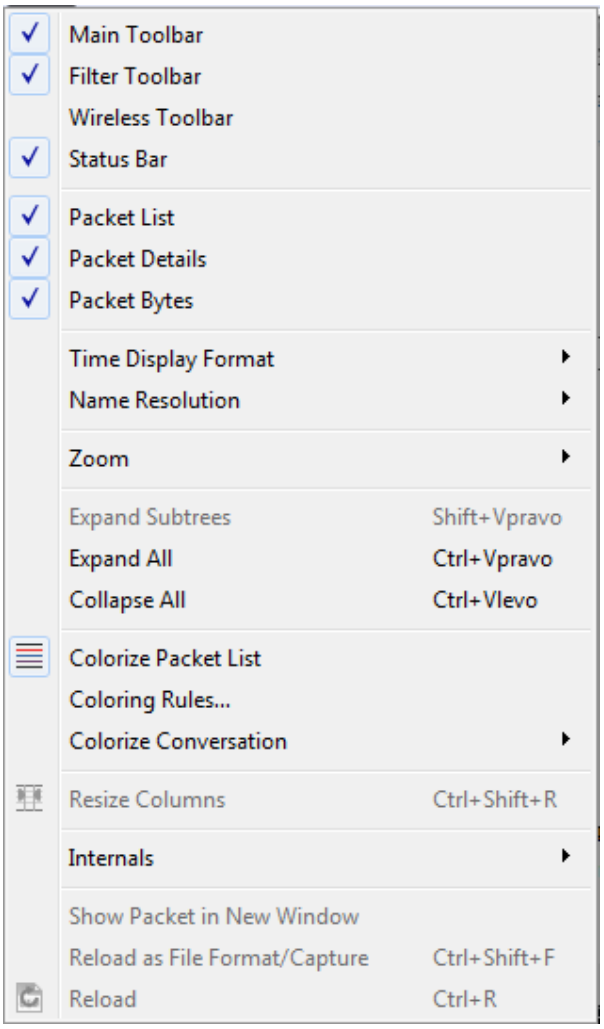
Zde se pracuje s jednotlivými pakety. Je tu vyhledávání paketů podle zadaných parametrů (běžný filtr, vyhledávání sekvence dat), možnost ignorování vybraného paketu (paket zešedne a nebude považován za existující), označení nebo odznačení některé sady paketů, nastavení referenčního časového bodu (následující časy zachycení budou přepočítány od tohoto bodu) a nastavení programu.



Obrázek 5 – Edit

View

Ve View se pracuje se zobrazením jednotlivých částí programu. První čtyři zobrazují rychlou nabídku, filtry a stavový řádek, další tři pracovní panely. Také se tu barevně označují vybrané pakety, zobrazují se v samostatných oknech nebo se tu přibližuje/oddaluje a tedy zvětšuje/zmenšuje velikost fontu.

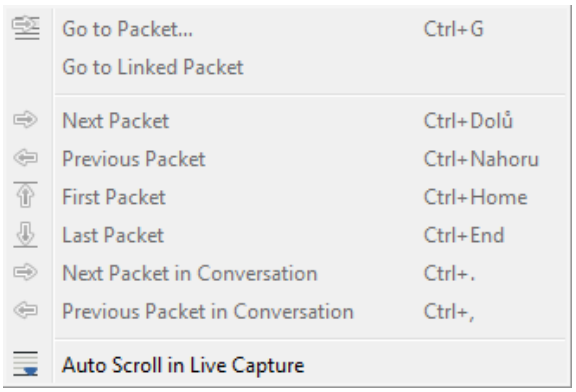


Obrázek 6 – View

Go

U každého paketu může být zobrazen obsah a tato nabídka slouží právě k tomuto účelu.

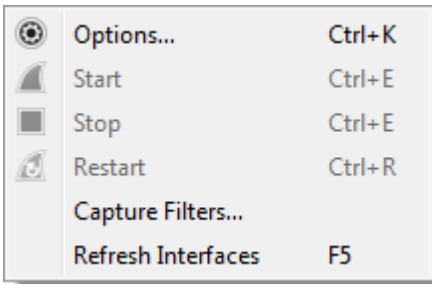
Go obsahuje položky pro ovládání výpisu paketů v těle programu. Přepíná se tady z jednoho paketu na druhý, vrací se zpět nebo se zapíná automatické přepínání jako v prezentaci.



Obrázek 7 – Go

Capture

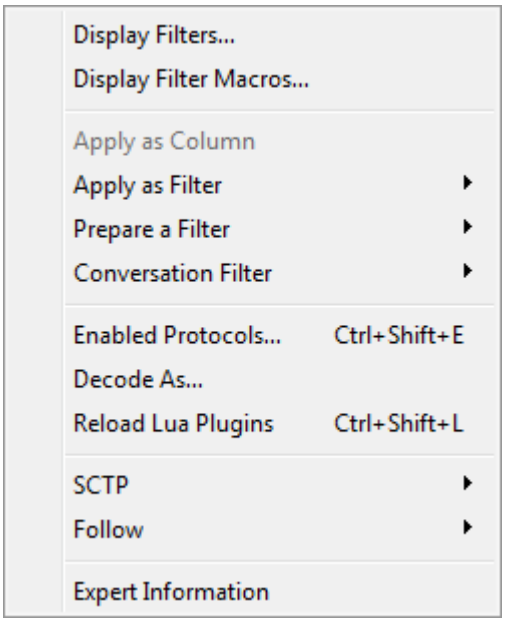
V nabídce Capture se spouští nebo vypíná samotné monitorování sítě. Nastavení způsobů zachytávání se provádí v Options…, síťová karty nebo rozhraní se vybírá v Refresh Interfaces.



Obrázek 8 – Capture

Analyze

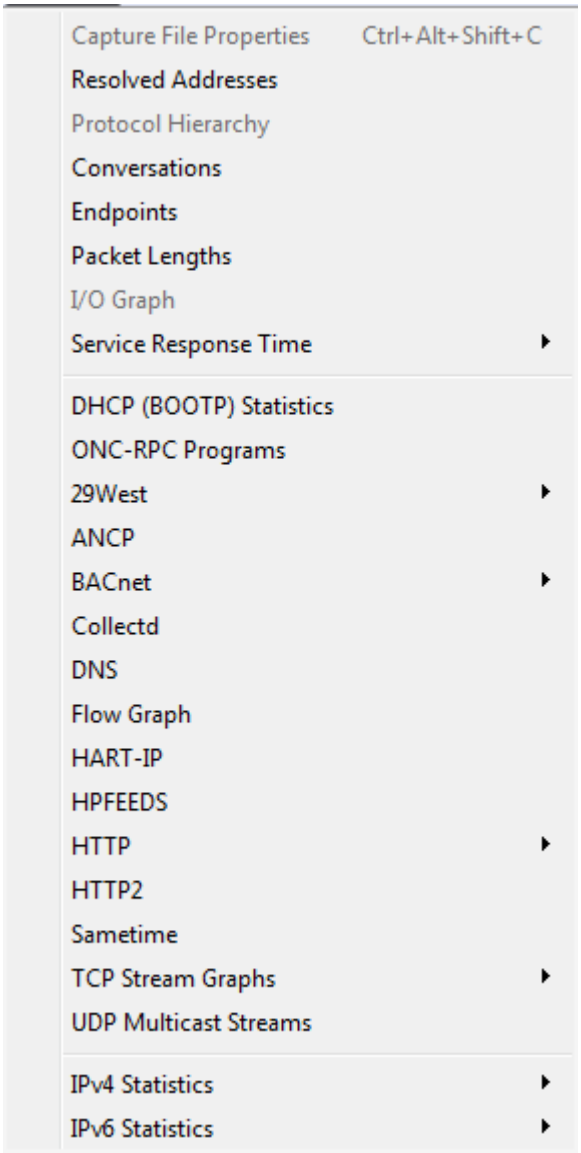
Analyze slouží ke správě filtrů a celkově pro správu zobrazení zaznamenaných paketů. V první části se nastavují filtry pro budoucí použití, ve druhé se vybírají filtry pro použití. Enabled Protocols… povoluje nebo zakazuje zobrazení vybraných protokolů.



Obrázek 9 – Analyze

Statistics

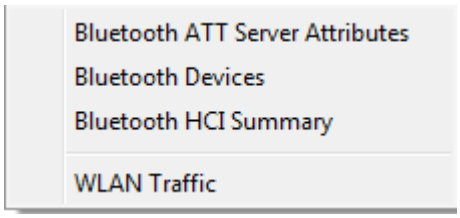
Položka Statistics umožňuje zobrazení přídavných oken se statistikami, shrnutí informací o paketech nebo hierarchii protokolů. Mezi ně patří mimo jiné např. informace o prošlých datech k jednotlivým koncovým bodům (Endpoints) nebo rozdíl mezi požadavkem a odpovědí pro některé protokoly. Kromě tabulkových statistik se dají zobrazit i grafy.



Obrázek 10 – Statistics

Telephony, Wireless

Zde se dají zobrazovat statistiky souvisejícími s telefonními přenosy včetně analýzy médií a diagramy. Umožňuje sledovat VoIP volání. Wireless zobrazuje statistiky Bluetooth a 802.11 bezdrátových přenosů.



Obrázek 11 – Wireless

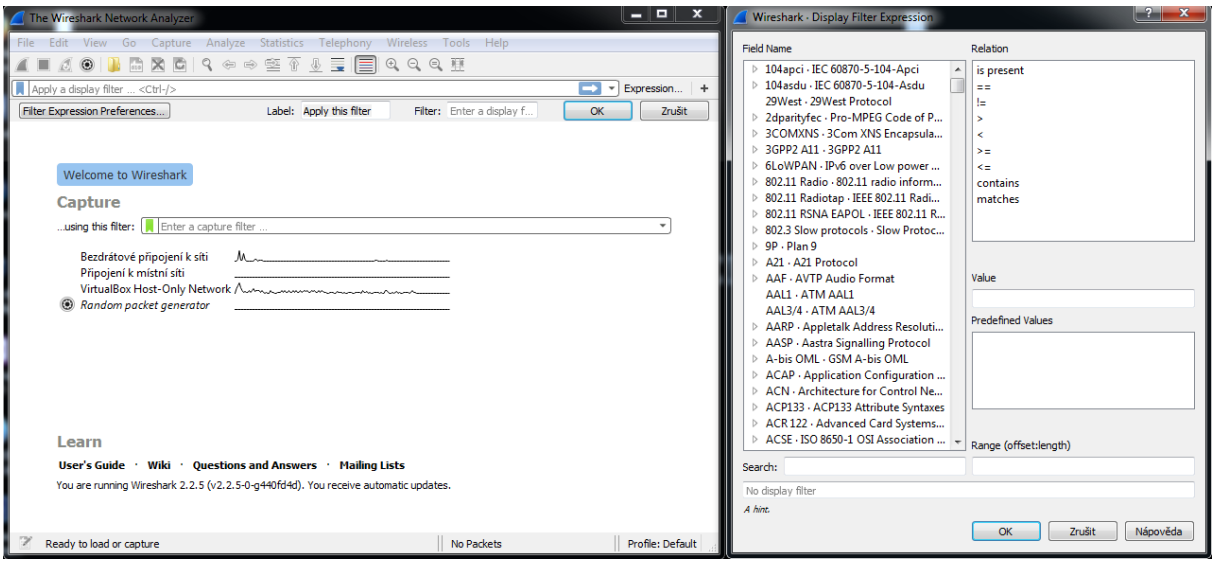
Help

Nabídka Help obsahuje odkazy na online i offline manuálové stránky, webové stránky vývojářů, nejčastěji kladené otázky s odpověďmi, Wiki nebo příklady použití. Dále je tu tlačítko pro aktualizaci programu a informace o něm.

5.7 Panel filtrů

Panel filtrů se nachází pod panelem nejčastěji používaných nástrojů. Obsahuje pole na ručně zadávané filtry, tlačítko Expression… a tlačítko plus. Po kliknutí na plus se pod tímto panelem zobrazí ještě jeden s nastavením programu z hlediska filtrů, možností pojmenovat zadávaný filtr, potvrzením nebo zrušením filtru.

Expression… otevírá dialogové okno s obrovským množstvím nabízených filtrů, ze kterých si pomocí relačních a dalších operátorů lze složit požadovaný filtr. Ve spodní části okna se vedle potvrzovacího a rušícího tlačítka nachází i tlačítko s nápovědou, které odkazuje na web s dokumentací.



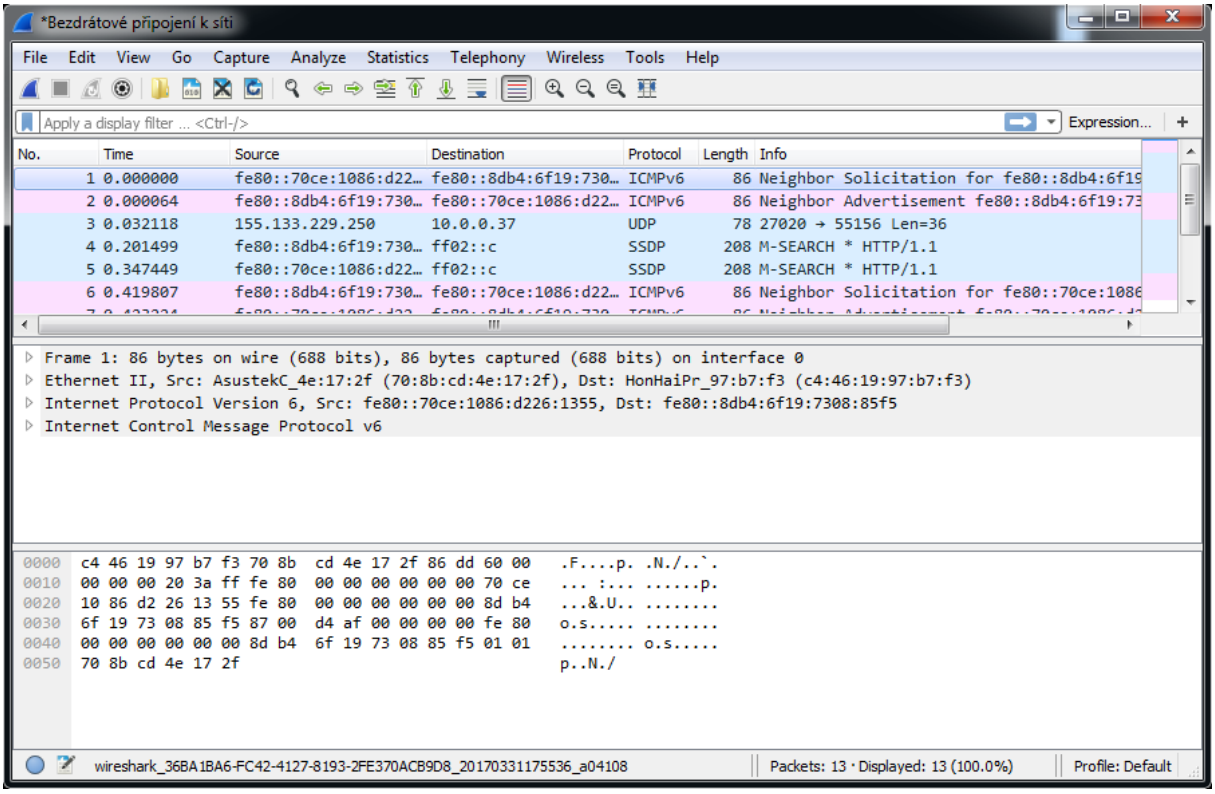
Obrázek 12 – Expression

5.8 Hlavní okno

Po zahájení snímání provozu se hlavní okno rozdělí na tři oblasti. Po vybrání paketu v první části se doplní informace do zbylých dvou. Těmto oblastem může uživatel měnit velikost posouvání oddělovacích čar.

V první části je výpis všech zachycených paketů s upravovatelnou hlavičkou. Plná hlavička se všemi daty obsahuje pořadové číslo paketu, čas zachycení, zdrojovou a cílovou adresu, použitý protokol, velikost paketu v bajtech a krátkou informaci.

V druhé oblasti jsou všechny podrobnosti o paketu a síťovém rozhraní. Zobrazované informace jsou například rozšířením základních informací z první oblasti nebo podrobnosti o protokolu. V nejnižší části je hexadecimální a textový výpis datové části paketu.



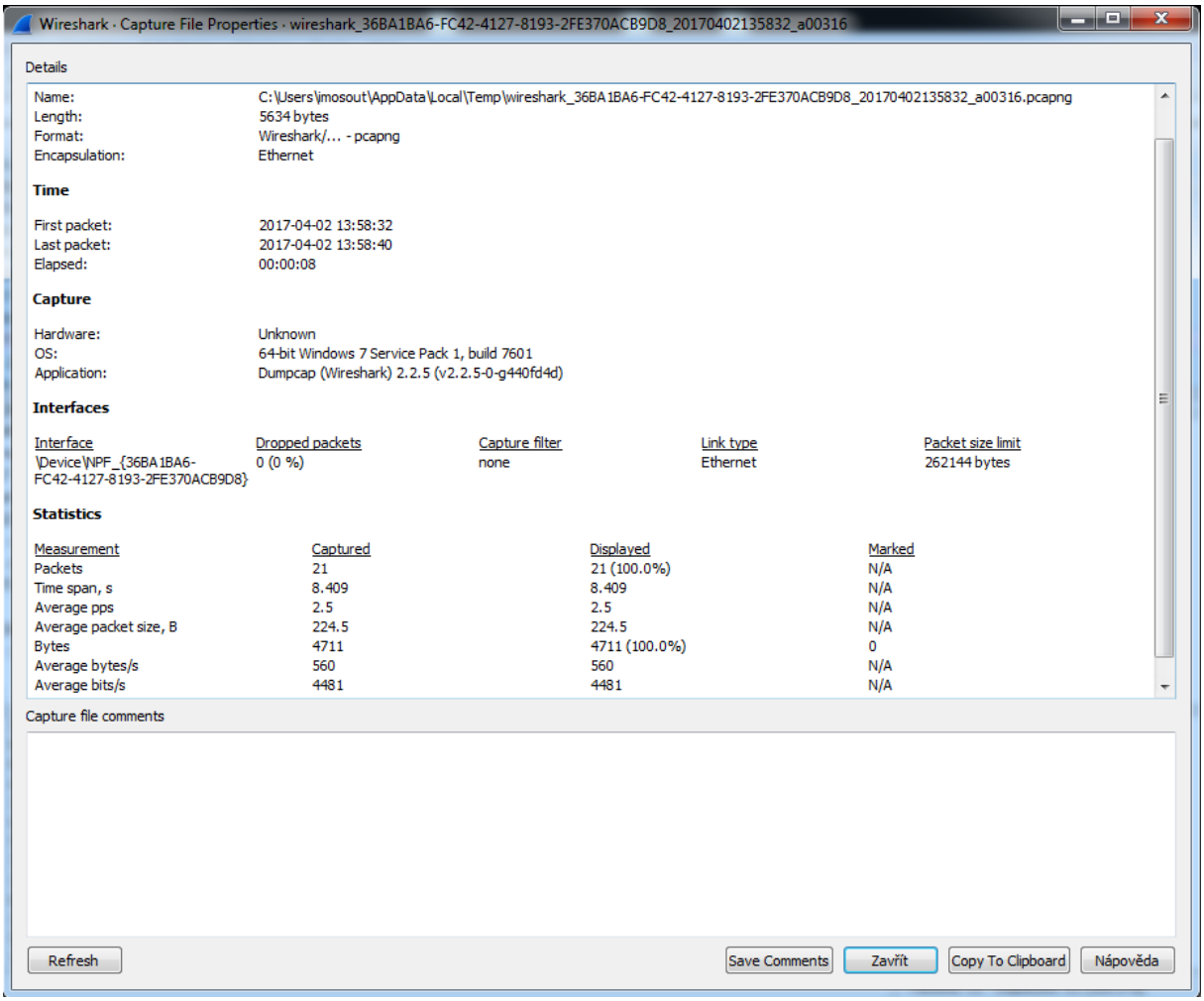
Obrázek 13 – Hlavní okno

5.9 Stavový panel

Stavový panel má opět tři části. Levá část může obsahovat barevnou semaforovou ikonu:

- šedá – vše probíhá standardně,
- tyrkysová – poznámka (příklad: aplikace vrátila běžný chybový kód),
- žlutá – varování (příklad: aplikace vrátila neobvyklý chybový kód),
- červená – kritická chyba.

Dále obsahuje ikonu spouštějící vlastnosti aktuálního souboru se zachycenými pakety. Mezi vlastnostmi lze najít cestu k souboru na disku, velikost souboru, časy monitorování, typ operačního systému, informace o rozhraních a statistiky. Tyto vlastnosti je možné uložit, zkopírovat do schránky nebo zavřít. Jako obvykle je tu i tlačítko s nápovědou.



Obrázek 14 – Vlastnosti souboru

Vedle ikony se nachází proměnný text s dodatkovými informacemi, například připravenost programu pro zachytávání, zkrácenou informaci o vybraném paketu nebo filtru.

Prostřední část zobrazuje celkový počet zachycených paketů a počet zobrazených paketů splňujících filtrovací pravidla. Vpravo je aktuální konfigurační profil, který lze změnit výběrem nového kliknutí na něj.

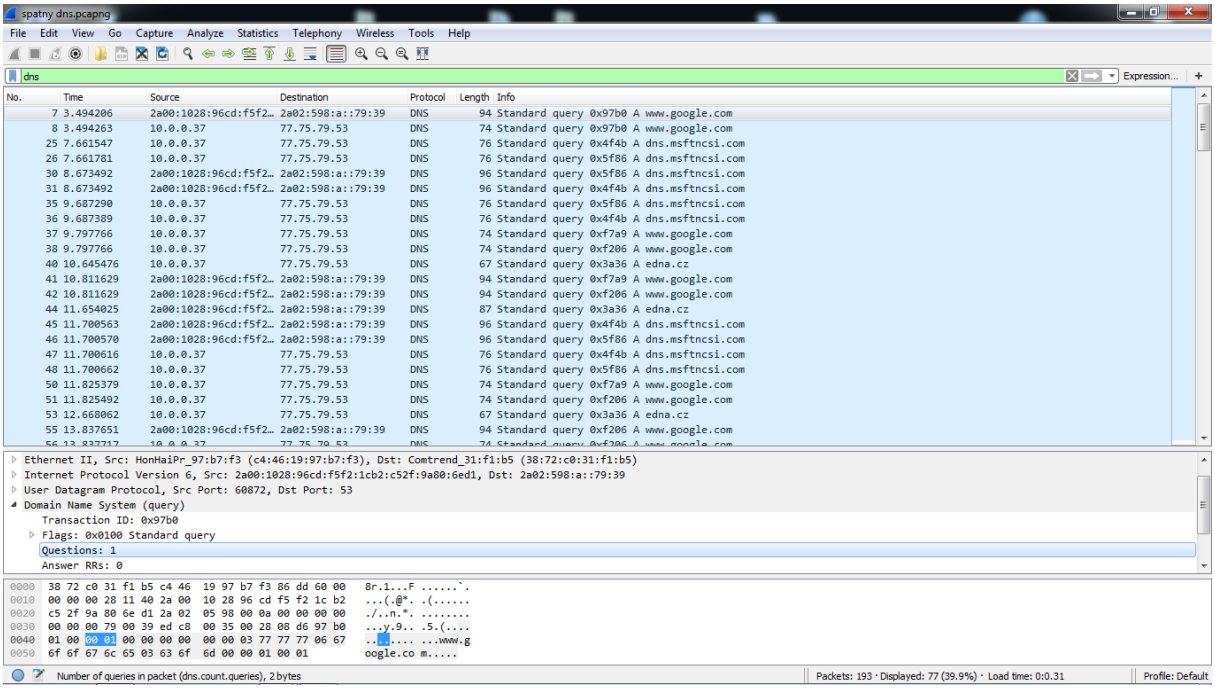
6 PRAKTICKÁ ČÁST

V praktické části bude představeno několik příkladů na zjišťování příčiny některých problémů nefunkčnosti sítě, ukázky základních situací, útoky na síť nebo práce s vybranými funkcemi programu.

6.1 Problém s DNS překladem adres

Při konfigurování nové sítě se může vyskytnout případ, kdy po úspěšném připojení k internetu nelze načíst webové stránky, ale po zadání jejich IP adresy ano. To je vždy způsobeno potížemi s DNS serverem, který překládá název domény na její IP adresu a naopak.

V tomto případě se jednalo o chybně nastavenou adresu DNS serveru. Při pokusu o kontaktování serveru se dotazy posílaly jinam a správná odpověď tedy nedorazila. Na následujícím obrázku je vidět množství nevyslyšených DNS dotazů.

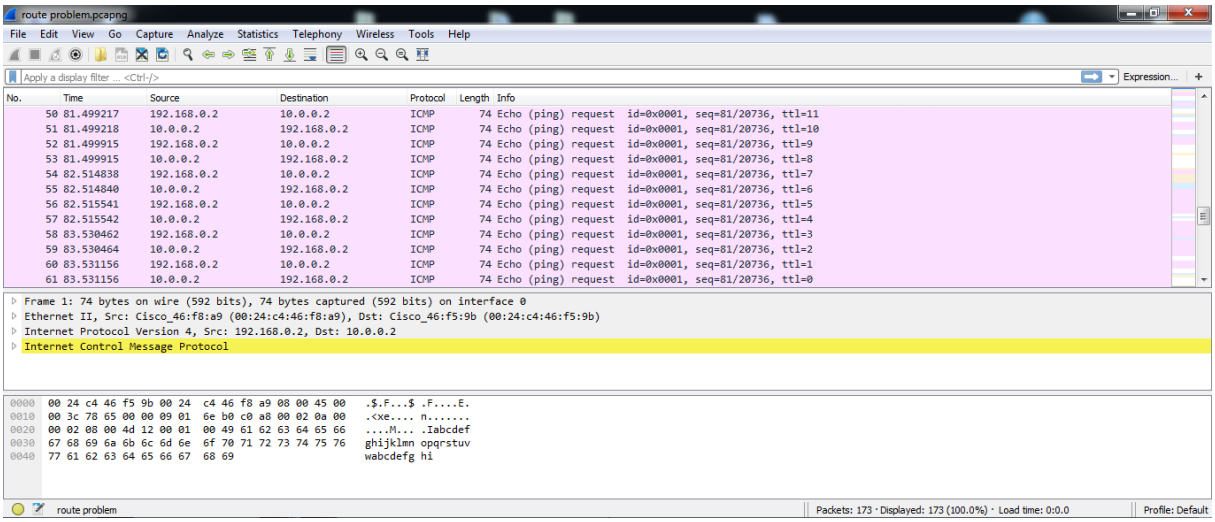


Obrázek 15 – Chybná adresa DNS serveru

6.2 Nefunkční komunikace kvůli chybě směrování

V konfiguraci směrování je díky možné rozsáhlosti sítě velmi snadné udělat chybu. Nalezení chyby proto může být celkem složitý proces.

V praktické ukázce se jedná o chybu nastavení směrování tak, že dva směrovače přeposílají pakety na ten druhý tak dlouho, dokud se paketu nesníží příznak TTL na 0. Poté se paket zahodí.



Obrázek 16 – Snižování hodnoty TTL

6.3 Duplikované IP adresy

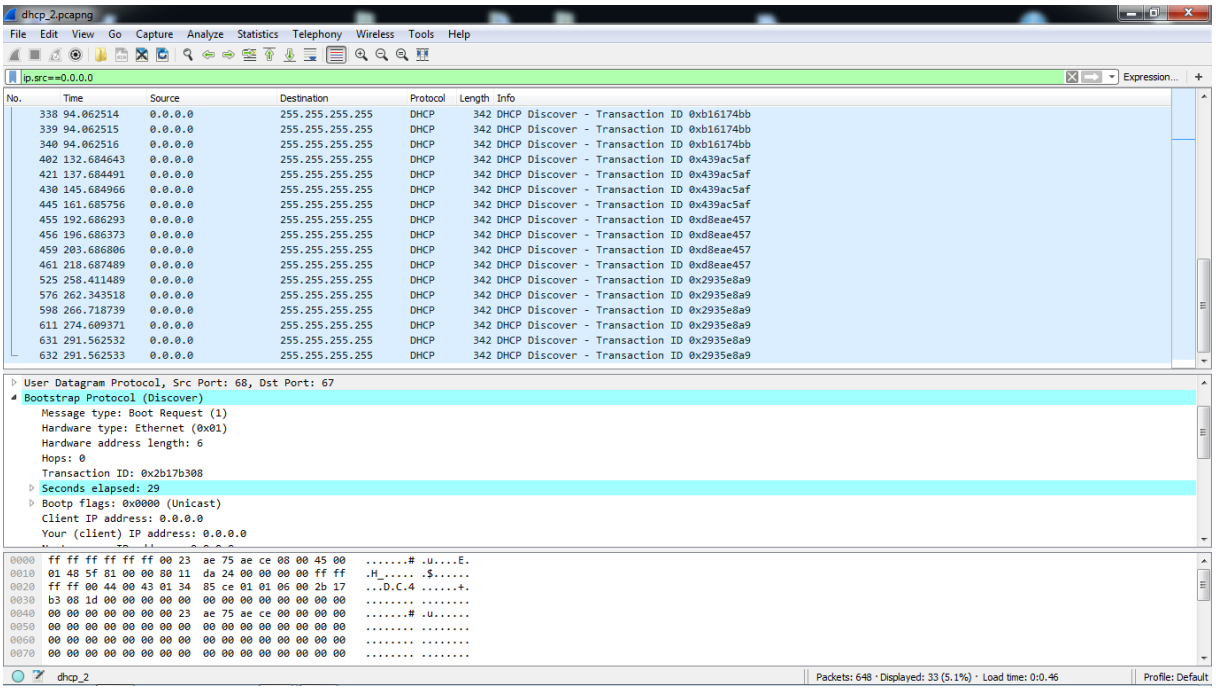
Existují dva druhy přidělování IP adres. Statické a dynamické. Statické přidělování znamená, že adresy zadává administrátor ručně podle předem daného plánu. Dynamické rozdělování řídí DHCP server, který dynamicky přiděluje adresy z definovaného rozsahu.

V ukázce (Příloha A) je zobrazeno dotazování na zařízení na určité adrese, jenže při ručním zadávání se dvěma zařízením přidělila stejná adresa. To vede k situaci, že směrovač neví, kam má paket poslat.

6.4 Nedostatek přidělovaných adres DHCP

Jak již bylo zmíněno, DHCP server přiděluje adresy z určitého rozsahu. Tento rozsah je dán možnostmi sítě a plánováním administrátora. Během rozšiřování sítě nebo v případě připojení více uživatelů v bezdrátové síti se stává, že nedostatek adres znemožní jejich přidělení.

Pomocí Wiresharku lze lehce zjistit tuto příčinu. Stačí si pomocí filtru zobrazit DHCP pakety a stejně jako v ukázce bude vidět množství nevyslyšených žádostí o přidělení adresy v krátkém časovém úseku.



Obrázek 17 – DHCP požadavky

6.5 Broadcast storm

V dnešní době je jedním z nejdůležitějších cílů návrhu sítě zajistit její spolehlivost a to i při výpadku některého jejího bodu. Nabízí se řešení pomocí zdvojení nebo jiné posílení těchto bodů. Tím ale vznikají smyčky, které způsobují nemalé problémy.

V případě zapojení více přepínačů do smyčky nastává tzv. broadcast storm. Při připojení zařízení se zjišťuje situace a rozložení sítě, zařízení vysílá ARP paket všem dostupným koncovým bodům. Přepínač paket přijme a rozešle ho všem ostatním, tedy i dalším přepínačům, které udělají to samé. Síť se tedy zahltí ARP pakety a vzniká tak broadcast storm. Situace se obvykle řeší STP protokolem, který podle svého algoritmu dočasně odpojí nepotřebné přepínače, jež připojí v případě výpadku běžících. Moderní hardware má navíc další ochranné funkce.

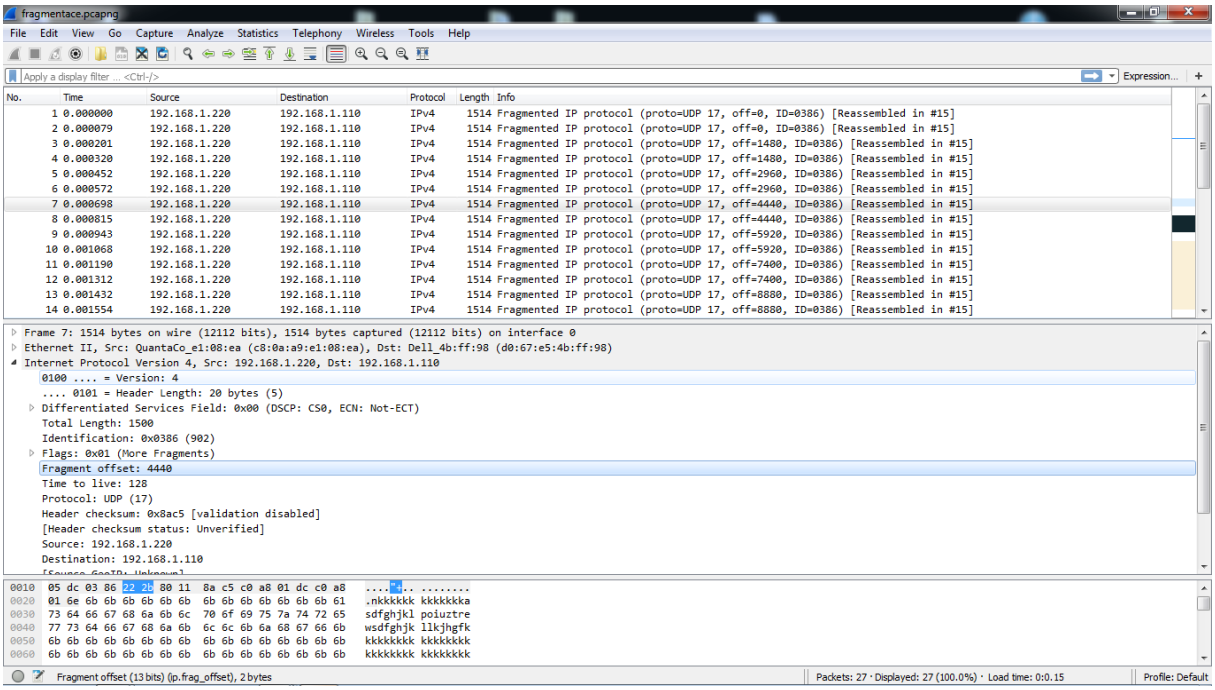
V praktickém příkladu byl na přepínačích zakázán STP protokol, aby se nasimuloval problém, ale zařízení mají své ochrany proti zahlcení pakety, takže místo broadcast stormu byly zachyceny běžné ARP pakety a pakety LOOP. Obrázek v Příloze B.

6.6 Ztráta fragmentů

Větší množství dat se při přenosu rozděluje na menší fragmenty, které se posílají jeden po druhém. V průběhu mohou nastat situace, že se data nepodaří v pořádku odeslat, resp.

přijmout, protože se některý z fragmentů po cestě ztratil. Pravděpodobně neprošel přes firewall.

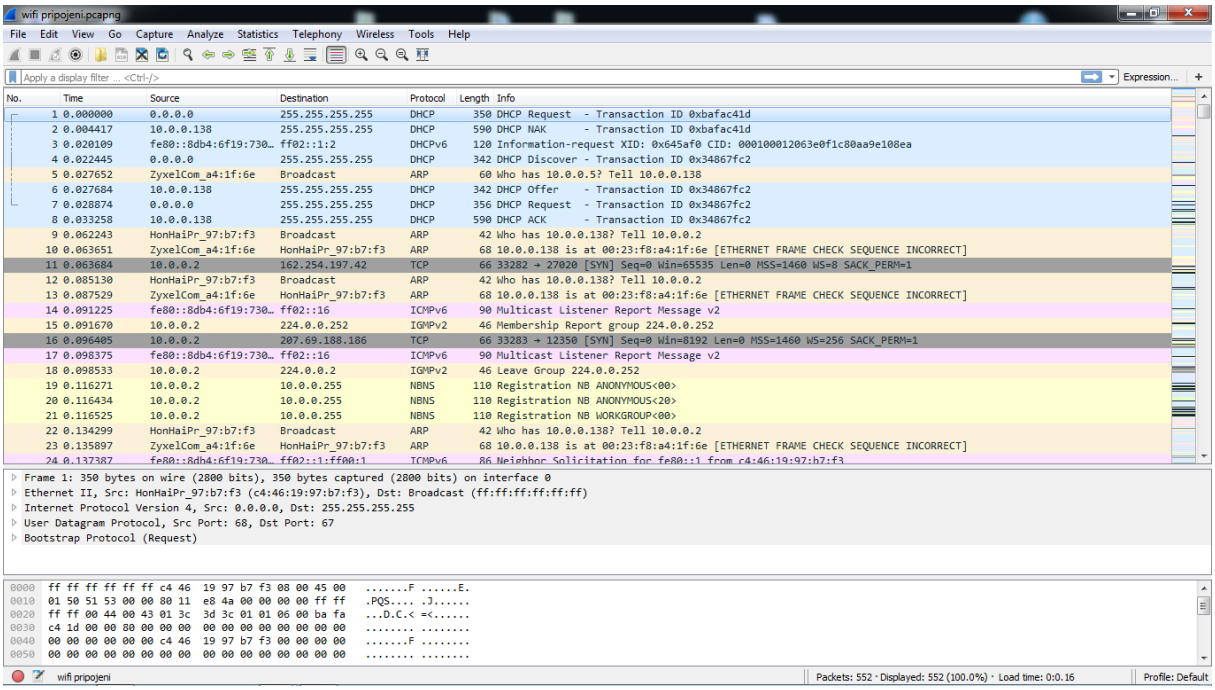
Pokud se dlouhodobě nedaří přijímat data, je dobré zkontrolovat komunikaci monitorovacím programem. Wireshark v ukázce ukazuje číslo fragmentu, a podle toho je možné zjistit, v jakém bodě sítě se pakety ztrácejí.



Obrázek 18 – Broadcast storm

6.7 Připojení k bezdrátové síti

Následující příklad ukazuje, co se děje po připojení k bezdrátové síti. Každá Wi-Fi síť vysílá na broadcast (všem dostupným) ARP pakety s informacemi o sobě, např. SSID (název sítě). Wireshark nevidí kontrolu správnosti údajů, ale ta proběhla úspěšně. Protože byly údaje správné, vysílač neignoruje DHCP požadavek a posílá na zařízení DHCP nabídku s IP adresou. Po nastavení adresy a připojení do sítě je nastaveno sdílení, atd.



Obrázek 19 – Přihlášení do bezdrátové sítě

6.8 Man-in-the-middle útok

Tento útok představuje připojení útočícího zařízení do sítě tak, aby odposlouchávalo veškerou komunikaci mezi vybranými uzlovými body. Útočník simuluje pro své oběti fyzickou MAC adresu toho druhého zařízení, takže si myslí, že mezi sebou bezpečně komunikují. Vhledem k tomu, že se dá lehce odposlechnout výměna šifrovacích klíčů, není problém tímto způsobem získat i šifrovaná data.

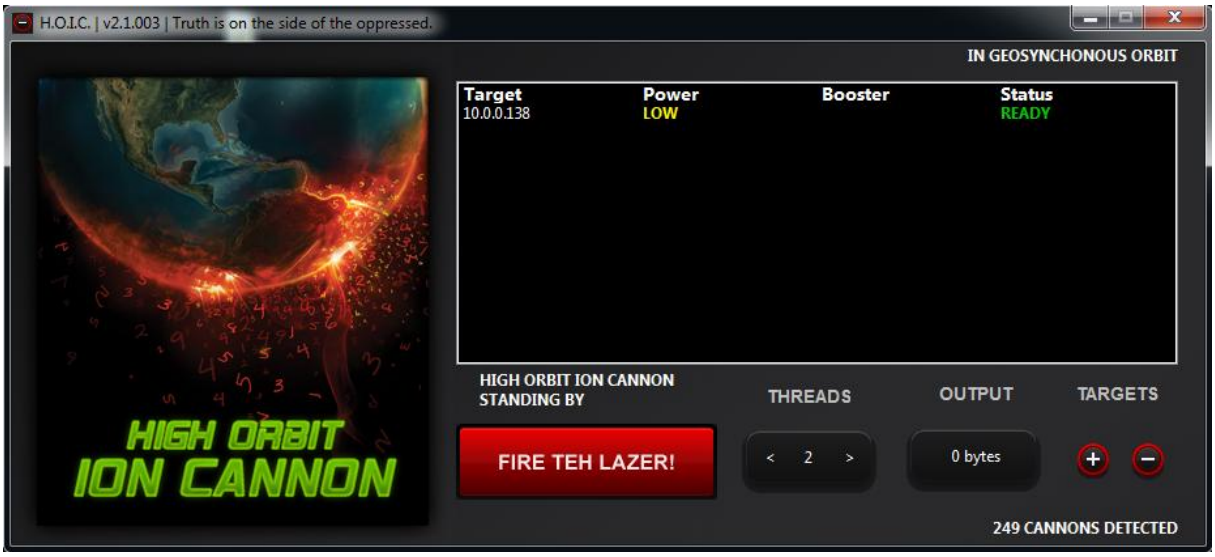
Pro simulaci byl použit program Ettercap, který je popsán výše. Průběh komunikace zachycené a filtrované Wiresharkem na útočícím zařízení je zobrazen spolu s ukázkou Ettercapu v Příloze C.

6.9 DoS útok

DoS útok, tedy odepření služby, spočívá v takovém množství požadavků proudících na server, že ten je nedokáže všechny obsloužit v reálném čase a začne se zpomalovat. To může vyústit v několik hodin až dní trvající nedostupnost serveru.

Útok se velmi lehce odhalí pomocí monitorovacího programu, kde je vidět množství požadavků (stejných nebo různých) přicházejících ze stejného zdroje během krátké doby.

DoS byl proveden pomocí programu H.O.I.C. v2.1.003 na router Zyxel P660HW-T3 a jeho výpis je v příloze D.

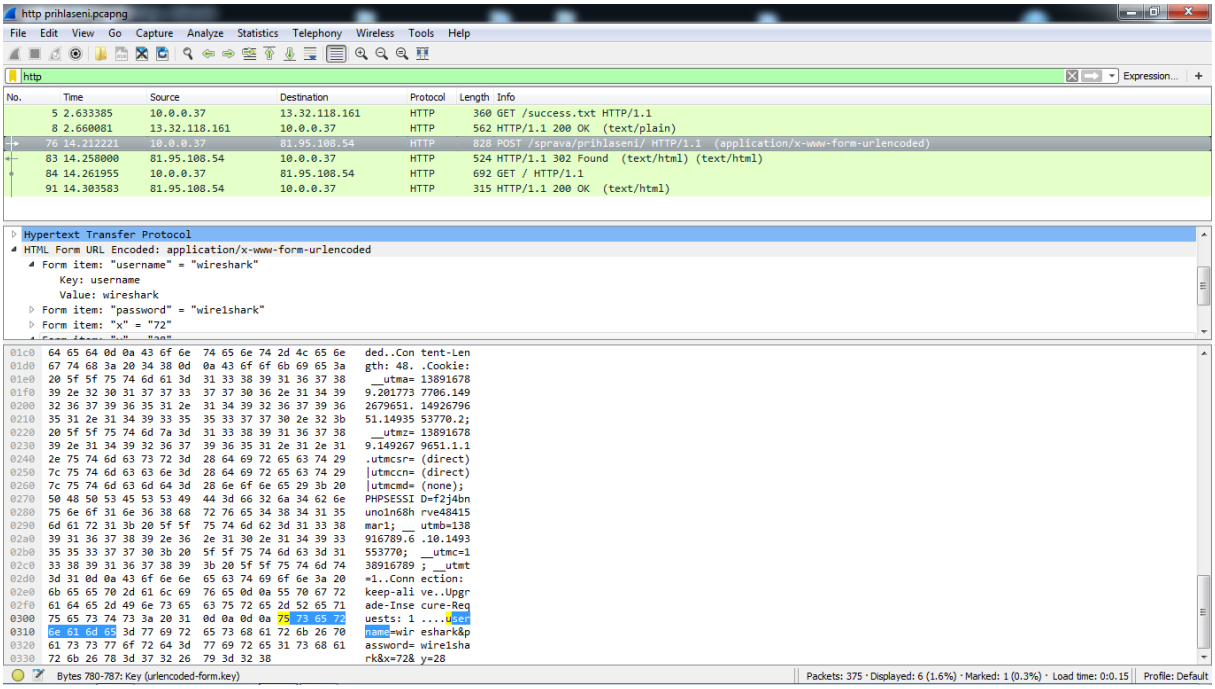


Obrázek 20 – H.O.I.C

6.10 Nalezení přihlašovacích údajů v HTTP paketu

K nalezení přihlašovacích údajů stačí jakýkoliv monitorovací nástroj snímající síť, přes kterou se oběť přihlašuje. HTTP pakety obsahují nezabezpečený obsah webových stránek.

Pro zjištění údajů si stačí pomocí filtru najít HTTP pakety a z jejich datové části se dají lehce přečíst. Ochranou proti tomuto útoku je zabezpečený šifrovaný HTTPS protokol.

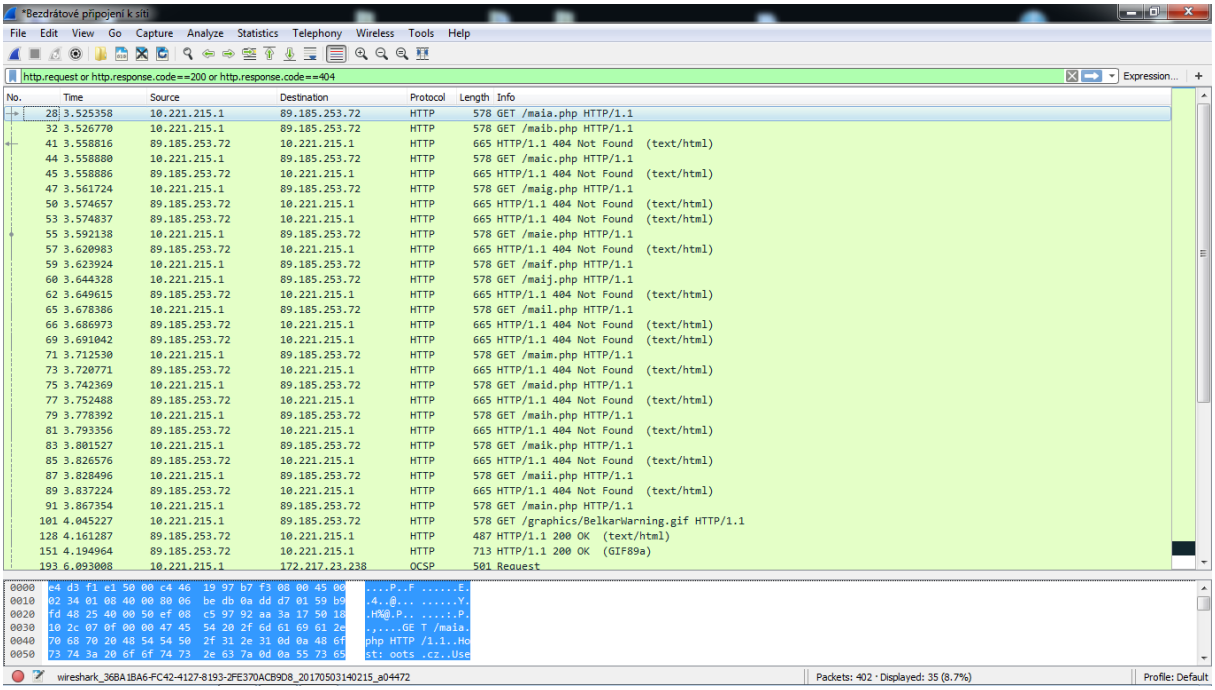


Obrázek 21 – Přihlášení přes HTTP protokol

6.11 Brute-force útok

Brute-force útok obecně znamená útok hrubou silou. Jeho využijí je mnohostranné. Vždy se jedná o větší množství pokusů s malými rozdíly s cílem zjistit, který dosáhne požadovaného výsledku. V informatice jde především o pokusy odhadnout přihlašovací heslo. Ve Wiresharku je tento útok zobrazován velkým počtem požadavků s negativní odpovědí, případně jednou pozitivní při úspěšném útoku.

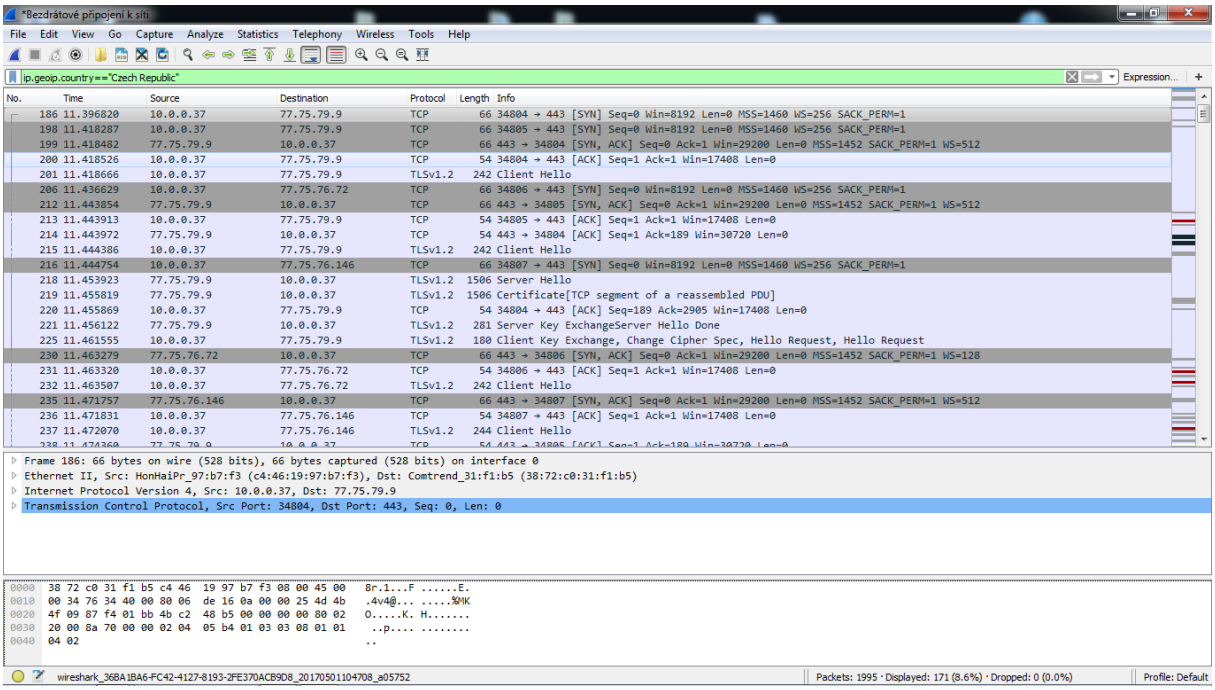
Při praktickém pokusu bylo cílem nalézt určitou stránku na webu (může to být soubor, na který není odkazováno, ale útočník ví, že tam je).



Obrázek 22 – Brute-force útok

6.12 Geolokace IP

Wireshark umožňuje vyčtení lokace z použité IP adresy. Aby bylo toto možné, musí instalace obsahovat rozšíření GeoIP a k Wiresharku musí být připojena databáze. Databází existuje více, některé placené, jiné zdarma. V ukázce jsou použity databáze z adresy http://geolite.maxmind.com/download/geoip/database/. Díky GeoIP lze poté například filtrovat komunikaci se zařízeními v určitém státu.



Obrázek 23 – GeoIP

7 ZÁVĚR

Cílem práce byl úvod do monitorování sítě pomocí programu Wireshark. Na začátku byl proto popsán ISO/OSI model sítě pro lepší představu fungování síťové komunikace. Ve třetí kapitole byly sepsány technické informace o protokolech z praktické části.

Jelikož je tématem práce monitorování a analýza, čtvrtá kapitola se zabývala bezpečností sítí a popisovala nástroje využívané v této oblasti. Poté již následovala kapitola Wireshark, která představuje manuál k tomuto programu. Po teoretické části byla sepsána praktická část s konkrétními praktickými příklady.

Z bakalářské práce je jasně vidět, že Wireshark je velmi mocný nástroj s obrovskými možnostmi. Je jedním z nejúčinnějších nástrojů využívaných pro monitorování sítí. To je vhodné provádět nejen při realizaci sítě, ale i v průběhu při běžných kontrolách a samozřejmě při případném problému.

Nejtěžším úkolem během praktické části bylo nasimulovat problém. Většina moderních zařízení má ochranné prvky zabraňující situacím, které jsou pro potřeby ukázky použity, přesto, jak je vidět, je možné je v praxi nedopatřením způsobit. Potom přichází čas na monitorovací nástroj.

Díky této práci jsem měl skvělou příležitost si program vyzkoušet a to především při řešení praktických situací. S jistotou budu Wireshark v budoucnu využívat a nadále prohlubovat získané zkušenosti při práci s ním.

8 POUŽITÁ LITERATURA

SANDERS, Chris. *Practical packet analysis: using wireshark to solve real-world network problems*. 2nd ed. San Francisco: No starch press, c2011. ISBN 1-59327-266-9.

BOUŠKA, Petr, 5. 3. 2007. *OSI model* [online]. 2007 [cit. 2017-05-03]. Dostupné z: http://www.samuraj-cz.com/clanek/osi-model/

Wireshark · Go Deep [online]. 2017 [cit. 2017-05-03]. Dostupné z: https://www.wireshark.org/

Wikipedie: Otevřená encyklopedie: Wireshark [online]. c2017 [cit. 2017-05-03]. Dostupné z: https://cs.wikipedia.org/wiki/Wireshark

AlternativeTo.net. *Wireshark Alternatives and Similar Software* [online]. 2017 [cit. 2017-05-03]. Dostupné z: http://alternativeto.net/software/wireshark/

LAMPING, Ulf, Richard SHARPE, Ed WARNICKE. *Wireshark User's Guide: For Wireshark 2.1* [online]. 2014 [cit. 2017-05-03]. Dostupné z: https://www.wireshark.org/docs/wsug_html_chunked/

IETF tools. *IETF Documents* [online]. 2017 [cit. 2017-05-03]. Dostupné z: https://tools.ietf.org/html/

IANA Internet Assigned Numbers Authority. *IANA – Protocol Registries* [online]. 2017 [cit. 2017-05-03]. Dostupné z: https://www.iana.org/protocols

BIGELOW, Stephen J. *Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů*. Brno: Computer Press, 2004. ISBN 80-251-0178-9.

Wikipedie: Otevřená encyklopedie: Tcpdump [online]. c2016 [cit. 2017-05-03]. Dostupné z: https://cs.wikipedia.org/wiki/Tcpdump

GIACOBBI, Giovanni. *The GNU Netcat – Official homepage* [online]. 2006 [cit. 2017-05-03]. Dostupné z: http://netcat.sourceforge.net/

Wikipedia, The Free Encyclopedia: ARP spoofing [online]. 2017 [cit. 2017-05-03]. Dostupné z: https://en.wikipedia.org/wiki/ARP_spoofing

LYON, Gordon. *Nmap: the Network Mapper – Free Security Scanner* [online]. 2017 [cit. 2017-05-03]. Dostupné z: https://nmap.org/

ORZACH, Yoram. *Network Analysis using Wireshark Cookbook: over 80 recipes to analyze and troubleshoot network problems using Wireshark*. Birmingham [u.a.]: Packt Publishing, 2013. ISBN 9781849517645.

CZ.NIC, z. s. p. o. *Web o DNS* [online]. 2015 [cit. 2017-05-03]. Dostupné z: https://www.nic.cz/page/2885/web-o-dns/

9 PŘÍLOHY

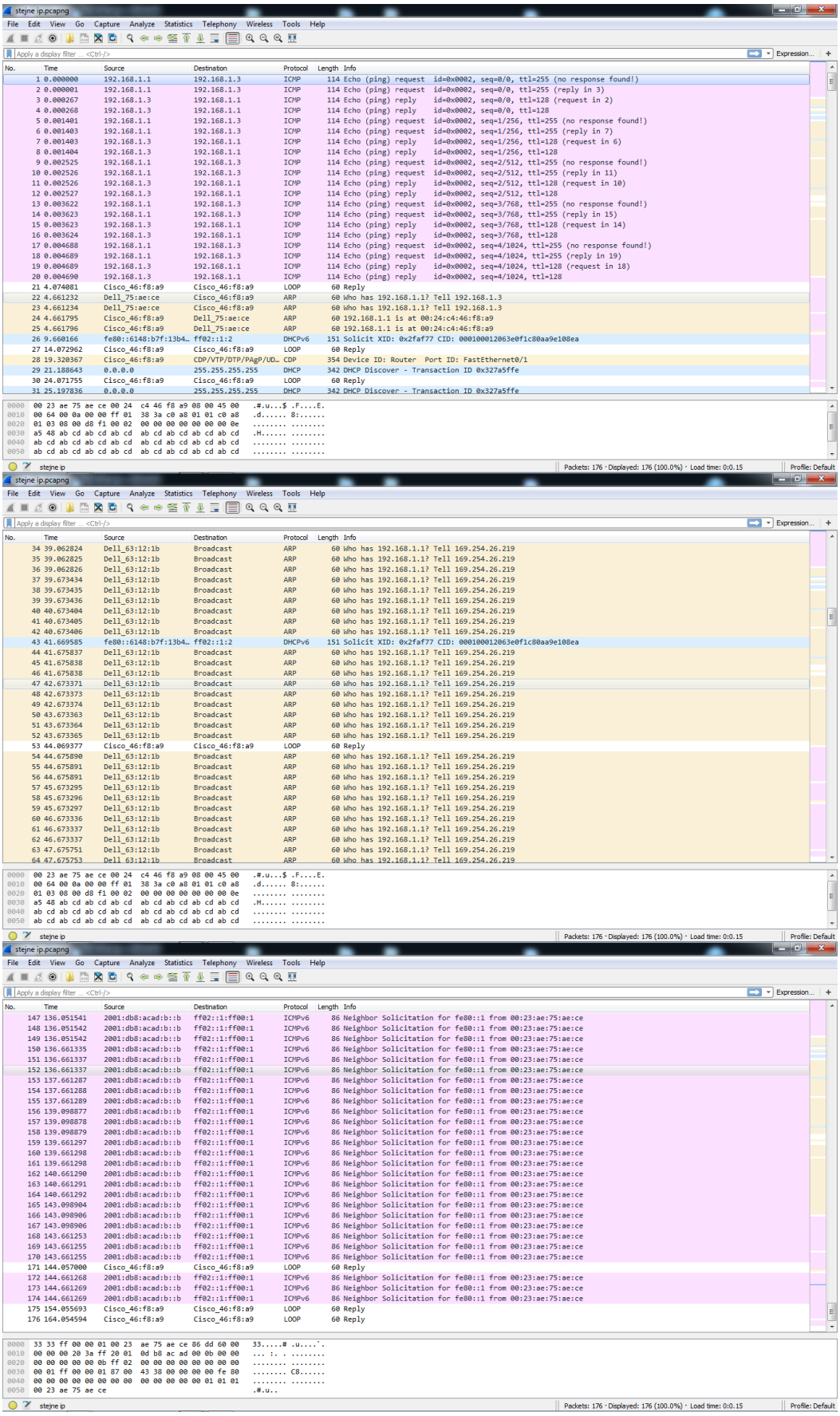
Příloha A – *Ukázka výpisu programu při zapojení zařízení se stejnými IP adresami*.....44

Příloha B – *Pakety ARP a LOOP při broadcast stormu*.....45

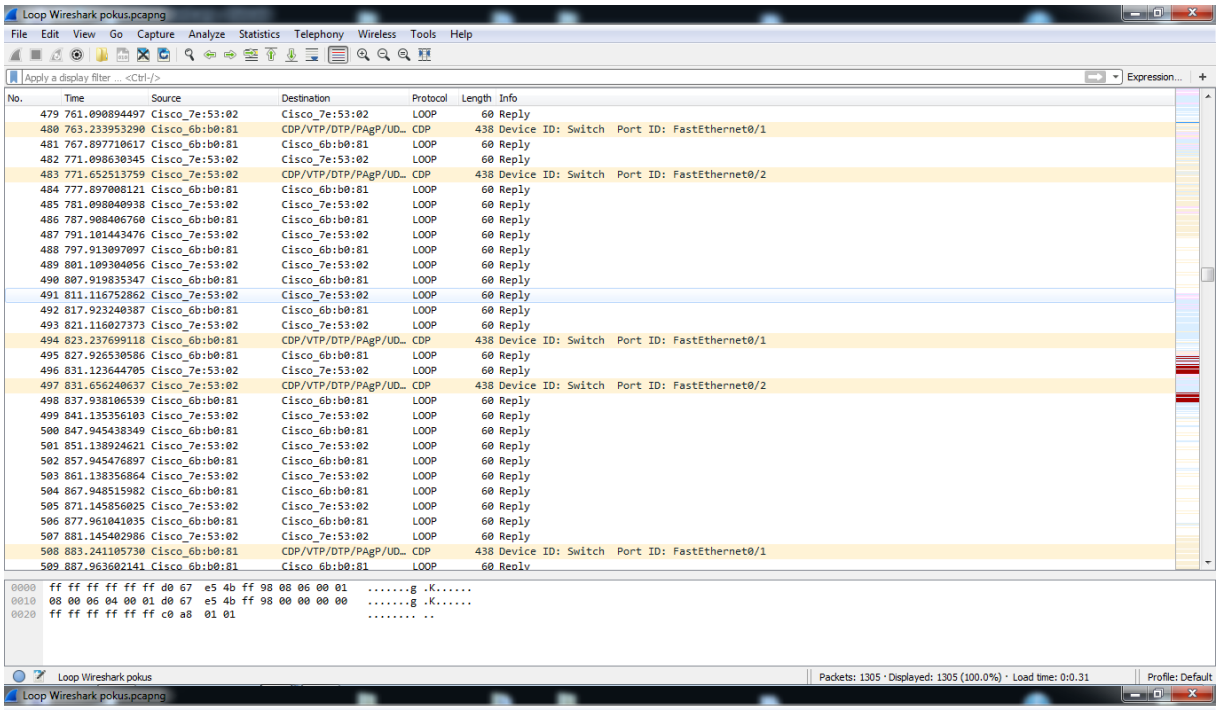
Příloha C – *Man-in-the-middle útok*.....46

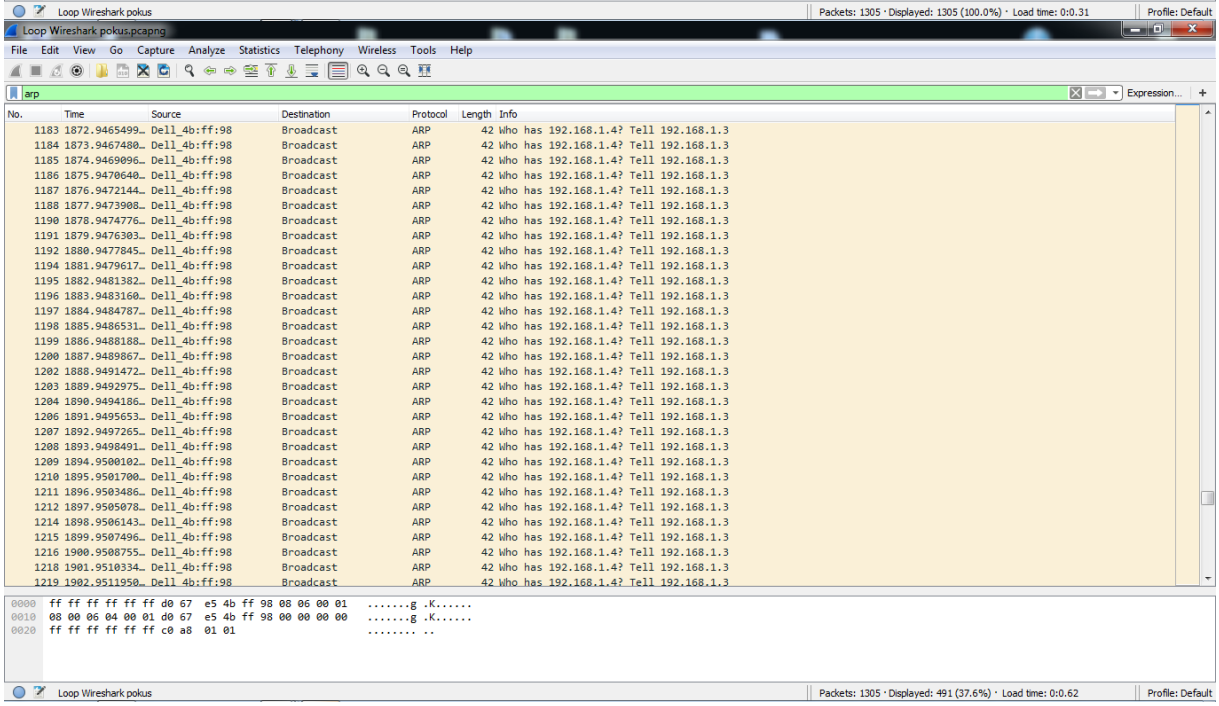
Příloha D – *Výpis programu při DDoS útoku*.....47

Příloha A – *Ukázka výpisu programu při zapojení zařízení se stejnými IP adresami*

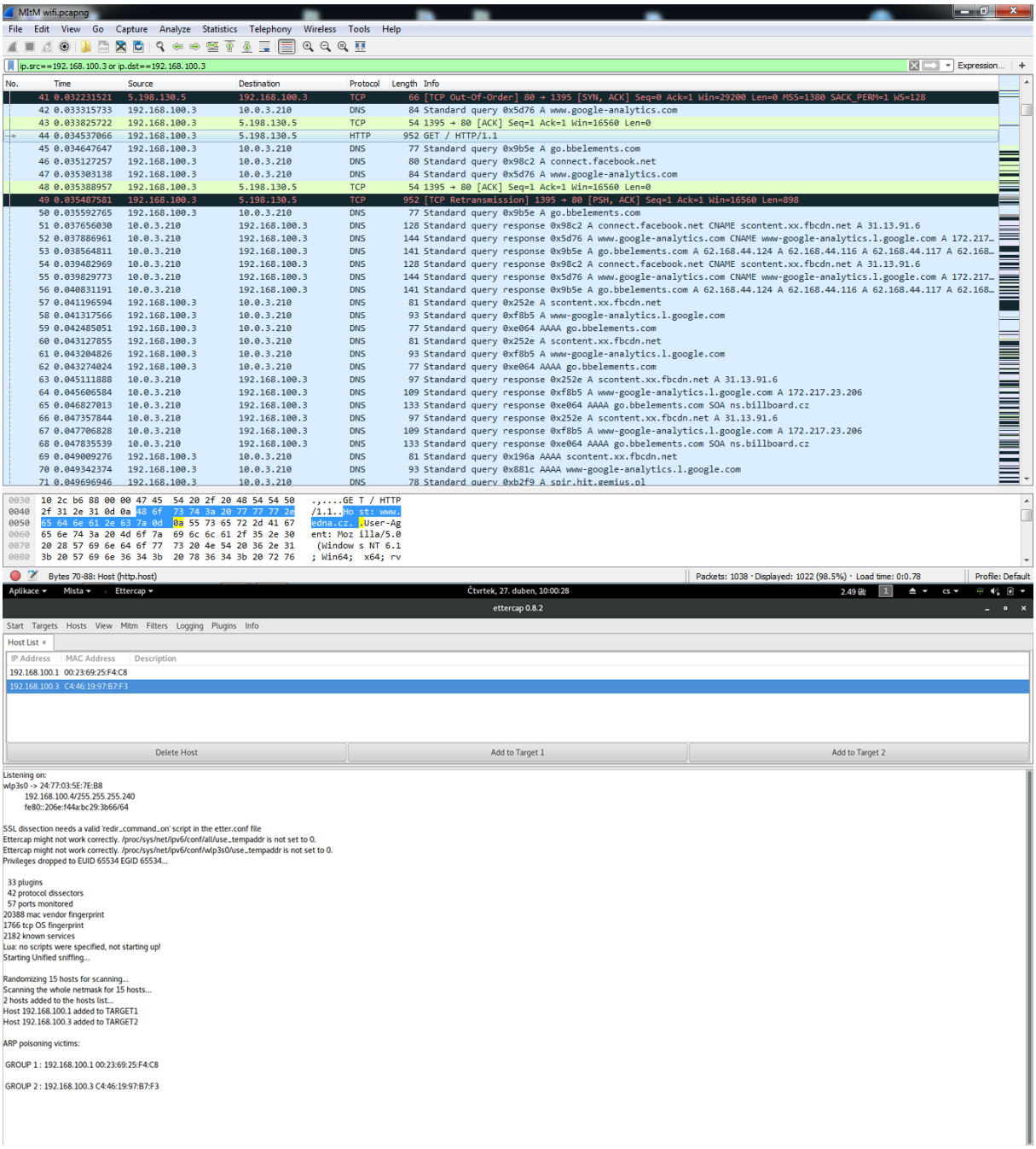


Příloha B – *Pakety ARP a LOOP při broadcast stormu*





Příloha C – *Man-in-the-middle útok*



Příloha D – *Výpis programu při DDoS útoku*

hoic od 26.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
26	*REF*	10.0.0.138	10.0.0.1	TCP	60	80 → 33931 [ACK] Seq=1 Ack=71 Win=21690 Len=0
27	0.001144	10.0.0.138	10.0.0.1	TCP	60	80 → 33930 [ACK] Seq=1 Ack=71 Win=21690 Len=0
28	0.008350	10.0.0.138	10.0.0.1	TCP	271	[TCP segment of a reassembled PDU]
29	0.010709	10.0.0.138	10.0.0.1	TCP	271	[TCP segment of a reassembled PDU]
30	0.075671	10.0.0.138	10.0.0.1	TCP	1514	[TCP segment of a reassembled PDU]
31	0.075717	10.0.0.1	10.0.0.138	TCP	54	33930 → 80 [ACK] Seq=71 Ack=1678 Win=65535 Len=0
32	0.077670	10.0.0.138	10.0.0.1	TCP	1494	[TCP segment of a reassembled PDU]
33	0.079474	10.0.0.138	10.0.0.1	TCP	1514	[TCP segment of a reassembled PDU]
34	0.079503	10.0.0.1	10.0.0.138	TCP	54	33931 → 80 [ACK] Seq=71 Ack=1678 Win=65535 Len=0
35	0.081682	10.0.0.138	10.0.0.1	TCP	1494	[TCP segment of a reassembled PDU]
36	0.087701	10.0.0.138	10.0.0.1	TCP	1514	[TCP segment of a reassembled PDU]
37	0.087726	10.0.0.1	10.0.0.138	TCP	54	33930 → 80 [ACK] Seq=71 Ack=4578 Win=65535 Len=0
38	0.089707	10.0.0.138	10.0.0.1	TCP	1494	[TCP segment of a reassembled PDU]
39	0.091377	10.0.0.138	10.0.0.1	TCP	1514	[TCP segment of a reassembled PDU]
40	0.091397	10.0.0.1	10.0.0.138	TCP	54	33931 → 80 [ACK] Seq=71 Ack=4578 Win=65535 Len=0
41	0.093631	10.0.0.138	10.0.0.1	TCP	1494	[TCP segment of a reassembled PDU]
42	0.099834	10.0.0.138	10.0.0.1	TCP	1514	[TCP segment of a reassembled PDU]
43	0.099864	10.0.0.1	10.0.0.138	TCP	54	33930 → 80 [ACK] Seq=71 Ack=7478 Win=65535 Len=0
44	0.101826	10.0.0.138	10.0.0.1	TCP	1494	[TCP segment of a reassembled PDU]
45	0.103818	10.0.0.138	10.0.0.1	TCP	1514	[TCP segment of a reassembled PDU]
46	0.103839	10.0.0.1	10.0.0.138	TCP	54	33931 → 80 [ACK] Seq=71 Ack=7478 Win=65535 Len=0
47	0.105850	10.0.0.138	10.0.0.1	TCP	1494	[TCP segment of a reassembled PDU]
48	0.112077	10.0.0.138	10.0.0.1	TCP	1514	[TCP segment of a reassembled PDU]
49	0.112129	10.0.0.1	10.0.0.138	TCP	54	33930 → 80 [ACK] Seq=71 Ack=10378 Win=65535 Len=0
50	0.113814	10.0.0.138	10.0.0.1	TCP	213	[TCP segment of a reassembled PDU]
51	0.115688	10.0.0.138	10.0.0.1	TCP	1514	[TCP segment of a reassembled PDU]
52	0.115708	10.0.0.1	10.0.0.138	TCP	54	33931 → 80 [ACK] Seq=71 Ack=10378 Win=65535 Len=0
53	0.117338	10.0.0.138	10.0.0.1	TCP	213	[TCP segment of a reassembled PDU]
54	0.122382	10.0.0.138	10.0.0.1	HTTP	60	HTTP/1.1 200 OK (text/html)
55	0.122408	10.0.0.1	10.0.0.138	TCP	54	33930 → 80 [ACK] Seq=71 Ack=10538 Win=65535 Len=0
56	0.124217	10.0.0.138	10.0.0.1	HTTP	60	HTTP/1.1 200 OK (text/html)

```
0000  c8 0a a9 e1 08 ea 00 23  f8 a4 1f 6e 08 00 45 00   .......# ...n..E.
0010  00 28 04 f0 00 00 fe 06  a3 55 0a 00 00 8a 0a 00   .(...... .U......
0020  00 01 00 50 84 8b 5d ce  a0 01 73 8f 45 09 50 10   ...P..]. ..s.E.P.
0030  54 ba 0b 4c 00 00 00 00  00 00 00 00               T..L.... ....
```

hoic od 26 | Packets: 1695 · Displayed: 1695 (100.0%) · Marked: 1 (0.1%) · Load time: 0:0.307 | Profile: Default

hoic od 26.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
1591	14.559190	10.0.0.138	10.0.0.1	TCP	271	[TCP segment of a reassembled PDU]
1592	14.561297	10.0.0.138	10.0.0.1	TCP	271	[TCP segment of a reassembled PDU]
1593	14.638466	10.0.0.138	10.0.0.1	TCP	1514	[TCP segment of a reassembled PDU]
1594	14.638512	10.0.0.1	10.0.0.138	TCP	54	34003 → 80 [ACK] Seq=71 Ack=1678 Win=65535 Len=0
1595	14.640281	10.0.0.138	10.0.0.1	TCP	1494	[TCP segment of a reassembled PDU]
1596	14.641932	10.0.0.138	10.0.0.1	TCP	1514	[TCP segment of a reassembled PDU]
1597	14.641954	10.0.0.1	10.0.0.138	TCP	54	34004 → 80 [ACK] Seq=71 Ack=1678 Win=65535 Len=0
1598	14.644035	10.0.0.138	10.0.0.1	TCP	1494	[TCP segment of a reassembled PDU]
1599	14.649035	10.0.0.138	10.0.0.1	TCP	1514	[TCP segment of a reassembled PDU]
1600	14.649058	10.0.0.1	10.0.0.138	TCP	54	34003 → 80 [ACK] Seq=71 Ack=4578 Win=65535 Len=0
1601	14.650823	10.0.0.138	10.0.0.1	TCP	1494	[TCP segment of a reassembled PDU]
1602	14.652245	10.0.0.138	10.0.0.1	TCP	1514	[TCP segment of a reassembled PDU]
1603	14.652266	10.0.0.1	10.0.0.138	TCP	54	34004 → 80 [ACK] Seq=71 Ack=4578 Win=65535 Len=0
1604	14.654121	10.0.0.138	10.0.0.1	TCP	1494	[TCP segment of a reassembled PDU]
1605	14.659400	10.0.0.138	10.0.0.1	TCP	1514	[TCP segment of a reassembled PDU]
1606	14.659426	10.0.0.1	10.0.0.138	TCP	54	34003 → 80 [ACK] Seq=71 Ack=7478 Win=65535 Len=0
1607	14.661273	10.0.0.138	10.0.0.1	TCP	1494	[TCP segment of a reassembled PDU]
1608	14.662662	10.0.0.138	10.0.0.1	TCP	1514	[TCP segment of a reassembled PDU]
1609	14.662716	10.0.0.1	10.0.0.138	TCP	54	34004 → 80 [ACK] Seq=71 Ack=7478 Win=65535 Len=0
1610	14.664492	10.0.0.138	10.0.0.1	TCP	1494	[TCP segment of a reassembled PDU]
1611	14.670168	10.0.0.138	10.0.0.1	TCP	1514	[TCP segment of a reassembled PDU]
1612	14.670196	10.0.0.1	10.0.0.138	TCP	54	34003 → 80 [ACK] Seq=71 Ack=10378 Win=65535 Len=0
1613	14.671673	10.0.0.138	10.0.0.1	TCP	213	[TCP segment of a reassembled PDU]
1614	14.673345	10.0.0.138	10.0.0.1	TCP	1514	[TCP segment of a reassembled PDU]
1615	14.673371	10.0.0.1	10.0.0.138	TCP	54	34004 → 80 [ACK] Seq=71 Ack=10378 Win=65535 Len=0
1616	14.674891	10.0.0.138	10.0.0.1	TCP	213	[TCP segment of a reassembled PDU]
1617	14.679213	10.0.0.138	10.0.0.1	HTTP	60	HTTP/1.1 200 OK (text/html)
1618	14.679234	10.0.0.1	10.0.0.138	TCP	54	34003 → 80 [ACK] Seq=71 Ack=10538 Win=65535 Len=0
1619	14.679881	10.0.0.1	10.0.0.138	TCP	54	34003 → 80 [FIN, ACK] Seq=71 Ack=10538 Win=65535 Len=0
1620	14.681215	10.0.0.138	10.0.0.1	TCP	60	80 → 34003 [ACK] Seq=10538 Ack=72 Win=21760 Len=0
1621	14.682068	10.0.0.138	10.0.0.1	HTTP	60	HTTP/1.1 200 OK (text/html)

```
0000  c8 0a a9 e1 08 ea 00 23  f8 a4 1f 6e 08 00 45 00   .......# ...n..E.
0010  00 28 04 f0 00 00 fe 06  a3 55 0a 00 00 8a 0a 00   .(...... .U......
0020  00 01 00 50 84 8b 5d ce  a0 01 73 8f 45 09 50 10   ...P..]. ..s.E.P.
0030  54 ba 0b 4c 00 00 00 00  00 00 00 00               T..L.... ....
```

hoic od 26 | Packets: 1695 · Displayed: 1695 (100.0%) · Marked: 1 (0.1%) · Load time: 0:0.307 | Profile: Default