Šablona pro odevzdávání výstupů z distančních cvičení předmětu BPC-KOM určená k editaci a odevzdání pro vytvoření PDF verze

Vaše jméno	Daniel Prachař
VUT ID	240969
Vypracovaný lab (označení)	Streda14.pcapng

Obsah

Aplikační vrstva - protokoly

Domain Name System (DNS)

- Jeho hlavním úkolem je převod IP adres v číslicové podobě na doménové jména, kterým člověk lépe rozumí
- Například z IP adresy 77.75.74.17, DNS převede na seznam.cz

Session Initiation Protocol (SIP)

- Slouží k inicializaci relací, signální protokol telefonie IP, používá se pro zahájení/modifikaci/ukončení telefonických hovorů

Session Description Protocol (SDP)

- Popisuje vlastnosti relací přenosu dat
- Používá se v kombinaci s SIP
- Nepřenáší data

Hypertext Transfer Protocol (HTTP)

- Jeho hlavní úkol je komunikace s www servery
- Přenáší hypertextové dokumenty HTML a další soubory

Real Time Protocol (RTP)

- Standardizovaný, přenáší audio a video data po internetu
- Využívá port

Real Time Control Protocol (RTCP)

- Doplňuje RTP protokol
- Poskytuje řídící informace RTP relace

Daniel Prachař
240969

Session Traversal Utilities for NAT (STUN)

- Sada pomocných internetových standardů, komunikují skrz NAT
- Typické využití u služeb typu VOIP

Transportní vrstva - protokoly

User Datagram Protocol(UDP)

- Internetový protokol odesílá pakety, pakety odesílá pomocí IP adresy
- Protokol nečeká, až se ujistí, že příjemce obdržel paket, odesílá pakety dál, a když nějaký paket nedojde, tak jej znovu nepošle. Díky odstranění těchto kontrol je protokol velmi rychlý
- Používá se pro přenos videa, zvuku, živého vysílání, online her
- Záhlaví minimálně 8b

Transmission Control Protocol(TCP)

- Nejpoužívanější internetový protokol
- Zařízení odešle pakety TCP na adresu serveru, ten zpřístupní danou webovou stránku, odešle TCP pakety a pomocí internetového prohlížeče se stránka zobrazí
- TCP protokol na rozdíl od UDP kontroluje, zda pakety dorazily do cíle tzn. Že se neztratily a nedošlo k poškození dat.
- TCP čísluje pakety a kontroluje, zda dorazili k příjemci, pokud ne pošle je znovu

Síťová vrstva – protokoly

Internet Control Message Protocol(ICMP)

- Používá se pro přenos chybových a řídících zpráv mezi uzly a směrovači sítě například: služba není dostupná
- Je vygenerován na základě nějaké události/příkazu

Daniel Prachař
240969

- Využívají jej příkazy traceroute, ping

Internet protocoll(IP)

- Hlavní protokol internetu, rozlišuje pomocí IP adresy dané síťové rozhraní
- Směruje datagramy ze zdrojového zařízení do cílového hostitele přes jednotlivé IP sítě. Data posílá po blocích, co nejblíže k jejich cíli, neručí za doručení dat
- Jeho součástí jsou protokoly IPV4 a IPV6

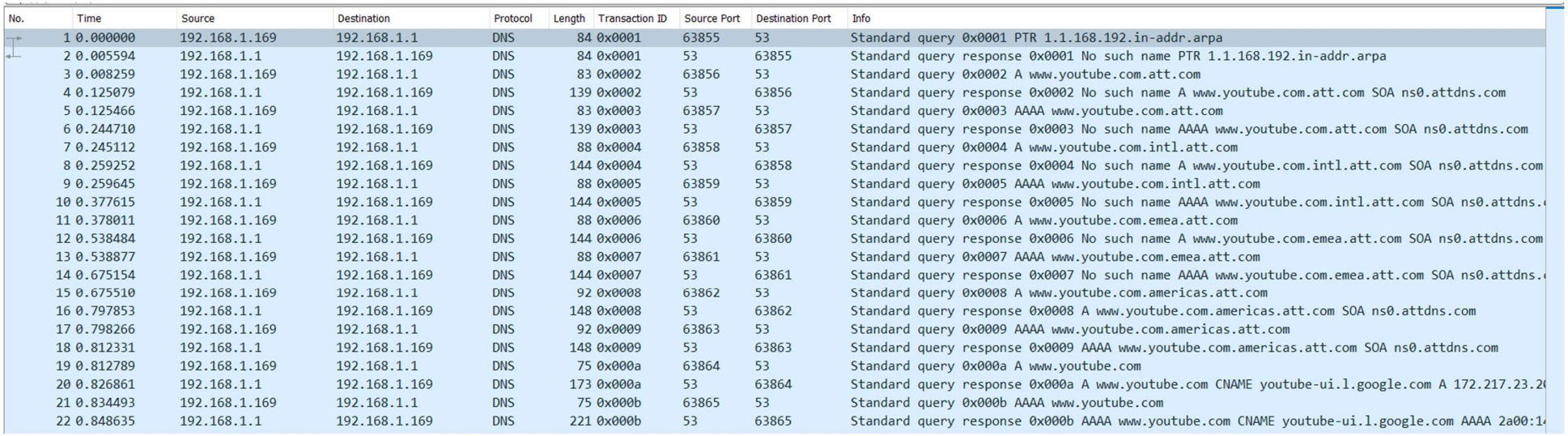
IPV4

- Základ pro komunikaci v internetu, datově orientovaný,
- Využívá IP adresy zapsané dekadicky po jednotlivých oktetech(192.168.1.1), má omezený adresní prostor 2^32
- Jednotlivé data posílá po částech(paketech/ethernetových rámcích), neručí za spolehlivost, doručení dat, pořadí
- Datagramy nesou pouze informace a služební údaje

IPV6

- Nahrazuje IPV4, má větší adresní prostor 2^128, zdokonalení přenosu dat
- IP adresa je zde v hexadecimálním formátu (2001:db8:0:1234:0:567:8:1)

Analýza síťového provozu DNS



No.	Time	Source	Destination	Protocol	Length	Transaction ID	Source Port	Destination Port	Info
1	0.000000	192.168.1.169	192.168.1.1	DNS	84	0x0001	63855	53	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
2	0.005594	192.168.1.1	192.168.1.169	DNS	84	0x0001	53	63855	Standard query response 0x0001 No such name PTR 1.1.168.192.in-addr.arpa
3	0.008259	192.168.1.169	192.168.1.1	DNS	83	0x0002	63856	53	Standard query 0x0002 A www.youtube.com.att.com
4	0.125079	192.168.1.1	192.168.1.169	DNS	139	0x0002	53	63856	Standard query response 0x0002 No such name A www.youtube.com.att.com SOA ns0.attdns.com
5	0.125466	192.168.1.169	192.168.1.1	DNS	83	0x0003	63857	53	Standard query 0x0003 AAAA www.youtube.com.att.com
6	0.244710	192.168.1.1	192.168.1.169	DNS	139	0x0003	53	63857	Standard query response 0x0003 No such name AAAA www.youtube.com.att.com SOA ns0.attdns.com
7	0.245112	192.168.1.169	192.168.1.1	DNS	88	0x0004	63858	53	Standard query 0x0004 A www.youtube.com.intl.att.com
8	0.259252	192.168.1.1	192.168.1.169	DNS	144	0x0004	53	63858	Standard query response 0x0004 No such name A www.youtube.com.intl.att.com SOA ns0.attdns.com
9	0.259645	192.168.1.169	192.168.1.1	DNS	88	0x0005	63859	53	Standard query 0x0005 AAAA www.youtube.com.intl.att.com
10	0.377615	192.168.1.1	192.168.1.169	DNS	144	0x0005	53	63859	Standard query response 0x0005 No such name AAAA www.youtube.com.intl.att.com SOA ns0.attdns.(
11	0.378011	192.168.1.169	192.168.1.1	DNS	88	0x0006	63860	53	Standard query 0x0006 A www.youtube.com.emea.att.com
12	0.538484	192.168.1.1	192.168.1.169	DNS	144	0x0006	53	63860	Standard query response 0x0006 No such name A www.youtube.com.emea.att.com SOA ns0.attdns.com
13	0.538877	192.168.1.169	192.168.1.1	DNS	88	0x0007	63861	53	Standard query 0x0007 AAAA www.youtube.com.emea.att.com
14	0.675154	192.168.1.1	192.168.1.169	DNS	144	0x0007	53	63861	Standard query response 0x0007 No such name AAAA www.youtube.com.emea.att.com SOA ns0.attdns.(
15	0.675510	192.168.1.169	192.168.1.1	DNS	92	0x0008	63862	53	Standard query 0x0008 A www.youtube.com.americas.att.com
16	0.797853	192.168.1.1	192.168.1.169	DNS	148	0x0008	53	63862	Standard query response 0x0008 A www.youtube.com.americas.att.com SOA ns0.attdns.com
17	0.798266	192.168.1.169	192.168.1.1	DNS	92	0x0009	63863	53	Standard query 0x0009 AAAA www.youtube.com.americas.att.com
18	0.812331	192.168.1.1	192.168.1.169	DNS	148	0x0009	53	63863	Standard query response 0x0009 AAAA www.youtube.com.americas.att.com SOA ns0.attdns.com
19	0.812789	192.168.1.169	192.168.1.1	DNS	75	0x000a	63864	53	Standard query 0x000a A www.youtube.com
20	0.826861	192.168.1.1	192.168.1.169	DNS	173	0x000a	53	63864	Standard query response 0x000a A www.youtube.com CNAME youtube-ui.l.google.com A 172.217.23.2(
21	0.834493	192.168.1.169	192.168.1.1	DNS	75	0x000b	63865	53	Standard query 0x000b AAAA www.youtube.com
22	0.848635	192.168.1.1	192.168.1.169	DNS	221	0x000b	53	63865	Standard query response 0x000b AAAA www.youtube.com CNAME youtube-ui.l.google.com AAAA 2a00:1(

Aplikační protokol: DNS

Transportní protokol: UDP

Síťový protokol: IPV4

Porty: Připojujeme se pomocí UDP protokolu z portů 63855-63865(port se s každým odeslaným dotazem změní) na DNS server, který běží na portu 53

IP adresy: Dotazujeme se z adresy 192.168.1.169 na DNS server s IP adresou 1.1.192.168.

Průběh komunikace:

No. 1-2 Dotazujeme se z adresy 192.168.1.169 na DNS server s IP adresou 1.1.192.168 nejdříve se dotaz odešle na Pointer(PTR), který se používá pro zpětné vyhledání DNS a překladu IP adresy na doménu.

No. 3-14 Následně se dotazujeme na stránka www.youtube.com pomocí DNS serveru, ale můžeme vidět že dotaz byl špatně zadán a DNS hlásí chybu

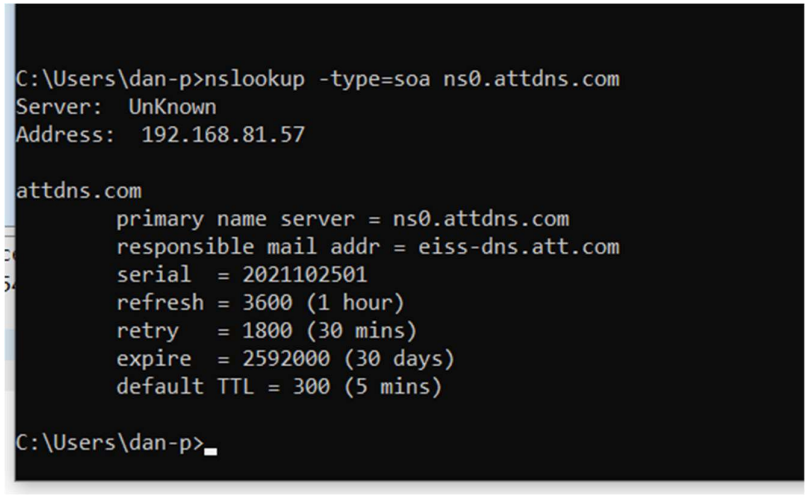
No. 15-23 Zde se už dotaz povedl whireshark vypsal veškeré záznamy(A,AAAA,CNAME)

DNS server zpřístupňuje obsah.

A(IPV4) a AAAA(IPV6) záznamy, které slouží pro nasměrování domény na IP adresu

CNAME záznam, který má na starost nasměrování jedné domény na jinou

Obrázek: zobrazení informací o serveru v CMD pomocí příkazu nslookup



Analýza síťového provozu linphone

Aplikační protokol: DNS, SIP(SIP/SDP, STUN), RTP(RTCP),

Transportní protokol: UDP

Síťový protokol: IPV4

Porty:

Připojujeme se pomocí UDP protokolu z portů 50561-50565(port se s každým odeslaným dotazem změní) na DNS server, který běží na portu 53

50558 – port protokolu SIP

5060 – port aplikace linphone

7076 – port protokolu STUN a RTP

20452 – port aplikace, kontrola ověření uživatele, samotný hovor

IP adresy:

Dotazujeme se z IP adresy 192.168.157.128 na DNS server 8.8.8.8.

Dotazujeme se z IP adresy 192.168.157.128 na IP adresu 54.37.202.229, což je IP adresa aplikace linphone

Z IP adresy 192.168.157.128 voláme s uživatelem s IP adresou 192.168.1.108

Průběh komunikace:

No. 23-34 dotazujeme se z IP adresy 192.168.157.128 na stránku liphone.org s využitím DNS serveru(8.8.8.8), ze síťového provozu jde vidět, že se o dost zvětšil čas oproti minulých dotazů na jiný DNS server.

23	132245.735715	192.168.157.128	8.8.8.8	DNS	86	0x62b8	50561	53	Standard query 0x62b8 SRV _sip._udp.sip.linphone.org
24	132245.747011	8.8.8.8	192.168.157.128	DNS	160	0x62b8	53	50561	Standard query response 0x62b8 SRV _sip._udp.sip.linphone.org SRV 0 100 5060 sip6.linphone.or
25	132245.800592	192.168.157.128	8.8.8.8	DNS	77	0xc97b	50562	53	Standard query 0xc97b A sip6.linphone.org
26	132245.801165	192.168.157.128	8.8.8.8	DNS	77	0x435f	50563	53	Standard query 0x435f AAAA sip6.linphone.org
27	132245.801860	192.168.157.128	8.8.8.8	DNS	77	0x8fff	50564	53	Standard query 0x8fff A sip1.linphone.org
28	132245.802772	192.168.157.128	8.8.8.8	DNS	77	0x16ab	50565	53	Standard query 0x16ab AAAA sip1.linphone.org
29	132245.815509	8.8.8.8	192.168.157.128	DNS	93	0xc97b	53	50562	Standard query response 0xc97b A sip6.linphone.org A 54.37.202.229
30	132245.815509	8.8.8.8	192.168.157.128	DNS	105	0x435f	53	50563	Standard query response 0x435f AAAA sip6.linphone.org AAAA 2001:41d0:700:789::2020
31	132245.817036	8.8.8.8	192.168.157.128	DNS	137	0x16ab	53	50565	Standard query response 0x16ab AAAA sip1.linphone.org SOA ns1.gandi.net
32	132245.817326	192.168.157.128	8.8.8.8	DNS	77	0xf39a	63926	53	Standard query 0xf39a AAAA sip1.linphone.org
33	132245.832058	8.8.8.8	192.168.157.128	DNS	137	0xf39a	53	63926	Standard query response 0xf39a AAAA sip1.linphone.org SOA ns1.gandi.net
34	132245.835296	8.8.8.8	192.168.157.128	DNS	93	0x8fff	53	50564	Standard query response 0x8fff A sip1.linphone.org A 91.121.209.194

DNS-servery

```
Standard query response 0xc97b A sip6.linphone.org A 54.37.202.229
Standard query response 0x435f AAAA sip6.linphone.org AAAA 2001:41d0:700:789::2020
Standard query response 0x16ab AAAA sip1.linphone.org SOA ns1.gandi.net
```

No. 35-39 Pod IP adresou 192.168.157.128 se přihlašujeme do aplikace linphone, přihlášení nejprve nevyšlo, na druhý pokus proběhlo úspěšně, odeslali jsem pozvánku uživateli

35	132245.844501	192.168.157.128	54.37.202.229	SIP	978	50558	5060	Request: REGISTER sip:sip.linphone.org (1 binding) |
36	132245.877617	54.37.202.229	192.168.157.128	SIP	546	5060	50558	Status: 401 Unauthorized |
37	132245.909441	192.168.157.128	54.37.202.229	SIP	1253	50558	5060	Request: REGISTER sip:sip.linphone.org (1 binding) |
38	132245.952446	54.37.202.229	192.168.157.128	SIP	879	5060	50558	Status: 200 Registration successful (1 binding) |
39	132253.828699	54.37.202.229	192.168.157.128	SIP/SDP	1141	5060	50558	Request: INVITE sip:bpc-kom-test-12@192.168.1.108:58010 |

No. 40-52 Zde vidíme pokus o navázaní spojení, vyzvánění, čekání na zprávu o ověření uživatele, ACK potvrzení ověření uživatele

40	132253.848534	192.168.157.128	54.37.202.229	SIP	385	50558	5060	Status: 100 Trying |
41	132253.920845	192.168.157.128	54.37.202.229	SIP	539	50558	5060	Status: 180 Ringing |
42	132256.039278	192.168.157.128	54.37.202.229	UDP	46	50558	5060	50558 → 5060 Len=4
43	132256.634606	192.168.157.128	54.37.202.229	SIP/SDP	1091	50558	5060	Status: 200 Ok |
44	132256.635305	192.168.157.128	54.37.202.229	STUN	62	7076	20452	Binding Request
45	132256.635422	192.168.157.128	54.37.202.229	RTCP	62	7077	20453	7077 → 20453 Len=20
46	132256.708949	192.168.157.128	54.37.202.229	STUN	62	7076	20452	Binding Request
47	132256.709051	192.168.157.128	54.37.202.229	RTCP	62	7077	20453	7077 → 20453 Len=20
48	132256.714512	54.37.202.229	192.168.157.128	STUN	62	20452	7076	Binding Request
49	132256.714512	54.37.202.229	192.168.157.128	RTCP	62	20453	7077	20453 → 7077 Len=20
50	132256.732449	54.37.202.229	192.168.157.128	SIP	837	5060	50558	Request: ACK sip:bpc-kom-test-12@192.168.1.108:58010;verified |
51	132256.735507	54.37.202.229	192.168.157.128	STUN	62	20452	7076	Binding Request
52	132256.735507	54.37.202.229	192.168.157.128	RTCP	62	20453	7077	20453 → 7077 Len=20

No.53-2276 Zde probíhá samotný hovor mezi uživateli využívá se protokolu RTP a RTCP

No.	Time	Source	Destination	Protocol	Length	Transaction ID	Source Port	Destination Port	Info
54	132256.751864	54.37.202.229	192.168.157.128	RTP	214		20452	7076	PT=ITU-T G.711 PCMU, SSRC=0x65C1D035, Seq=0, Time=4047825119
55	132256.772092	54.37.202.229	192.168.157.128	RTP	214		20452	7076	PT=ITU-T G.711 PCMU, SSRC=0x65C1D035, Seq=1, Time=4047825279
56	132256.773838	192.168.157.128	54.37.202.229	RTP	214		7076	20452	PT=ITU-T G.711 PCMU, SSRC=0xB9DDAF5A, Seq=1, Time=2907549409
57	132256.792376	54.37.202.229	192.168.157.128	RTP	214		20452	7076	PT=ITU-T G.711 PCMU, SSRC=0x65C1D035, Seq=2, Time=4047825439
58	132256.792958	192.168.157.128	54.37.202.229	RTP	214		7076	20452	PT=ITU-T G.711 PCMU, SSRC=0xB9DDAF5A, Seq=2, Time=2907549569
59	132256.813226	192.168.157.128	54.37.202.229	RTP	214		7076	20452	PT=ITU-T G.711 PCMU, SSRC=0xB9DDAF5A, Seq=3, Time=2907549729
60	132256.813495	54.37.202.229	192.168.157.128	RTP	214		20452	7076	PT=ITU-T G.711 PCMU, SSRC=0x65C1D035, Seq=3, Time=4047825599
61	132256.833219	192.168.157.128	54.37.202.229	RTP	214		7076	20452	PT=ITU-T G.711 PCMU, SSRC=0xB9DDAF5A, Seq=4, Time=2907549889
62	132256.833737	54.37.202.229	192.168.157.128	RTP	214		20452	7076	PT=ITU-T G.711 PCMU, SSRC=0x65C1D035, Seq=4, Time=4047825759
63	132256.852985	192.168.157.128	54.37.202.229	RTP	214		7076	20452	PT=ITU-T G.711 PCMU, SSRC=0xB9DDAF5A, Seq=5, Time=2907550049
64	132256.854462	54.37.202.229	192.168.157.128	RTP	214		20452	7076	PT=ITU-T G.711 PCMU, SSRC=0x65C1D035, Seq=5, Time=4047825919
65	132256.872894	192.168.157.128	54.37.202.229	RTP	214		7076	20452	PT=ITU-T G.711 PCMU, SSRC=0xB9DDAF5A, Seq=6, Time=2907550209
66	132256.874364	54.37.202.229	192.168.157.128	RTP	214		20452	7076	PT=ITU-T G.711 PCMU, SSRC=0x65C1D035, Seq=6, Time=4047826079
67	132256.900424	192.168.157.128	54.37.202.229	RTP	214		7076	20452	PT=ITU-T G.711 PCMU, SSRC=0xB9DDAF5A, Seq=7, Time=2907550369
68	132256.900577	192.168.157.128	54.37.202.229	RTP	214		7076	20452	PT=ITU-T G.711 PCMU, SSRC=0xB9DDAF5A, Seq=8, Time=2907550529
69	132256.914822	54.37.202.229	192.168.157.128	RTP	214		20452	7076	PT=ITU-T G.711 PCMU, SSRC=0x65C1D035, Seq=7, Time=4047826239
70	132256.919934	192.168.157.128	54.37.202.229	RTP	214		7076	20452	PT=ITU-T G.711 PCMU, SSRC=0xB9DDAF5A, Seq=9, Time=2907550689
71	132256.935029	54.37.202.229	192.168.157.128	RTP	214		20452	7076	PT=ITU-T G.711 PCMU, SSRC=0x65C1D035, Seq=8, Time=4047826399
72	132256.941119	192.168.157.128	54.37.202.229	RTP	214		7076	20452	PT=ITU-T G.711 PCMU, SSRC=0xB9DDAF5A, Seq=10, Time=2907550849
73	132256.955474	54.37.202.229	192.168.157.128	RTP	214		20452	7076	PT=ITU-T G.711 PCMU, SSRC=0x65C1D035, Seq=9, Time=4047826559
74	132256.958226	192.168.157.128	54.37.202.229	RTP	214		7076	20452	PT=ITU-T G.711 PCMU, SSRC=0xB9DDAF5A, Seq=11, Time=2907551009
75	132256.979967	192.168.157.128	54.37.202.229	RTP	214		7076	20452	PT=ITU-T G.711 PCMU, SSRC=0xB9DDAF5A, Seq=12, Time=2907551169
76	132256.980072	54.37.202.229	192.168.157.128	RTP	214		20452	7076	PT=ITU-T G.711 PCMU, SSRC=0x65C1D035, Seq=10, Time=4047826719
77	132256.995986	54.37.202.229	192.168.157.128	RTP	214		20452	7076	PT=ITU-T G.711 PCMU, SSRC=0x65C1D035, Seq=11, Time=4047826879
78	132257.000227	192.168.157.128	54.37.202.229	RTP	214		7076	20452	PT=ITU-T G.711 PCMU, SSRC=0xB9DDAF5A, Seq=13, Time=2907551329
79	132257.011412	54.37.202.229	192.168.157.128	RTP	214		20452	7076	PT=ITU-T G.711 PCMU, SSRC=0x65C1D035, Seq=12, Time=4047827039
80	132257.016254	192.168.157.128	54.37.202.229	RTP	214		7076	20452	PT=ITU-T G.711 PCMU, SSRC=0xB9DDAF5A, Seq=14, Time=2907551489
81	132257.026981	54.37.202.229	192.168.157.128	RTP	214		20452	7076	PT=ITU-T G.711 PCMU, SSRC=0x65C1D035, Seq=13, Time=4047827199
82	132257.042357	54.37.202.229	192.168.157.128	RTP	214		20452	7076	PT=ITU-T G.711 PCMU, SSRC=0x65C1D035, Seq=14, Time=4047827359
83	132257.053076	192.168.157.128	54.37.202.229	RTP	214		7076	20452	PT=ITU-T G.711 PCMU, SSRC=0xB9DDAF5A, Seq=15, Time=2907551649
84	132257.063061	54.37.202.229	192.168.157.128	RTP	214		20452	7076	PT=ITU-T G.711 PCMU, SSRC=0x65C1D035, Seq=15, Time=4047827519
85	132257.069309	192.168.157.128	54.37.202.229	RTP	214		7076	20452	PT=ITU-T G.711 PCMU, SSRC=0xB9DDAF5A, Seq=16, Time=2907551809

Informace o hovoru

Zde můžeme vidět informace o hovoru: Kdy hovor začal a skončil, kdo a komu volal, využívaný protokol, délka hovoru, přenesení paketů

Start Time	Stop Time	Initial Speaker	From	To	Protocol	Duration	Packets	State	Comments
132253.828699	132278.806367	54.37.202.229	<sip:bpc-kom-test-12@sip.linphone.org>	<sip:bpc-kom-test-12@sip.linphone.org>	SIP	00:00:24	7	COMPLETED	INVITE 200

Source Address	Source Port	Destination Address	Destination Port	SSRC	Payload	Packets	Lost	Max Delta (ms)	Max Jitter	Mean Jitter
54.37.202.229	20452	192.168.157.128	7076	0x65c1d035	g711U	1099	0 (0.0%)	69.378	7.819	4.054
192.168.157.128	7076	54.37.202.229	20452	0xb9ddaf5a	g711U	1101	0 (0.0%)	39.229	8.526	2.748

Daniel Prachař
240969

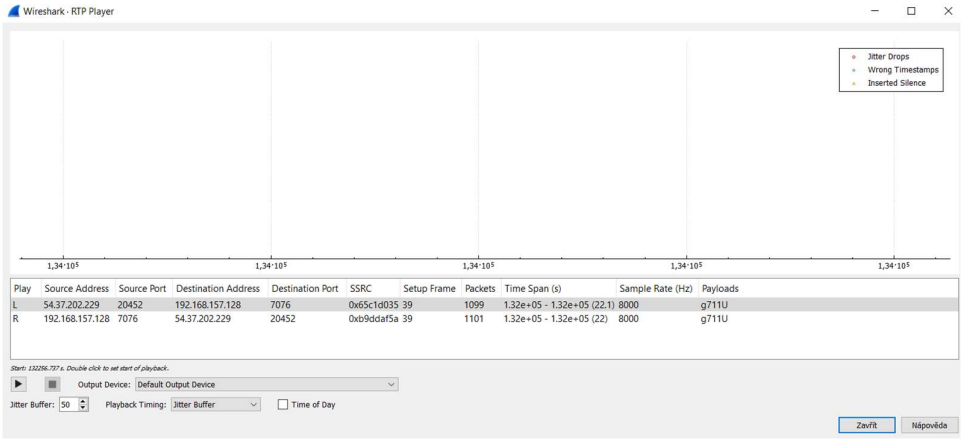
Délka hovoru: 24 sekund

Ztrátovost paketů: žádná

Počet paketů: 1099(54.37.202.229) 1101(192.168.157.128)

Bezpečnost: nezašifrovaný hovor, kdokoliv si hovor může odposlechnout

Tajná zpráva: Vysoké učení technické v Brně



No. 2277-2281 Zde je žádost na ukončení hovoru, žádost je přijata a hovor končí

```
2277 132278.749721 192.168.157.128      54.37.202.229       SIP      440      Request: BYE sip:bpc-kom-test-12@147.229.146.74:58304 |
2278 132278.806367 54.37.202.229        192.168.157.128     RTP      214      PT=ITU-T G.711 PCMU, SSRC=0x65C1D035, Seq=1098, Time=4048000799
2279 132278.806367 54.37.202.229        192.168.157.128     SIP      427      Status: 200 Ok |
2280 132286.047067 192.168.157.128      54.37.202.229       UDP       46      50558 → 5060 Len=4
2281 132296.054225 192.168.157.128      54.37.202.229       UDP       46      50558 → 5060 Len=4
```

Analýza síťového provozu ICMP – Ping

Aplikační protokol: DNS

Transportní protokol: UDP

Síťový protokol: IPV4, ICMP

Porty:

Připojujeme se pomocí UDP protokolu z portu 50443 na DNS server, který běží na portu 53

IP adresy:

Dotazujeme se z IP adresy 192.168.1.108 na DNS server 192.168.1.1, dále zadáváme příkaz ping

Průběh komunikace:

No.2282-2287 V CMD byl zadán příkaz ping na stránku www.seznam.cz, můžeme zde vidět, že ping byl zadaný s parametrem -n 2, který místo defaultně nastavených 4 dotazů pošle 2.

Ping neproběhl úspěšně, protože TTL přesáhlo limit a protokol ICMP vypsal chybovou hlášku

2282	424797.152890	192.168.1.108	192.168.1.1	DNS	73	0x5b7d	50443	53	Standard query 0x5b7d A www.seznam.cz
2283	424797.160757	192.168.1.1	192.168.1.108	DNS	137	0x5b7d	53	50443	Standard query response 0x5b7d A www.seznam.cz A 77.75.74.172 A 77.75.74.176 A 77.75.75.172 A
2284	424797.170705	192.168.1.108	77.75.74.172	ICMP	74				Echo (ping) request id=0x0001, seq=41/10496, ttl=6 (no response found!)
2285	424797.176223	91.210.16.195	192.168.1.108	ICMP	70				Time-to-live exceeded (Time to live exceeded in transit)
2286	424798.179343	192.168.1.108	77.75.74.172	ICMP	74				Echo (ping) request id=0x0001, seq=42/10752, ttl=6 (no response found!)
2287	424798.184268	91.210.16.195	192.168.1.108	ICMP	70				Time-to-live exceeded (Time to live exceeded in transit)

Obrázek: Ukázka v CMD úspěšné pingu

```
C:\Users\dan-p>ping seznam.cz -n 2

Pinging seznam.cz [77.75.75.176] with 32 bytes of data:
Reply from 77.75.75.176: bytes=32 time=56ms TTL=54
Reply from 77.75.75.176: bytes=32 time=20ms TTL=54

Ping statistics for 77.75.75.176:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 20ms, Maximum = 56ms, Average = 38ms
```

Analýza síťového provozu UDP

Transportní protokol: UDP

Síťový protokol: IPV4

Porty:

Připojujeme se pomocí UDP protokolu přes port 8910 na cílový port 80

IP adresy:

Dotaz z IP adresy 172.40.10.125 na cílovou IP adresu 172.40.10.1

Průběh komunikace:

No.	Time	Source	Destination	Protocol	Length	Transaction ID	Source Port	Destination Port	Source Port	Destination Port	Data	Length	Info
2288	30291560.724…	172.40.10.125	172.40.10.1	UDP	1514		8910	80			✓	1472	8910 → 80 Len=1472
2289	30291560.882…	172.40.10.125	172.40.10.1	UDP	1514		8910	80			✓	1472	8910 → 80 Len=1472
2290	30291562.757…	172.40.10.1	172.40.10.125	UDP	60		80	8910			✓	18	80 → 8910 Len=18
2291	30291562.920…	172.40.10.125	172.40.10.1	UDP	1514		8910	80			✓	1472	8910 → 80 Len=1472
2292	30291563.911…	172.40.10.125	172.40.10.1	UDP	1514		8910	80			✓	1472	8910 → 80 Len=1472
2293	30291564.946…	172.40.10.1	172.40.10.125	UDP	60		80	8910			✓	18	80 → 8910 Len=18
2294	30291565.115…	172.40.10.125	172.40.10.1	UDP	619		8910	80			✓	577	8910 → 80 Len=577
2295	30291565.935…	172.40.10.1	172.40.10.125	UDP	60		80	8910			✓	18	80 → 8910 Len=18
2296	30291568.162…	172.40.10.125	172.40.10.1	UDP	619		8910	80			✓	577	8910 → 80 Len=577
2297	30291570.189…	172.40.10.1	172.40.10.125	UDP	60		80	8910			✓	18	80 → 8910 Len=18

No. 2288-2297 Dotazujeme se z adresy 172.40.10.125 na webový server běžící na portu 80 na stránku https://forms.office.com můžeme zde vidět přenos dat, takže uživatel dále stránku používal

Analýza síťového provozu TCP, HTTP

Aplikační protokol: HTTP

Transportní protokol: TCP

Síťový protokol: IPV4

Porty:

Připojujeme se pomocí UDP protokolu z portů 57233 na DNS server, který běží na portu 53

80 – na tomto portu běží http protokol

50710 – na tomto portu běží TCP

IP adresy:

Dotazujeme se z IP adresy 147.229.146.144 na DNS server 147.229.71.14

Průběh komunikace:

No.	Time	Source	Destination	Protocol	Length	Transaction ID	Source Port	Destination Port	Source Port	Destination Port	Info
2298	30301063.684…	147.229.146.114	147.229.71.14	DNS	73	0xba83	57233	53			Standard query 0xba83 A jigsaw.w3.org
2299	30301063.684…	147.229.71.14	147.229.146.114	DNS	89	0xba83	53	57233			Standard query response 0xba83 A jigsaw.w3.org A 128.30.52.21
2300	30301063.686…	147.229.146.114	128.30.52.21	TCP	66				50710	80	50710 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2301	30301063.790…	128.30.52.21	147.229.146.114	TCP	66				80	50710	80 → 50710 [SYN, ACK] Seq=0 Ack=1 Win=42340 Len=0 MSS=1460 SACK_PERM=1
2302	30301063.790…	147.229.146.114	128.30.52.21	TCP	54				50710	80	50710 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
2303	30301063.790…	147.229.146.114	128.30.52.21	HTTP	213				50710	80	GET /HTTP/300/301.html HTTP/1.1
2304	30301063.896…	128.30.52.21	147.229.146.114	HTTP	645				80	50710	HTTP/1.1 301 (text/html)
2305	30301063.899…	147.229.146.114	128.30.52.21	HTTP	213				50710	80	GET /HTTP/300/301.html HTTP/1.1
2306	30301064.005…	128.30.52.21	147.229.146.114	HTTP	645				80	50710	HTTP/1.1 301 (text/html)
2307	30301064.007…	147.229.146.114	128.30.52.21	HTTP	213				50710	80	GET /HTTP/300/301.html HTTP/1.1
2308	30301064.114…	128.30.52.21	147.229.146.114	HTTP	645				80	50710	HTTP/1.1 301 (text/html)
2309	30301064.116…	147.229.146.114	128.30.52.21	TCP	54				50710	80	50710 → 80 [FIN, ACK] Seq=478 Ack=1774 Win=262656 Len=0
2310	30301064.220…	128.30.52.21	147.229.146.114	TCP	60				80	50710	80 → 50710 [FIN, ACK] Seq=1774 Ack=479 Win=42496 Len=0
2311	30301064.220…	147.229.146.114	128.30.52.21	TCP	54				50710	80	50710 → 80 [ACK] Seq=479 Ack=1775 Win=262656 Len=0

No.2298-2299 Dotazujeme se z IP adresy 147.229.146.114, pomocí DNS serveru na stránku http://jigsaw.w3.org/HTTP/300/301.html protokol pro komunikaci je zde TCP

Daniel Prachař
240969

Navázání spojení:

No.2300-2302 Pro komunikaci se používá trojcestný handshaking:

SYN – odeslání datagramu klientem(navázání komunikace) http

SYN ACK – server odešle potvrzovací datagram klientovi,

ACK – potvrzení, že stanice je připravena přijímat přenosy, přenos byl přijat

No.2303-2308 Get – dotazovací metoda http, využívá URL dokumentů, zpřístupňuje www stránku z webového serveru, oproti metodě POST se používá pro weby, které se tak často nemění

Ukončení spojení

No.2309-2311 Z adresy 147.229.146.114 jsme odeslali datagram, že nechceme posílat další data

FIN – ukončovací datagram

FIN ACK – odpověď protistrany na ukončení spojení

ACK – potvrzení ukončení přenosu

Statistiky

Zde můžeme vidět zastoupení jednotlivých protokolů, počet přenesených paketů a Bytů

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	2311	100.0	498302	0	0	0	0
Ethernet	100.0	2311	6.5	32354	0	0	0	0
Internet Protocol Version 4	100.0	2311	9.3	46220	0	0	0	0
User Datagram Protocol	99.3	2295	3.7	18360	0	19	152	0
Session Traversal Utilities for NAT	0.2	4	0.0	80	0	4	80	0
Session Initiation Protocol	0.5	11	1.6	8054	0	11	8054	0
Real-Time Transport Protocol	95.2	2200	75.9	378400	0	2200	378400	0
Real-time Transport Control Protocol	1.7	40	0.4	2112	0	8	352	0
Domain Name System	1.6	38	0.5	2536	0	38	2536	0
Data	0.6	15	1.4	7134	0	15	7134	0
Transmission Control Protocol	0.5	12	0.5	2514	0	6	144	0
Hypertext Transfer Protocol	0.3	6	0.5	2250	0	3	477	0
Line-based text data	0.1	3	0.2	1167	0	3	1167	0
Internet Control Message Protocol	0.2	4	0.0	152	0	4	152	0