

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

Vaše jméno	Alex Sporní
VUT ID	204633
Vypracovaný lab (označení)	Lab6 (Protokol DNS)

1. Číslovaný úkol z návodu

Zadání úkolu: **Spustte si program Wireshark, zapněte zachytávání paketů, zadejte filtr dnsa porovnejte jak se liší provoz při zadání dotazu na vutbr.cz a vutbr.cz. (s tečkou na konci) v interaktivním režimu programu nslookup.**

Řešení:

- **nslookup vutbr.cz** → Primárne vyhľadáva v lokálnej DNS doméne - DNS resolver na lokálnom PC
- **nslookup vutbr.cz.** → Primárne vyhľadáva priamo cez root DNS doménu rhino.cis.vutbr.cz a preskakuje lokálnu datbázu vutbr.cz.localdomain

dns							
No.	Time	Source	Destination	Sekvenční	Protocol	Length	Info
1	0.000000	192.168.17.138	8.8.8.8		DNS	80	Standard query 0x0002 A vutbr.cz.localdomain
2	0.012615	8.8.8.8	192.168.17.138		DNS	155	Standard query response 0x0002 No such name A vutbr.cz.localdomain S
3	0.012803	192.168.17.138	8.8.8.8		DNS	80	Standard query 0x0003 AAAA vutbr.cz.localdomain
vutbr.cz 4	0.030480	8.8.8.8	192.168.17.138		DNS	155	Standard query response 0x0003 No such name AAAA vutbr.cz.localdomai
5	0.030763	192.168.17.138	8.8.8.8		DNS	68	Standard query 0x0004 A vutbr.cz
6	0.062704	8.8.8.8	192.168.17.138		DNS	84	Standard query response 0x0004 A vutbr.cz A 147.229.2.90
7	0.065852	192.168.17.138	8.8.8.8		DNS	68	Standard query 0x0005 AAAA vutbr.cz
8	0.083770	8.8.8.8	192.168.17.138		DNS	125	Standard query response 0x0005 AAAA vutbr.cz SOA rhino.cis.vutbr.cz
11	6.287941	192.168.17.138	8.8.8.8		DNS	68	Standard query 0x0006 A vutbr.cz
vutbr.cz 12	6.300279	8.8.8.8	192.168.17.138		DNS	84	Standard query response 0x0006 A vutbr.cz A 147.229.2.90
13	6.300670	192.168.17.138	8.8.8.8		DNS	68	Standard query 0x0007 AAAA vutbr.cz
14	6.313174	8.8.8.8	192.168.17.138		DNS	125	Standard query response 0x0007 AAAA vutbr.cz SOA rhino.cis.vutbr.cz

> Frame 8: 125 bytes on wire (1000 bits), 125 bytes captured (1000 bits) on interface 0, id 0

> Ethernet II, Src: VMware_fb:de:3c (00:50:56:fb:de:3c), Dst: VMware_vmxnet3:00:0c:29:14:00:00:00:00

> Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.17.138

> User Datagram Protocol, Src Port: 53, Dst Port: 63514

> Domain Name System (response)

```

C:\Users\student\Desktop\xsporn01>nslookup
Default Server:  dns.google
Address:  8.8.8.8

> vutbr.cz
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    vutbr.cz
Address: 147.229.2.90

> vutbr.cz.
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    vutbr.cz
Address: 147.229.2.90

>

```

2. číslovaný úkol z návodu

Zadání úkolu: **Jaký transportní protokol je využit ve výchozím režimu pro přenos DNS paketů? Ověřte ve Wiresharku.**


Řešení: Je to protokol UDP (User Datagram Protocol) a operuje na portu 53 vid'. Screen.

```
> Internet Protocol Version 4, Src: 192.168.17.138, Dst: 8.8.8.8
▼ User Datagram Protocol, Src Port: 63512, Dst Port: 53
    Source Port: 63512
    Destination Port: 53
    Length: 46
    Checksum: 0xe281 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
    > [Timestamps]
```

3. číslovaný úkol z návodu

Zadání úkolu: **Nalezněte doménu, která má i IPv6 záznam (AAAA).**

Řešení:



```
C:\Users\student\Desktop\xsporn01>nslookup
Default Server:  dns.google
Address:  8.8.8.8

> fit.vut.cz
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    fit.vut.cz
Addresses:  2001:67c:1220:809::93e5:91a
            147.229.9.26

> -
```

4. číslovaný úkol z návodu

Zadání úkolu: **Pro doménu wikipedia.org. najděte pomocí serveru 1.1.1.1: odpovídající IPv4 adresu, IPv6 adresu, doménové jméno k IPv4 adrese, jmenný server a mailový server. Ověřte i ve Wiresharku, že byl skutečně použit zadaný server.**

Řešení:

```
Příkazový řádek - nslookup

C:\Users\student\Desktop\xsporn01>nslookup
Default Server:  dns.google
Address:  8.8.8.8

> server 1.1.1.1
Default Server:  one.one.one.one
Address:  1.1.1.1

> www.wikipedia.org
Server:  one.one.one.one
Address:  1.1.1.1

Non-authoritative answer:
Name:    dyna.wikimedia.org
Addresses: 2620:0:862:ed1a::1
          91.198.174.192
Aliases:  www.wikipedia.org

> set type=NS
> www.wikipedia.org
Server:  one.one.one.one
Address:  1.1.1.1

Non-authoritative answer:
www.wikipedia.org      canonical name = dyna.wikimedia.org

wikipedia.org
    primary name server = ns0.wikimedia.org
    responsible mail addr = hostmaster.wikimedia.org
    serial = 2021031621
    refresh = 43200 (12 hours)
    retry = 7200 (2 hours)
    expire = 1209600 (14 days)
    default TTL = 600 (10 mins)

>
```

No.	Time	Source	Destination	Sekvenční	Protocol	Length	Info
1	0.000000	192.168.17.138	1.1.1.1		DNS	89	Standard query 0x0009 NS www.wikipedia.org.localdomain
2	0.024818	1.1.1.1	192.168.17.138		DNS	164	Standard query response 0x0009 No such name NS www.wikipedia.o
3	0.025236	192.168.17.138	1.1.1.1		DNS	77	Standard query 0x000a NS www.wikipedia.org
4	0.150429	1.1.1.1	192.168.17.138		DNS	157	Standard query response 0x000a NS www.wikipedia.org CNAME dyna
7	27.304321	192.168.17.138	8.8.8.8		DNS	76	Standard query 0x8ce3 A wpad.localdomain
8	27.308899	8.8.8.8	192.168.17.138		DNS	151	Standard query response 0x8ce3 No such name A wpad.localdomain

<

> Frame 4: 157 bytes on wire (1256 bits), 157 bytes captured (1256 bits) on interface \Device\NPF_{F54A6428-385F-4667-8D33-4C9ADC633F43}

> Ethernet II, Src: VMware_fb:de:3c (00:50:56:fb:de:3c), Dst: VMware_28:f7:4b (00:0c:29:28:f7:4b)

▼ Internet Protocol Version 4, Src: 1.1.1.1, Dst: 192.168.17.138

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 143

Identification: 0xf7c5 (63429)

> Flags: 0x0000

Fragment offset: 0

Time to live: 128

Protocol: UDP (17)

Header checksum: 0x6e64 [validation disabled]

[Header checksum status: Unverified]

Source: 1.1.1.1

Destination: 192.168.17.138

> User Datagram Protocol, Src Port: 53, Dst Port: 61798

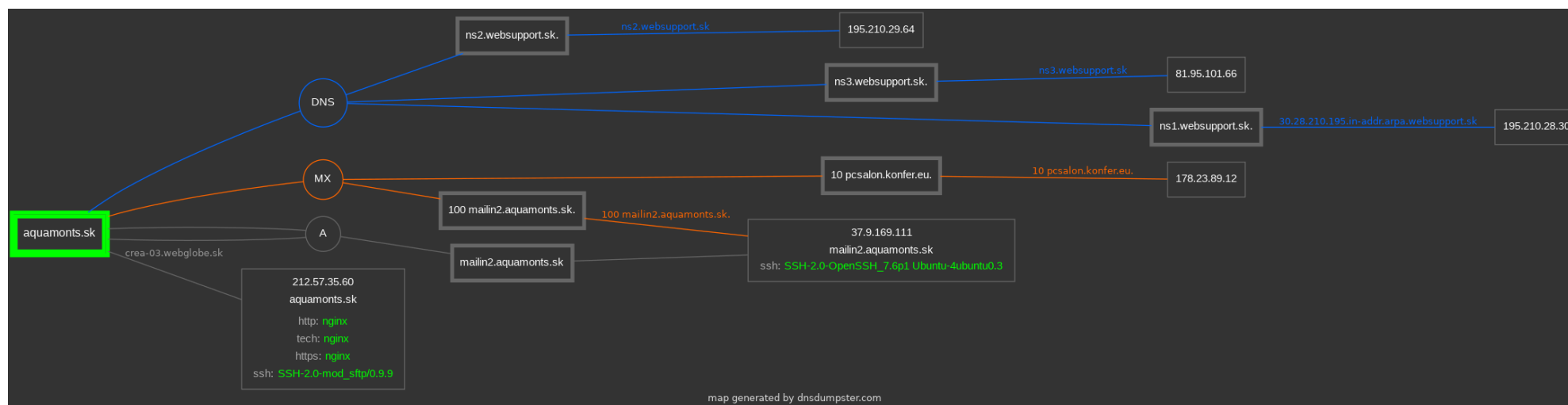
> Domain Name System (response)

5. číslovaný úkol z návodu

Zadání úkolu: **Pomocí nástroje dnsdumpster.com zaznamenejte do protokolu graficky z mapovanou doménu vaší oblíbené webové stránky a ve zkratce popište obdržené výsledky.**

Řešení:

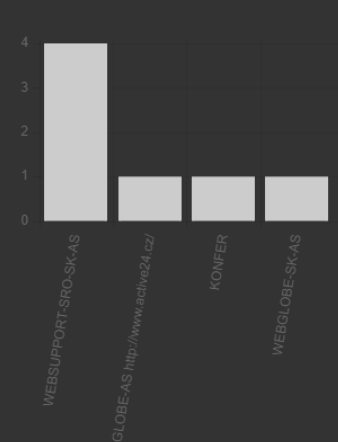
- z NS záznamov vyplýva, že majiteľom (poskytovateľom) domény je spoločnosť WEBSUPPORT s.r.o.
- rovnako v MX záznamoch je vidieť, že spoločnosť websupport ponúka aj mailové služby, serveri bežia pravdepodobne na linuxe



Showing results for aquamonts.sk

DNS ServersMX RecordsTXT RecordsHost (A) RecordsDomain Map

Hosting (IP block owners)



GeoIP of Host Locations



DNS Servers

ns2.websupport.sk. 🏠🔗🔒🔑🔍🟢	195.210.29.64 ns2.websupport.sk	WEBSUPPORT-SRO-SK-AS Slovakia
ns3.websupport.sk. 🏠🔗🔒🔑🔍🟢	81.95.101.66 ns3.websupport.sk	GLOBE-AS http://www.active24.cz/ Czechia
ns1.websupport.sk. 🏠🔗🔒🔑🔍🟢	195.210.28.30 30.28.210.195.in-addr.arpa.websupport.sk	WEBSUPPORT-SRO-SK-AS Slovakia

MX Records ** This is where email for the domain goes...

100 mailin2.aquamonts.sk. 🏠🔗🔒🟢	37.9.169.111 mail-proxymxphy-7.websupport.sk	WEBSUPPORT-SRO-SK-AS Slovakia
10 pcsalon.konfer.eu. 🏠🔗🔒🟢	178.23.89.12 mail2.konfer.eu	KONFER Slovakia

TXT Records ** Find more hosts in Sender Policy Framework (SPF) configurations

"spf2.0/pra a mx include:_sid.websupport.sk ?all"
"v=spf1 a mx include:_spf.websupport.sk ?all"

Host Records (A) ** this data may not be current as it uses a static database (updated monthly)

aquamonts.sk 🏠🔗🔒🔑🔍🟢 HTTP: nginx HTTPS: nginx SSH: SSH-2.0-mod_sftp/0.9.9 HTTP TECH: nginx HTTPS TECH: nginx	212.57.35.60 crea-03.webglobe.sk	WEBGLOBE-SK-AS Slovakia
---	-------------------------------------	----------------------------

6. číslovaný úkol z návodu

Zadání úkolu: **Objasněte stručně DNS Flags, i společně s bitem TC.**

Řešení:

- **QR** indikuje či správa je typu **query (0)** – dotaz alebo **reply (1)** – odpověď → délka je 1 bit
- **OPCODE** může mať viacero typov, QUERY (standard query, 0), IQUERY (inverse query, 1) alebo STATUS (server status request, 2) → délka je 4 bity
- **AA** je skratke pre autoritatívnu odpoveď, v odpovedi indikuje, či server je autoritatívny pre daný hostname → délka je 1 bit
- **TC** alebo TrunCation označuje či bola správa skrátená z dôvodu nadmernej veľkosti → délka je 1 bit
- **RD** Recursion Desired označuje či klient požaduje rekurzívny dopyt → délka je 1 bit
- **RA** Recursion Available označuje, že server podporuje rekurziu → délka je 1 bit
- **Z** Zero, tento flag je rezervovaný do budúcnosti → délka je 3 bity
- **RCODE** tzv. Response code označuje kód chyby NOERROR (0), FORMERR (1, Format error), SERVFAIL (2), NXDOMAIN (3, Nonexistent domain).

✓ **Flags: 0x8180 Standard query response, No error**

1... = Response: Message is a response

.000 0... = Opcode: Standard query (0)

.... .0.. = Authoritative: Server is not an authority for domain

.... ..0. = Truncated: Message is not truncated

.... ...1 = Recursion desired: Do query recursively

.... 1... = Recursion available: Server can do recursive queries

....0.. = Z: reserved (0)

....0. = Answer authenticated: Answer/authority portion was not authenticated by the server

....0 = Non-authenticated data: Unacceptable

.... 0000 = Reply code: No error (0)

7. číslování úkol z návodu

Zadání úkolu: **Vyplňte tabulku a vyhodnoťte naměřené hodnoty, zkuste se zamyslet nad výsledky. U dvou serverů s nejdelší dobou odezvy naleznete, kde se fyzicky tyto DNS servery nachází (<https://public-dns.info>).**

Řešení:

Jméno DNS serveru	IP adresa	Doba odezvy [ms]	Fyzická lokalita
google.com	8.8.8.8	0,0123 s	
Cloudflare	1.1.1.1	0,0270 s	
OpenDNS	208.67.222.222	0,0040 s	
CZ.NIC	193.17.47.1	0,0086 s	
ICONZ Ltd	210.48.77.69	0,3124 s	Nový Zéland
HKT Limited	203.198.68.197	0,3571 s	Hong Kong
ns1.artechinfo.in.	202.86.251.201	0,1649 s	

8. číslování úkol z návodu

Zadání úkolu: **Jaké doménové jméno se skrývá za hledanou IP adresou 147.229.71.30?**

Řešení: **feec.vutbr.cz**

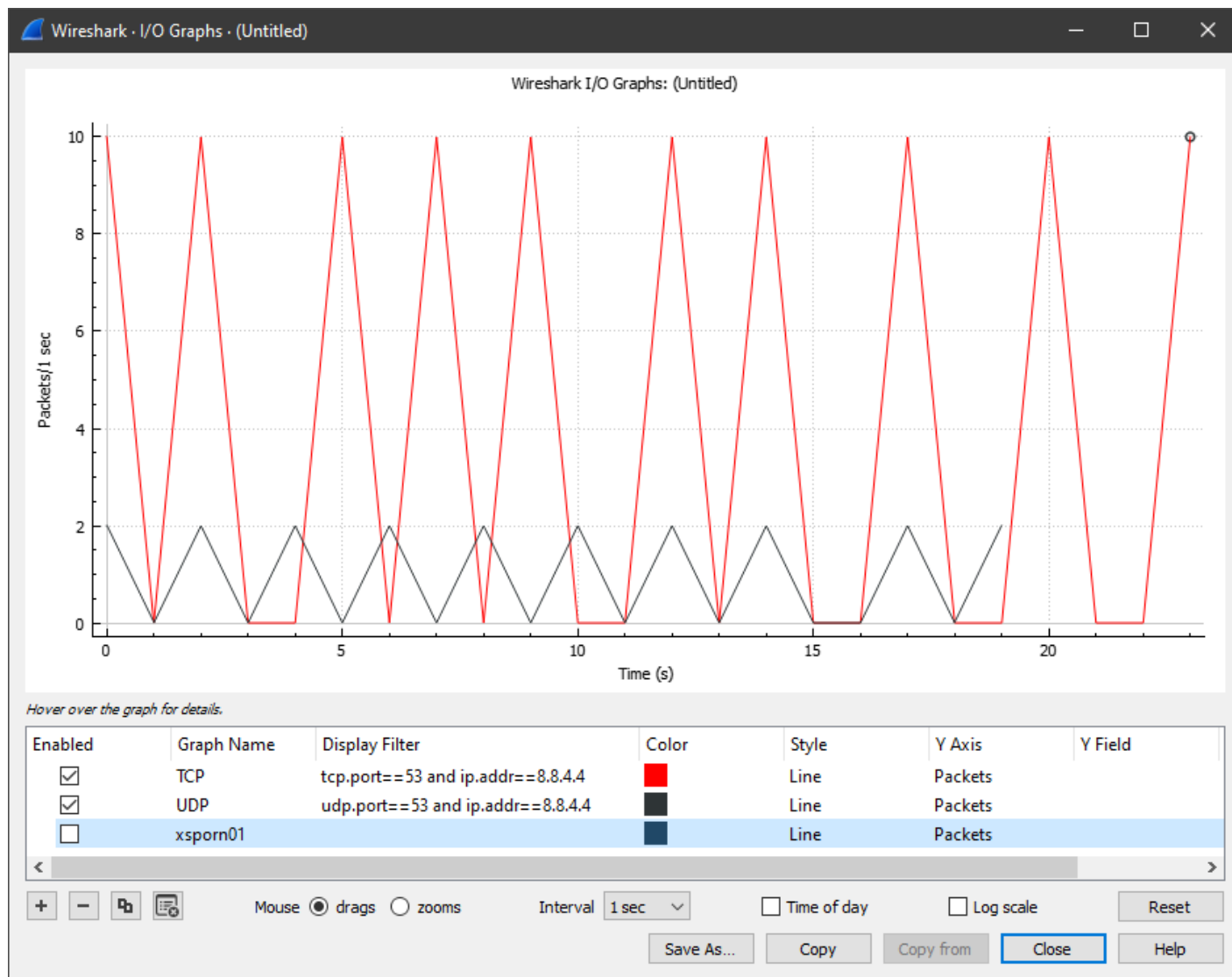
```
C:\Users\student\Desktop\xsporn01>nslookup 147.229.71.30
Server:  dns.google
Address:  8.8.8.8

Name:     www.feec.vutbr.cz
Address:  147.229.71.30
```

9. číslovaný úkol z návodu

Zadání úkolu: **Vytvořený graf uložte do protokolu, název grafu bude váš login.**

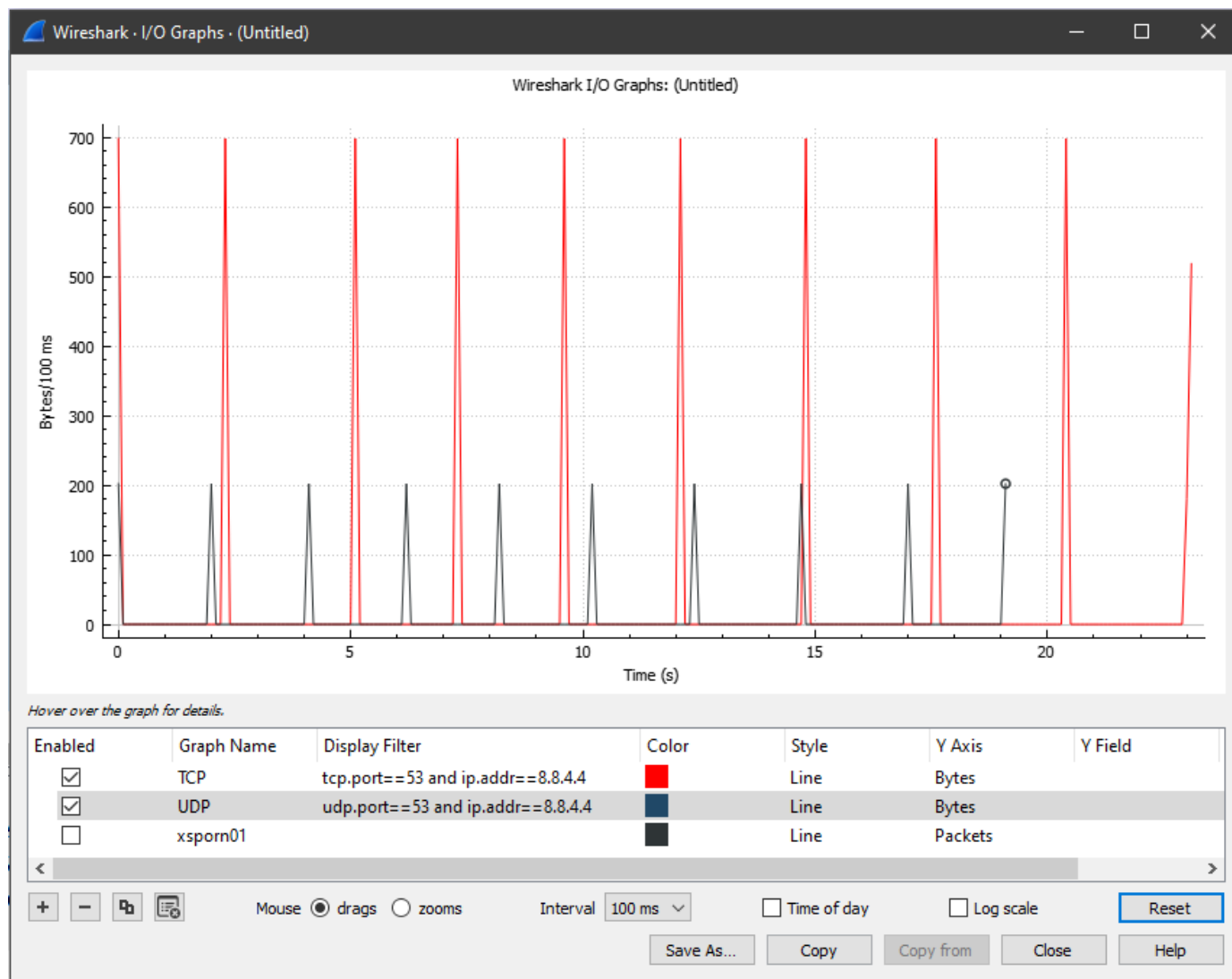
Řešení:



10. číslovaný úkol z návodu

Zadání úkolu: **Vytvořený graf upravte tak, aby neukazoval počty paketů v čase, ale počty přenesených bajtů.**

Řešení:



11. číslovaný úkol z návodu

Zadání úkolu: **Zjistěte, kolik celkem paketů potřeboval který transportní protokol pro přenos těchto DNS zpráv v testovaném případě. Proč tomu tak je?**

Řešení:

- V případě TCP je to dokopy 10 zpráv. 3 way handshake, request, ack, response a 4way handshake na ukončení spojení

1 0.000000	192.168.17.138	8.8.4.4	TCP	66	50889 → 53 [SYN] Seq=0 Win=6424
2 0.004582	8.8.4.4	192.168.17.138	TCP	60	53 → 50889 [SYN, ACK] Seq=0 Ack=
3 0.004675	192.168.17.138	8.8.4.4	TCP	54	50889 → 53 [ACK] Seq=1 Ack=1 Wi
4 0.004771	192.168.17.138	8.8.4.4	DNS	83	Message is a query Standard query 0x0000 A seznam.
5 0.004935	8.8.4.4	192.168.17.138	TCP	60	53 → 50889 [ACK] Seq=1 Ack=30 W
6 0.008697	8.8.4.4	192.168.17.138	DNS	147	Message is a response 0.003926000 Standard query response 0x0000
7 0.008851	192.168.17.138	8.8.4.4	TCP	54	50889 → 53 [FIN, ACK] Seq=30 Ac
8 0.009060	8.8.4.4	192.168.17.138	TCP	60	53 → 50889 [ACK] Seq=94 Ack=31
9 0.013056	8.8.4.4	192.168.17.138	TCP	60	53 → 50889 [FIN, PSH, ACK] Seq=
10 0.013112	192.168.17.138	8.8.4.4	TCP	54	50889 → 53 [ACK] Seq=31 Ack=95

- V případě UDP sú to len 2 správy. Request a response.

101 *REF*	192.168.17.138	8.8.4.4	DNS	69	Message is a query Standard query 0x0000 A seznam.
102 0.004261	8.8.4.4	192.168.17.138	DNS	133	Message is a response 0.004261000 Standard query response 0x0000

12. číslovaný úkol z návodu

Zadání úkolu: **Do protokolu vložte printscreen z programu Wireshark, kde lze pozorovat, že DNS odpověď byla zaslána pomocí protokolu TCP, podobně jako tomu je na obr.2.11.**

Řešení:

(udp.port==53 or tcp.port==53) and ip.addr == 1.1.1.1									
No.	Time	Source	Destination	Sekvenční	Protocol	Length	Response	Time	Info
40	77.463102	192.168.17.138	1.1.1.1		TCP	66		50938 → 53	[SYN] Seq=0 Win=64240 Len=0 MSS=1460
41	77.468396	1.1.1.1	192.168.17.138		TCP	60		53 → 50938	[SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
42	77.468518	192.168.17.138	1.1.1.1		TCP	54		50938 → 53	[ACK] Seq=1 Ack=1 Win=64240 Len=0
43	77.468699	192.168.17.138	1.1.1.1		DNS	98	Message is a qu...		Standard query 0x0000 DNSKEY feec.vutbr.cz OPT
44	77.468833	1.1.1.1	192.168.17.138		TCP	60		53 → 50938	[ACK] Seq=1 Ack=45 Win=64240 Len=0
45	77.473871	1.1.1.1	192.168.17.138		TCP	1514		53 → 50938	[ACK] Seq=1 Ack=45 Win=64240 Len=1460
46	77.473871	1.1.1.1	192.168.17.138		DNS	304	Message is a re... 0...		Standard query response 0x0000 DNSKEY feec.vutbr.cz
47	77.473975	192.168.17.138	1.1.1.1		TCP	54		50938 → 53	[ACK] Seq=45 Ack=1711 Win=64240 Len=0
48	77.474038	192.168.17.138	1.1.1.1		TCP	54		50938 → 53	[FIN, ACK] Seq=45 Ack=1711 Win=64240 Len=0
49	77.474246	1.1.1.1	192.168.17.138		TCP	60		53 → 50938	[ACK] Seq=1711 Ack=46 Win=64239 Len=0
50	77.478423	1.1.1.1	192.168.17.138		TCP	60		53 → 50938	[FIN, PSH, ACK] Seq=1711 Ack=46 Win=64240 Len=0
51	77.478473	192.168.17.138	1.1.1.1		TCP	54		50938 → 53	[ACK] Seq=46 Ack=1712 Win=64240 Len=0

> [2 Reassembled TCP Segments (1710 bytes): #45(1460), #46(250)]

▼ Domain Name System (response)

Length: 1708

Transaction ID: 0x0000

> Flags: 0x81a0 Standard query response, No error

Questions: 1

Answer RRs: 4

Authority RRs: 0

Additional RRs: 1

> Queries

> Answers

> Additional records

[\[Request In: 43\]](#)

[Time: 0.005172000 seconds]

13. číslovaný úkol z návodu

Zadání úkolu: **Nalezněte v komunikaci první příznak TC - truncated, velikost odpovědi a zaznamenejte printscreenem, společně s celou TCP komunikací pro dotaz na alibabacloud.com.**

Řešení:

Wireshark capture showing network traffic between 192.168.17.138 and 1.1.1.1. The capture includes DNS queries and responses, as well as a TCP connection establishment and data transfer.

No.	Time	Source	Destination	Sekvenční	Protocol	Length	Response	Time	Info
2	26.999118	192.168.17.138	1.1.1.1		DNS	80	Message is a qu...		Standard query 0x0001 PTR 1.1.1.1.in-addr.arpa
3	27.003448	1.1.1.1	192.168.17.138		DNS	109	Message is a re...	0...	Standard query response 0x0001 PTR 1.1.1.1.in-a
4	27.005918	192.168.17.138	1.1.1.1		DNS	88	Message is a qu...		Standard query 0x0002 A alibabacloud.com.locald
5	27.042028	1.1.1.1	192.168.17.138		DNS	163	Message is a re...	0...	Standard query response 0x0002 No such name A a
6	27.042274	192.168.17.138	1.1.1.1		DNS	76	Message is a qu...		Standard query 0x0003 A alibabacloud.com
7	27.545890	1.1.1.1	192.168.17.138		DNS	76	Message is a re...	0...	Standard query response 0x0003 A alibabacloud.c
8	27.546194	192.168.17.138	1.1.1.1		TCP	66			50939 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
9	27.550569	1.1.1.1	192.168.17.138		TCP	60			53 → 50939 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
10	27.550638	192.168.17.138	1.1.1.1		TCP	54			50939 → 53 [ACK] Seq=1 Ack=1 Win=64240 Len=0
11	27.550754	192.168.17.138	1.1.1.1		TCP	56			50939 → 53 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=0
12	27.551009	1.1.1.1	192.168.17.138		TCP	60			53 → 50939 [ACK] Seq=1 Ack=3 Win=64240 Len=0
13	27.551027	192.168.17.138	1.1.1.1		DNS	88	Message is a qu...		Standard query 0x0003 A alibabacloud.com
14	27.551201	1.1.1.1	192.168.17.138		TCP	60			53 → 50939 [ACK] Seq=1 Ack=37 Win=64240 Len=0
15	27.559361	1.1.1.1	192.168.17.138		DNS	570	Message is a re...	0...	Standard query response 0x0003 A alibabacloud.c
16	27.559496	192.168.17.138	1.1.1.1		TCP	54			50939 → 53 [FIN, ACK] Seq=37 Ack=517 Win=63724
17	27.559793	1.1.1.1	192.168.17.138		TCP	60			53 → 50939 [ACK] Seq=517 Ack=38 Win=64239 Len=0
18	27.563465	1.1.1.1	192.168.17.138		TCP	60			53 → 50939 [FIN, PSH, ACK] Seq=517 Ack=38 Win=6
19	27.563490	192.168.17.138	1.1.1.1		TCP	54			50939 → 53 [ACK] Seq=38 Ack=518 Win=63724 Len=0

Packet 15 details:

```
> User Datagram Protocol, Src Port: 53, Dst Port: 50527
> Domain Name System (response)
  Transaction ID: 0x0003
  > Flags: 0x8380 Standard query response, No error
    1... .. = Response: Message is a response
    .000 0... .. = Opcode: Standard query (0)
    .... 0... .. = Authoritative: Server is not an authority for domain
    .... 01. .... = Truncated: Message is truncated
    .... 011 .... = Recursion desired: Do query recursively
    .... 1... .. = Recursion available: Server can do recursive queries
    .... 0... .. = Z: reserved (0)
    .... 0... .. = Answer authenticated: Answer/authority portion was not authenticated by the server
    .... 0... .. = Non-authenticated data: Unacceptable
    .... 0000 = Reply code: No error (0)
Questions: 1
```

Zadání úkolu: **Co konkrétně uvádí pole Signature v programu DNS resolver, použijte k tomu záznam z Wiresharku a doložte printscreen.**

No.	Time	Source	Destination	Sekven	Protocol	Length	Response	Time	Info
2	1.355783	192.168.17.138	8.8.8.8		DNS	79	Message is a query		Standard query 0x0000 A vutbr.cz OPT
3	1.418429	8.8.8.8	192.168.17.138		DNS	263	Message is a response	0...	Standard query response 0x0000 A vutbr.cz

No.	Time	Source	Destination	Sekven	Protocol	Length	Response	Time	Info
2	1.355783	192.168.17.138	8.8.8.8		DNS	79	Message is a query		Standard query 0x0000 A vutbr.cz OPT
3	1.418429	8.8.8.8	192.168.17.138		DNS	263	Message is a response	0...	Standard query response 0x0000 A vutbr.cz

```

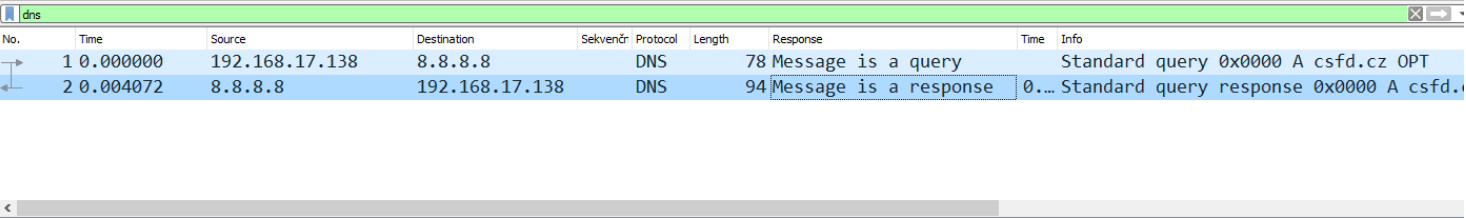
<
Authority RRs: 0
Additional RRs: 1
v Queries
  > vutbr.cz: type A, class IN
v Answers
  v vutbr.cz: type A, class IN, addr 147.229.2.90
    Name: vutbr.cz
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 299 (4 minutes, 59 seconds)
    Data length: 4
    Address: 147.229.2.90
  v vutbr.cz: type RRSIG, class IN
    Name: vutbr.cz
    Type: RRSIG (Resource Record Signature) (46)
    Class: IN (0x0001)
    Time to live: 299 (4 minutes, 59 seconds)
    Data length: 156
    Type Covered: A (Host Address) (1)
    Algorithm: RSA/SHA1 (5)
    Labels: 2
    Original TTL: 300 (5 minutes)
    Signature Expiration: Mar 26, 2021 12:42:01.000000000 Strední Evropa (bežný čas)
    Signature Inception: Feb 24, 2021 12:42:01.000000000 Strední Evropa (bežný čas)
    Key Tag: 39756
    Signer's name: vutbr.cz
    Signature: 7a00adc10d54bf9b3102454f75b7076e662ab8d68c59f0d7...
v Additional records
  v <Root>: type OPT

```

15. číslovaný úkol z návodu

Zadání úkolu: **Stejný proces přes DNS resolver a Wireshark aplikujte na webovou stránku csfd.cz a nalezněte hodnotu pole Signature (printscreen Wireshark).**

Řešení: csfd.cz pravděpodobně nepodporuje DNSSEC, z tohoto důvodu sekcia Signature vo wiresharku absenteuje.



No.	Time	Source	Destination	Sekvenční	Protocol	Length	Response	Time	Info
1	0.000000	192.168.17.138	8.8.8.8		DNS	78	Message is a query		Standard query 0x0000 A csfd.cz OPT
2	0.004072	8.8.8.8	192.168.17.138		DNS	94	Message is a response	0.004072	Standard query response 0x0000 A csfd.cz

```
.... 1 = Recursion desired: Do query recursively
.... 1 = Recursion available: Server can do recursive queries
.... 0 = Z: reserved (0)
.... 0 = Answer authenticated: Answer/authority portion was not authenticated by the server
.... 0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)

Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 1
Queries
  > csfd.cz: type A, class IN
Answers
  > csfd.cz: type A, class IN, addr 93.185.98.100
    Name: csfd.cz
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 2169 (36 minutes, 9 seconds)
    Data length: 4
    Address: 93.185.98.100
Additional records
  > <Root>: type OPT
    Name: <Root>
    Type: OPT (41)
    UDP payload size: 512
    Higher bits in extended RCODE: 0x00
    EDNS0 version: 0
  > Z: 0x8000
    1... = DO bit: Accepts DNSSEC security RRs
    .000 0000 0000 0000 = Reserved: 0x0000
    Data length: 0
[Request In: 1]
[Time: 0.004072000 seconds]
```


16. číslovaný úkol z návodu

Zadání úkolu: **Vyhledejte pomocí nástroje <https://dnsviz.net> doménu csfd.cz a výsledný diagram si stáhněte, vložte do protokolu a okomentujte obdržené výsledky.**

Řešení: Z diagramu je možné vidieť, že DNSKEY je podporovaný root aj cz doménou. Doména csfd.cz nepodporuje DNSKEY a na samotnej stránke dnsviz.net je označená ako INSECURE. DNSKEY obsahuje informácie o algoritme, veľkosti použitých bitov a timestamps (časové značky).

