lŠablona pro odevzdávání výstupů z distančních cvičení předmětu MPC-PKT určená k editaci a odevzdání po vytvoření PDF verze

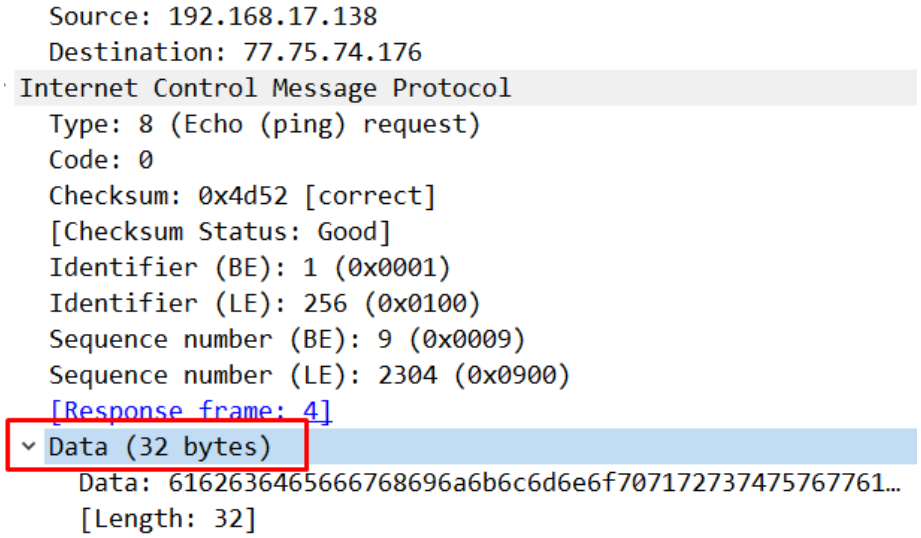
Vaše jméno	Alex Sporni
VUT ID	204633
Vypracovaný lab (označení)	**Lab5 (Úvod do programu Wireshark s pomocí utility ping ICMP protokolu, DNS resolveru a DHCP protokolu)**

---

1. číslovaný úkol z návodu

Zadání úkolu: **Zjistěte, kolik bajtů má celá ICMP část kteréhokoliv ze zachycených paketů.**

Řešení: Celá ICMP časť má **40B** a dátová časť má **32B**

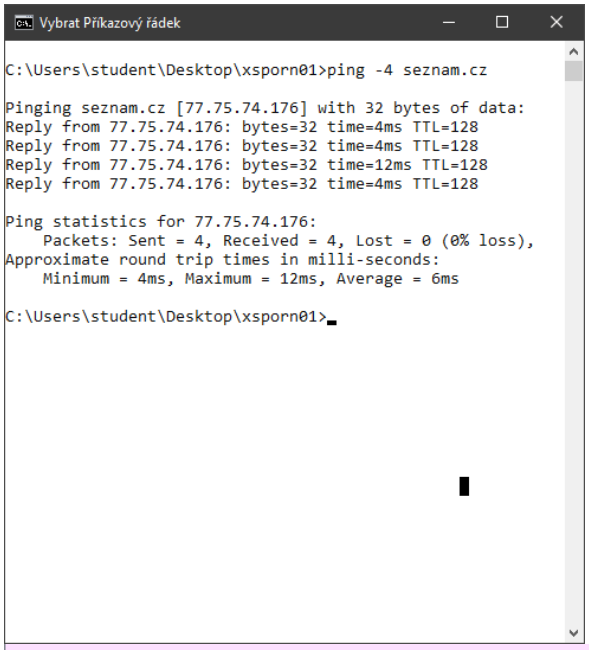


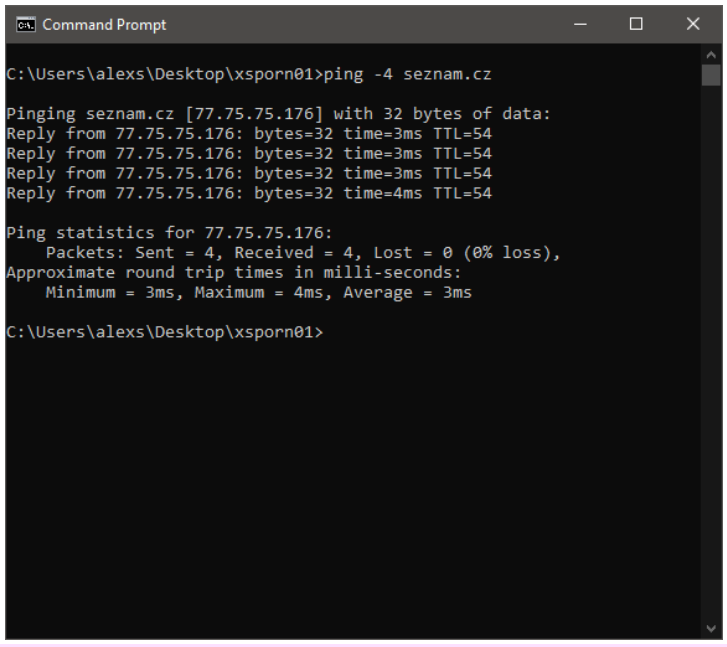
---

2. číslovaný úkol z návodu

Zadání úkolu: **Ve svém hlavním operačním systému si nainstalujte Wireshark a opakujte z něj úkony výše. Zjistěte z Wiresharku, jakou konkrétní hodnotu TTL využívá váš hlavní operační systém u ICMP echo request paketu a jaká hodnota je u ICMP echo reply. V tomto i dalších relevantních úkolech nezapomeňte, že u printscreenu příkazové řádky musí být vidět název složky dle vašeho VUT loginu.**

Řešení: Hodnota TTL na **VM** predstavuje **TTL = 128** pre request aj reply a hodnota na **PC** představuje **TTL = 54** pre reply a **TTL = 128** pre request.





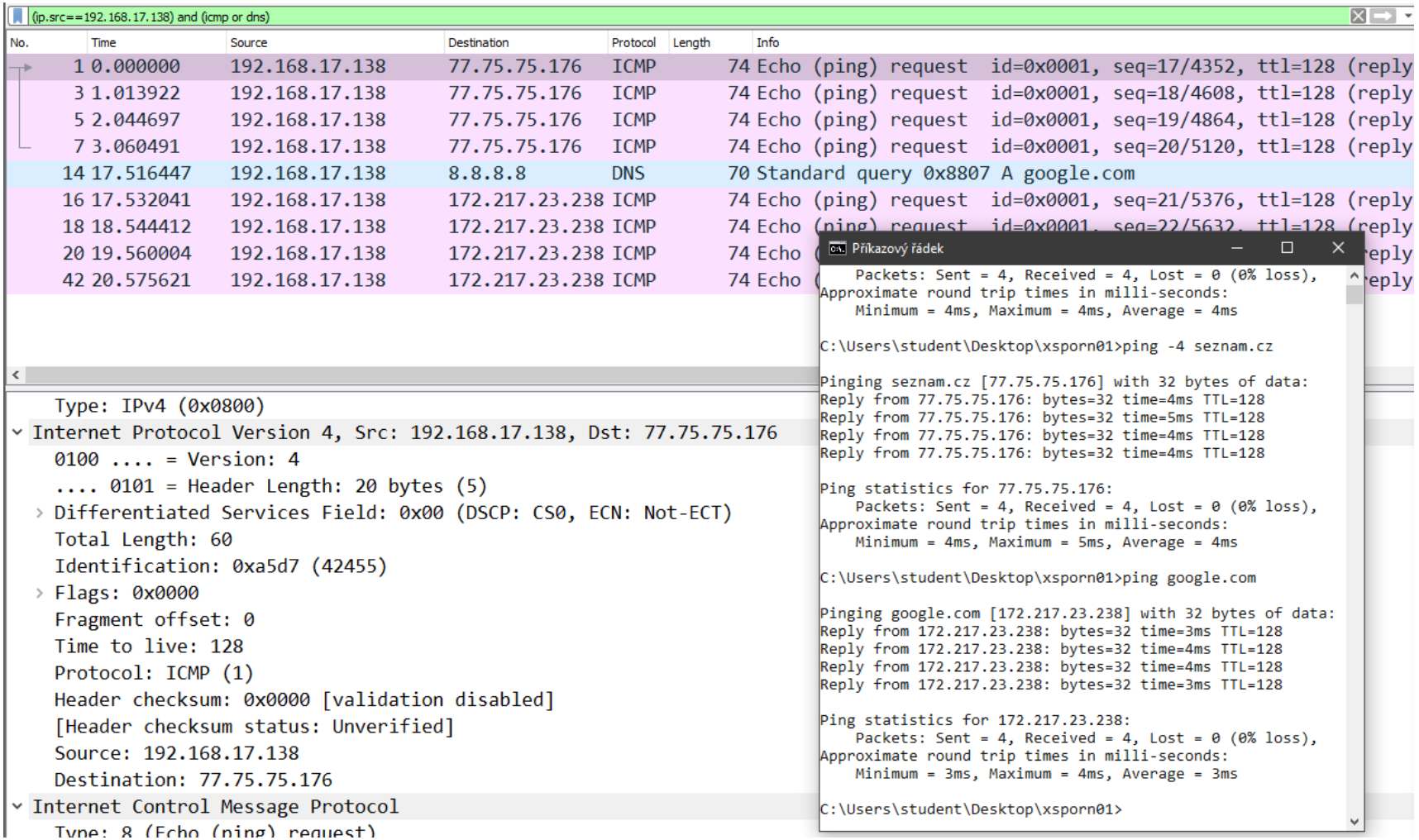
166 3.669267	147.229.192.11	77.75.75.176	ICMP	74 Echo (ping) request	id=0x0001, seq=18/4608, ttl=128 (reply in 167)
167 3.672941	77.75.75.176	147.229.192.11	ICMP	74 Echo (ping) reply	id=0x0001, seq=18/4608, ttl=54 (request in 166)
221 4.673371	147.229.192.11	77.75.75.176	ICMP	74 Echo (ping) request	id=0x0001, seq=19/4864, ttl=128 (reply in 222)
222 4.677059	77.75.75.176	147.229.192.11	ICMP	74 Echo (ping) reply	id=0x0001, seq=19/4864, ttl=54 (request in 221)
264 5.678795	147.229.192.11	77.75.75.176	ICMP	74 Echo (ping) request	id=0x0001, seq=20/5120, ttl=128 (reply in 265)
265 5.682559	77.75.75.176	147.229.192.11	ICMP	74 Echo (ping) reply	id=0x0001, seq=20/5120, ttl=54 (request in 264)
313 6.682612	147.229.192.11	77.75.75.176	ICMP	74 Echo (ping) request	id=0x0001, seq=21/5376, ttl=128 (reply in 314)
314 6.686525	77.75.75.176	147.229.192.11	ICMP	74 Echo (ping) reply	id=0x0001, seq=21/5376, ttl=54 (request in 313)

Destination	Protocol	Length	Info
8.8.8.8	DNS	69	Standard query 0xac08 A seznam.cz
192.168.17.138	DNS	133	Standard query response 0xac08 A seznam.cz A 77.75.74
77.75.74.176	ICMP	74	Echo (ping) request id=0x0001, seq=9/2304, ttl=128 (
192.168.17.138	ICMP	74	Echo (ping) reply id=0x0001, seq=9/2304, ttl=128 (
77.75.74.176	ICMP	74	Echo (ping) request id=0x0001, seq=10/2560, ttl=128
192.168.17.138	ICMP	74	Echo (ping) reply id=0x0001, seq=10/2560, ttl=128
77.75.74.176	ICMP	74	Echo (ping) request id=0x0001, seq=11/2816, ttl=128
192.168.17.138	ICMP	74	Echo (ping) reply id=0x0001, seq=11/2816, ttl=128
77.75.74.176	ICMP	74	Echo (ping) request id=0x0001, seq=12/3072, ttl=128
192.168.17.138	ICMP	74	Echo (ping) reply id=0x0001, seq=12/3072, ttl=128

3. číslovaný úkol z návodu

Zadání úkolu: **Vyzkoušejte si filtr (ip.src==192.168.0.1) and (icmp or dns). IP adresu ve filtru však upravte, tak aby byla relevantní pro váš virtuální operační systém. Řádně dokumentujte do protokolu, stejně jako všechny ostatní úkoly.**

Řešení: Na obrázku nižšie vidieť, že zadaný filter filtruje ako icmp tak aj dns.

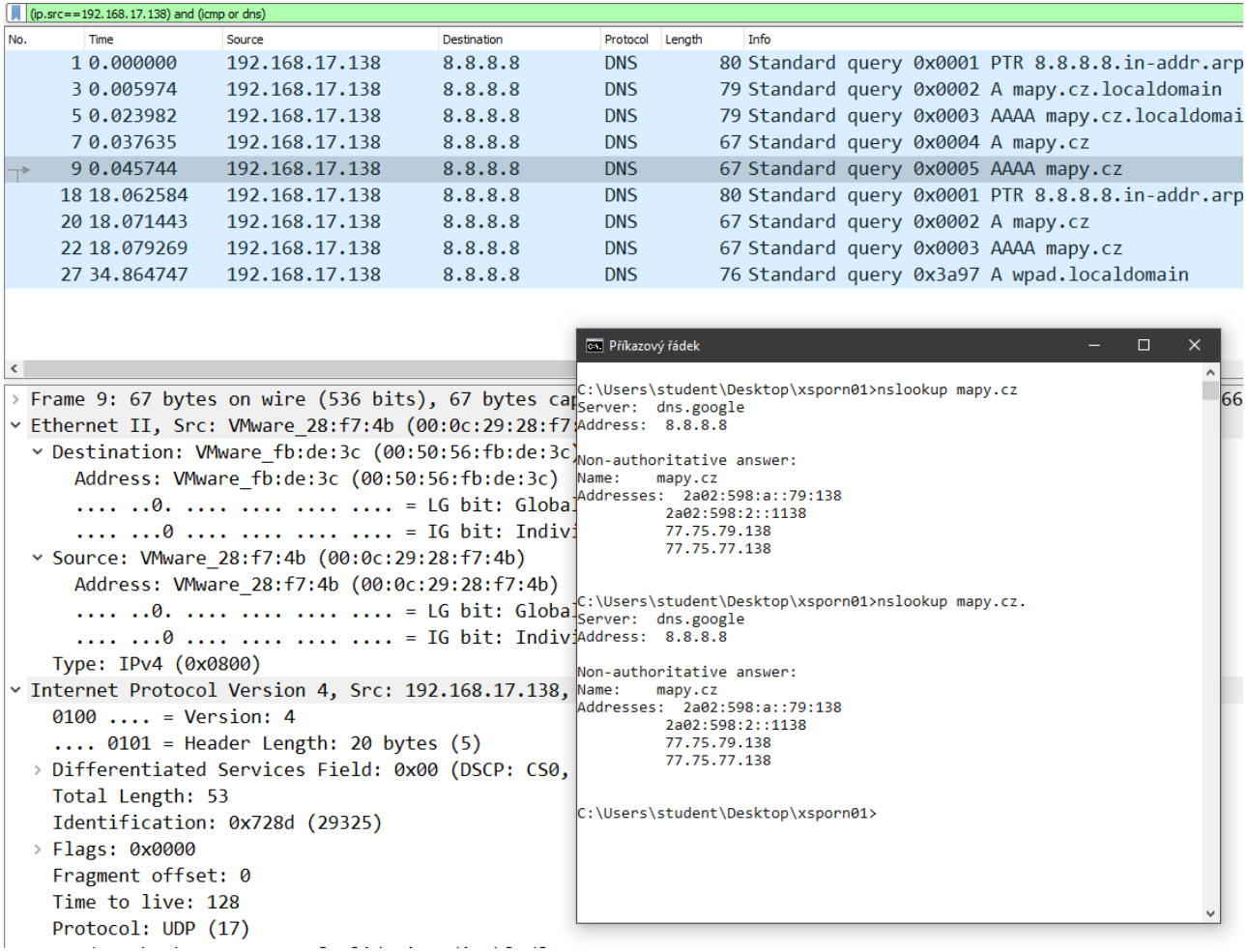


4. číslovaný úkol z návodu

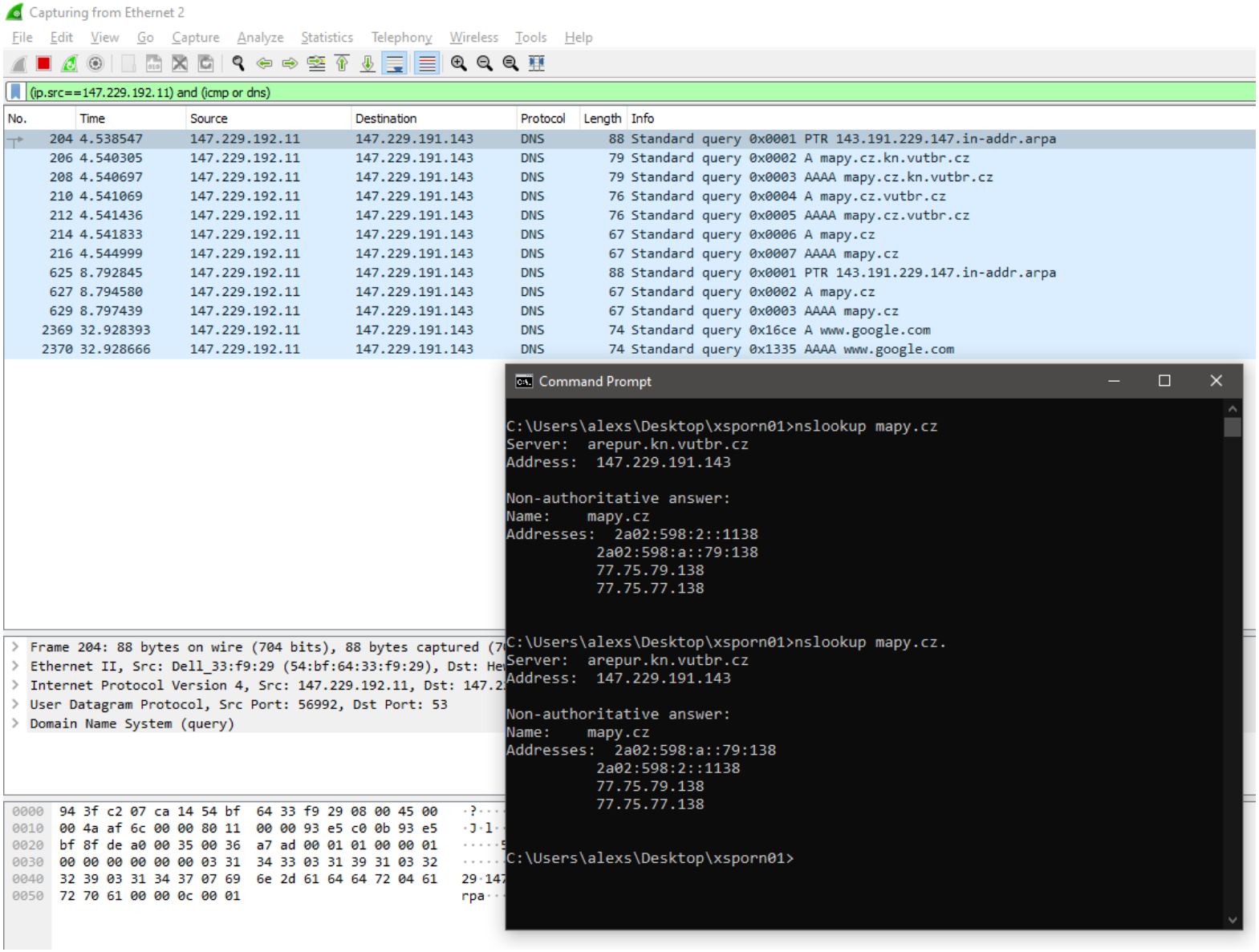
Zadání úkolu: **Výše uvedený příkaz vyzkoušejte i v hlavním OS a to ve variantě s tečkou na konci i bez ní. Jak se liší komunikace zachycená ve Wiresharku v těchto dvou případech?**

Řešení: Príkaz s bodkou hľadá DNS záznamy priamo na root serveri. Príkaz bez bodky zisťuje DNS najprv v lokálnej tabuľke.

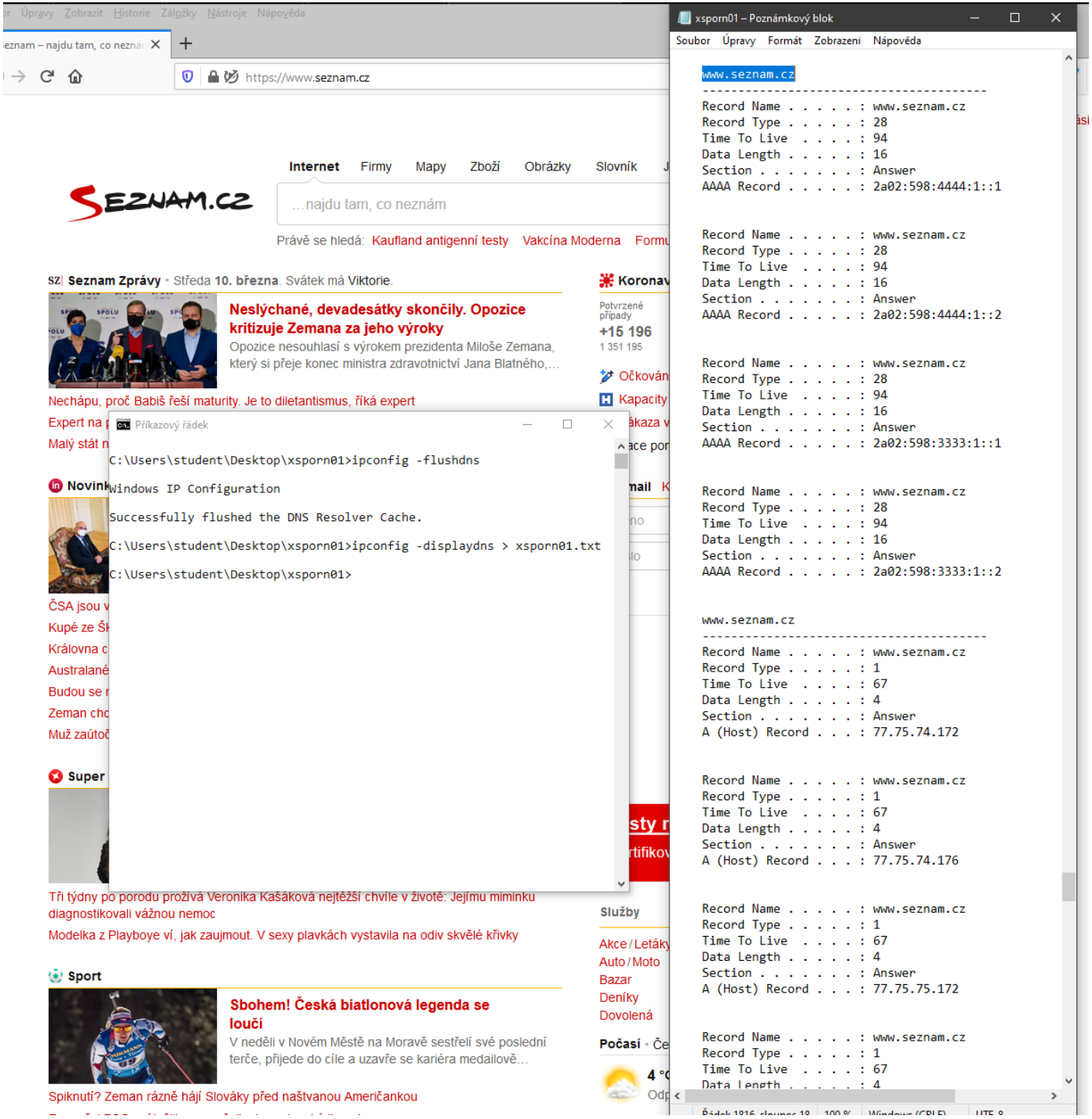
- Screenshot nižšie je z **VM:**



Screenshot nižšie je z hosťovského PC



-

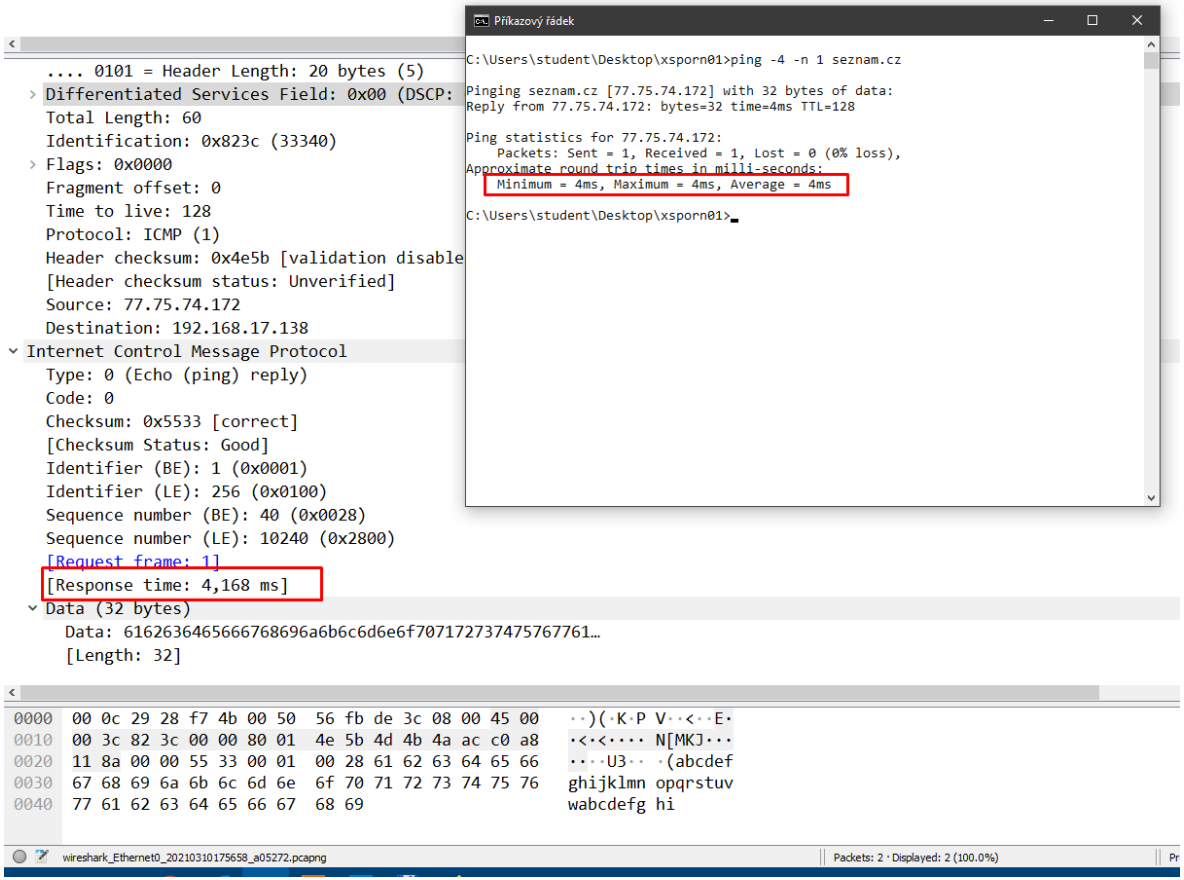

Úpravy Zobrazit Historie Záložky Nástroje Nápověda
https://www.seznam.cz
Internet Firmy Mapy Zboží Obrázky Slovník
SEZNAM.CZ
...najdu tam, co neznám
Právě se hledá: Kaufland antigenní testy Vakcína Moderna
Seznam Zprávy • Středa 10. března. Svátek má Viktorie.
Neslýchané, devadesátky skončily. Opozice kritizuje Zemana za jeho výroky
Opozice nesouhlasí s výrokem prezidenta Miloše Zemana, který si přeje konec ministra zdravotnictví Jana Blatného,...
Nechápu, proč Babiš řeší maturity. Je to diletantismus, říká expert
Expert na
Malý stát
Příkazový řádek
C:\Users\student\Desktop\xsporn01>ipconfig -flushdns
Windows IP Configuration
Successfully flushed the DNS Resolver Cache.
C:\Users\student\Desktop\xsporn01>ipconfig -displaydns > xsporn01.txt
C:\Users\student\Desktop\xsporn01>
Novink
ČSA jsou v
Kupé ze Š
Královna c
Australané
Budou se
Zeman cho
Muž zaúto
Super
Tři týdny po porodu prožívá Veronika Kašáková nejtěžší chvíle v životě: Jejímu miminku diagnostikovali vážnou nemoc
Modelka z Playboye ví, jak zaujmout. V sexy plavkách vystavila na odiv skvělé křivky
Sport
Sbohem! Česká biatlonová legenda se loučí
V neděli v Novém Městě na Moravě sestřelí své poslední terče, přijede do cíle a uzavře se kariéra medailově...
Spiknutí? Zeman rázně hájí Slováky před naštvanou Američankou
Koronav
Potvrzené případy
+15 196
1 351 195
Očkován
Kapacity
Služby
Akce / Letáky
Auto / Moto
Bazar
Deníky
Dovolená
Počasí
xsporn01 – Poznámkový blok
Soubor Úpravy Formát Zobrazení Nápověda
www.seznam.cz
Record Name . . . . . : www.seznam.cz
Record Type . . . . . : 28
Time To Live . . . . : 94
Data Length . . . . . : 16
Section . . . . . : Answer
AAAA Record . . . . . : 2a02:598:4444:1::1
Record Name . . . . . : www.seznam.cz
Record Type . . . . . : 28
Time To Live . . . . : 94
Data Length . . . . . : 16
Section . . . . . : Answer
AAAA Record . . . . . : 2a02:598:4444:1::2
Record Name . . . . . : www.seznam.cz
Record Type . . . . . : 28
Time To Live . . . . : 94
Data Length . . . . . : 16
Section . . . . . : Answer
AAAA Record . . . . . : 2a02:598:3333:1::1
Record Name . . . . . : www.seznam.cz
Record Type . . . . . : 28
Time To Live . . . . : 94
Data Length . . . . . : 16
Section . . . . . : Answer
AAAA Record . . . . . : 2a02:598:3333:1::2
www.seznam.cz
Record Name . . . . . : www.seznam.cz
Record Type . . . . . : 1
Time To Live . . . . : 67
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 77.75.74.172
Record Name . . . . . : www.seznam.cz
Record Type . . . . . : 1
Time To Live . . . . : 67
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 77.75.74.176
Record Name . . . . . : www.seznam.cz
Record Type . . . . . : 1
Time To Live . . . . : 67
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 77.75.75.172
Record Name . . . . . : www.seznam.cz
Record Type . . . . . : 1
Time To Live . . . . : 67
Data Length . . . . . : 4

5. číslovaný úkol z návodu

Zadání úkolu: **Jak se liší hodnota doby odezvy udávaná v příkazové řádce od té zobrazené ve Wiresharku?**

Řešení: Hodnota je v oboch prípadoch takmer rovnaká, jediný rozdiel je v zobrazení na počet desatinných miest.

```
    1 0.000000    192.168.17.138   77.75.74.172   ICMP      74 Echo (ping) request  id=0x0001, seq=40/10240, ttl=128
    2 0.004168    77.75.74.172     192.168.17.138 ICMP      74 Echo (ping) reply    id=0x0001, seq=40/10240, ttl=128
```



6. číslovaný úkol z návodu

Zadání úkolu: **Postupně zvyšujte hodnotu parametru -l a zjistěte tak maximální hodnotu objemu dat, které je možné odeslat ICMP pingem bez fragmentace z vašeho virtuálního operačního systému.**

Řešení: Maximálna hodnota, ktorú je možné nastaviť tak, aby sa paket nefragmentoval je **1472 B**.

```
    1 0.000000     192.168.17.138      147.229.2.90    ICMP     1514 Echo (ping) request  id=0x0001, seq=75/19200, ttl=128 (rep
    2 0.000922     147.229.2.90        192.168.17.138  ICMP     1514 Echo (ping) reply    id=0x0001, seq=75/19200, ttl=128 (req
```

```
Příkazový řádek

C:\Users\student\Desktop\xsporn01>ping -4 -n 1 -f -l 1472 vutbr.cz

Pinging vutbr.cz [147.229.2.90] with 1472 bytes of data:
Reply from 147.229.2.90: bytes=1472 time=1ms TTL=128

Ping statistics for 147.229.2.90:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\student\Desktop\xsporn01>ping -4 -n 1 -f -l 1473 vutbr.cz

Pinging vutbr.cz [147.229.2.90] with 1473 bytes of data:
Packet needs to be fragmented but DF set.

Ping statistics for 147.229.2.90:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

C:\Users\student\Desktop\xsporn01>
```

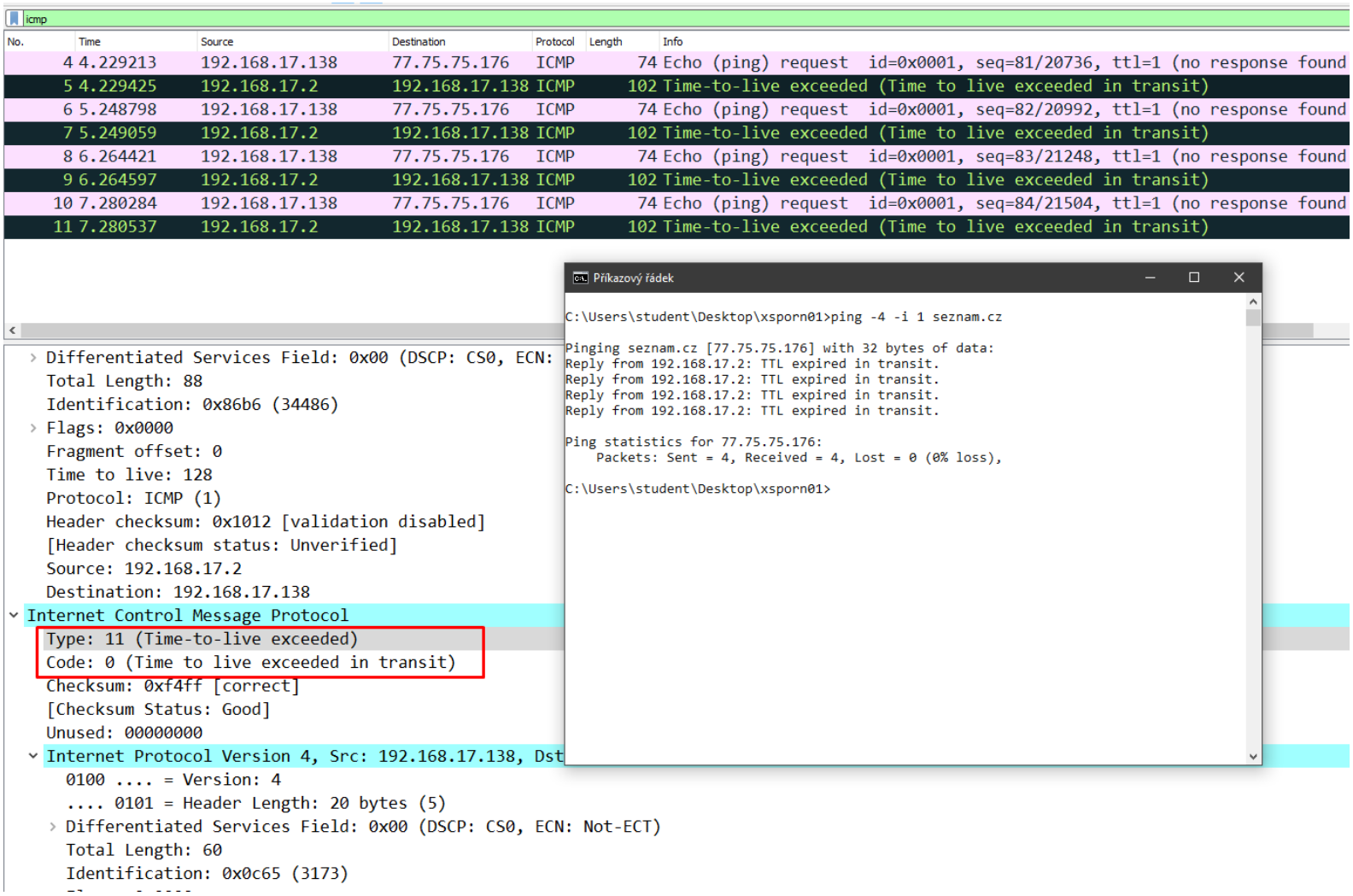
```
> Frame 1: 1514 bytes on wire (12112 bits), 1514 by                                    8D3
v Ethernet II, Src: VMware_28:f7:4b (00:0c:29:28:f7
  v Destination: VMware_fb:de:3c (00:50:56:fb:de:3c
      Address: VMware_fb:de:3c (00:50:56:fb:de:3c)
      .... ..0. .... .... .... .... = LG bit: Globa
      .... ...0 .... .... .... .... = IG bit: Indiv
  v Source: VMware_28:f7:4b (00:0c:29:28:f7:4b)
      Address: VMware_28:f7:4b (00:0c:29:28:f7:4b)
      .... ..0. .... .... .... .... = LG bit: Globa
      .... ...0 .... .... .... .... = IG bit: Indiv
    Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 192.168.17.138,
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0,
    Total Length: 1500
    Identification: 0x6c91 (27793)
  v Flags: 0x4000, Don't fragment
      0... .... .... .... = Reserved bit: Not set
      .1.. .... .... .... = Don't fragment: Set
      ..0. .... .... .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 128
    Protocol: ICMP (1)
    Header checksum: 0x0000 [validation disabled]
```

7. číslovaný úkol z návodu

Zadání úkolu: **Druhý případ zachyťte ve Wiresharku a vyhledejte typ a kód chyby ICMP protokolu, který souvisí se zprávou „TTL expired in transit“. Pozn.: Jedná se o případ neúspěšného pingu.**

Řešení:

- Typ 11 predstavuje, že time to live je prekročený
- Code 0 predstavuje že sa time to live prekročil pri prenose

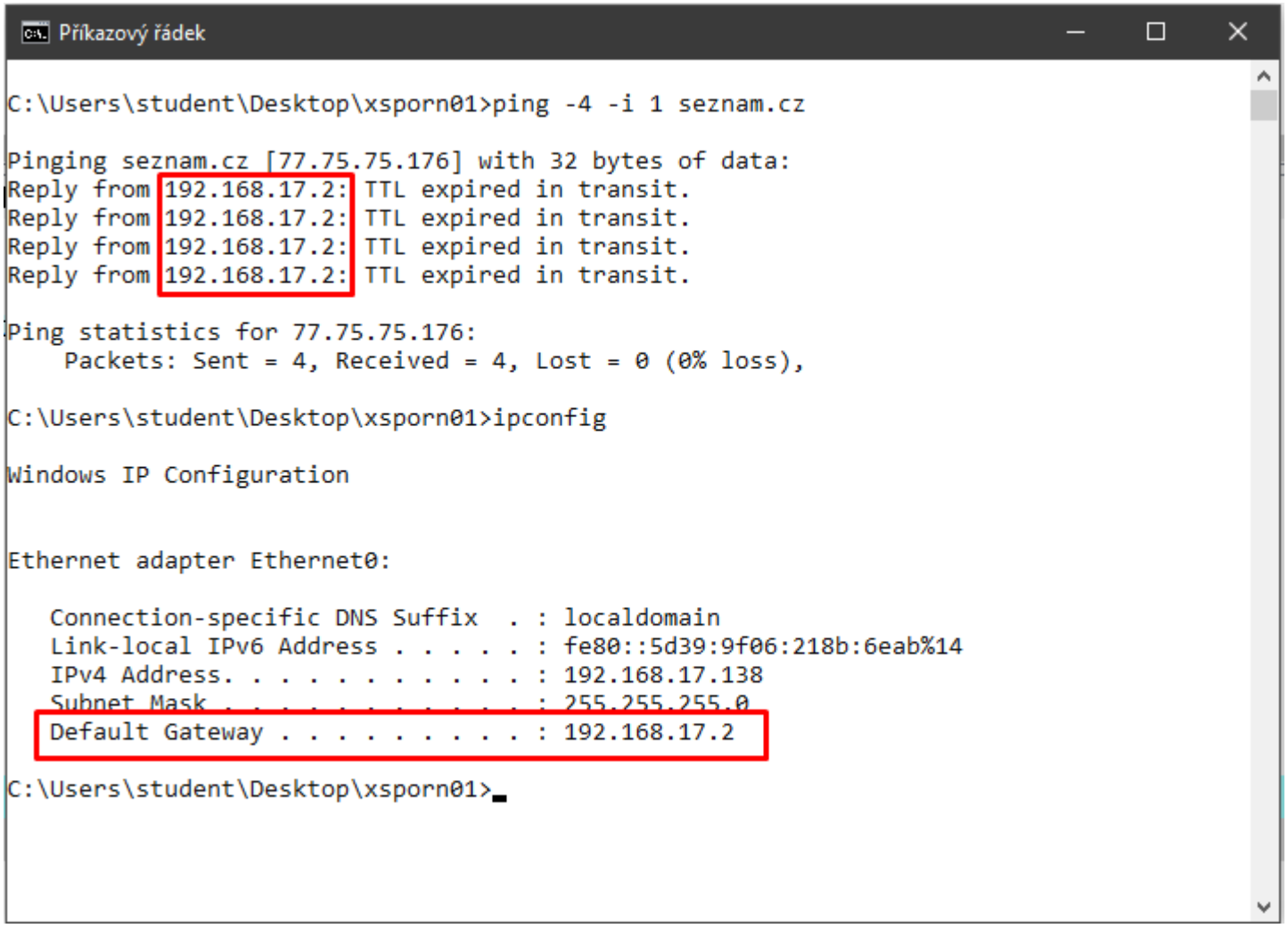


-

8. číslovaný úkol z návodu

Zadání úkolu: **Ve výpisu paketů ve Wiresharku vidíme chybové zprávy protokolu ICMP (v základním nastavení podbarveny černě), které v informační části mají popisek Time-to-Live exceeded. Kdo je odesilatelem těchto paketů z hlediska síťové vrstvy (IP adresy)?**

Řešení: Jedná sa o **Default Gateway** (východzia brána, router), ktorý má IP adresu **192.168.17.2**

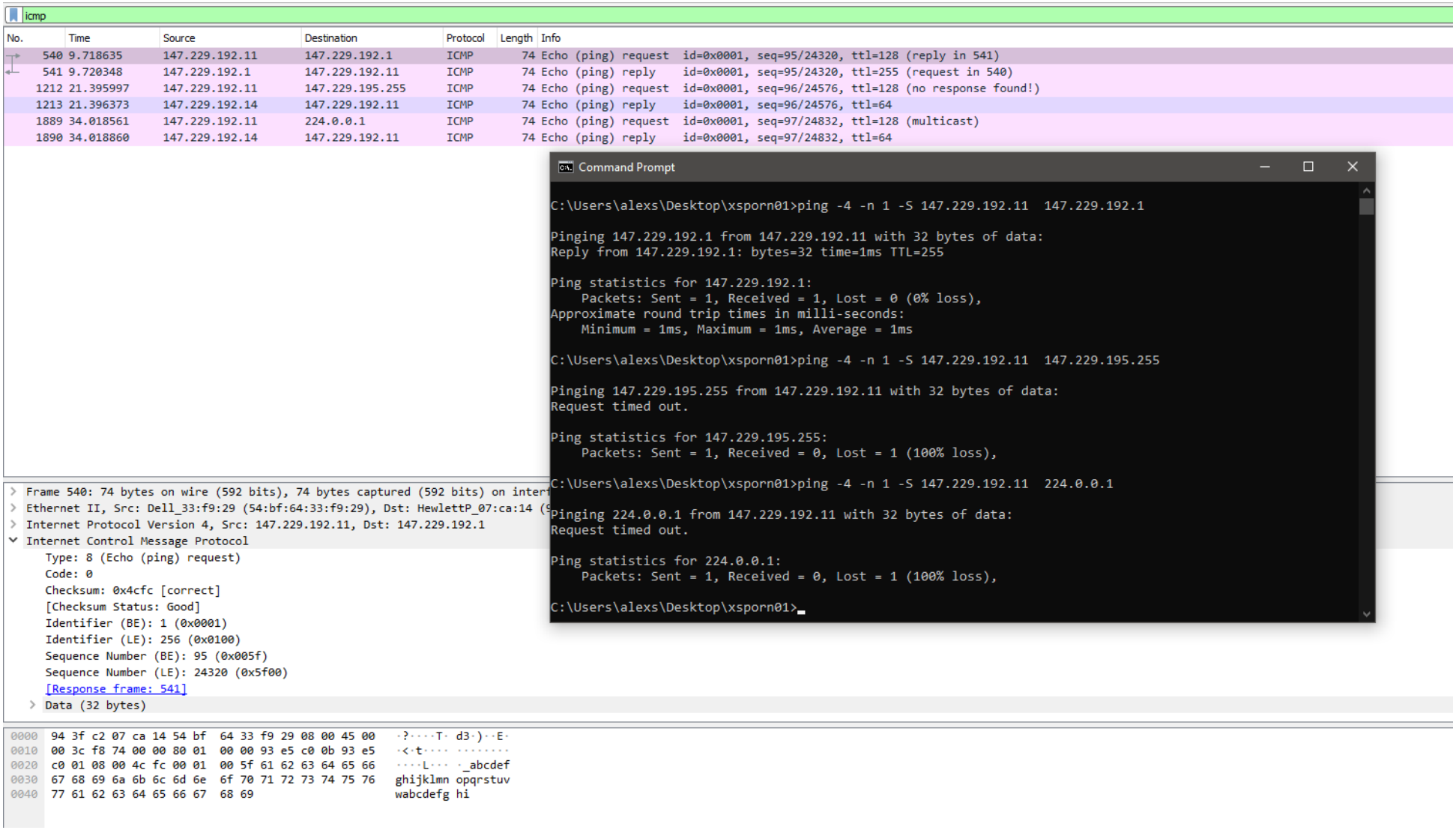


---

9. číslovaný úkol z návodu

Zadání úkolu: **Vyzkoušejte stejný pokus se třemi pingy odeslanými unicastem, broadcastem a multicastem ve svém hlavním OS. IP adresy upravte odpovídajícím způsobem. V případě, že některý z pingů ve Wiresharku nevidíte, byl pro jeho odeslání použit špatný interface. Pro použití správného rozhraní je nutné příkaz doplnit o parametr -S se zdrojovou IP adresou, která je nakonfigurovaná na daném rozhraní.**

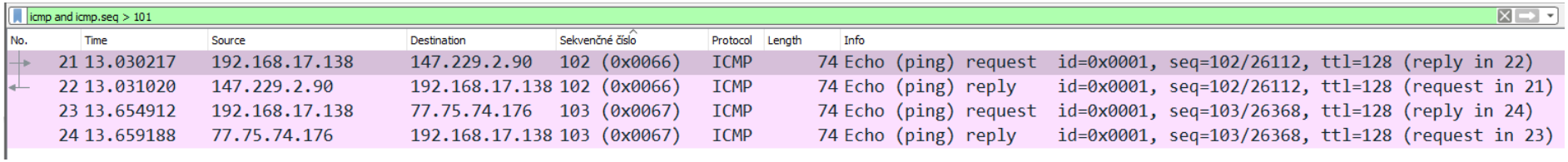
Řešení:



10. číslovaný úkol z návodu

Zadání úkolu: **Pomocí vámi navrženého filtru zobrazení paketů ve Wiresharku vyfiltrujte ze zobrazených pingů pomocí ICMP sekvenčních čísel pouze poslední dva zobrazené pingy (v obou případech zprávu echo request i echo reply).**

Řešení: **icmp and icmp.seq > 101**



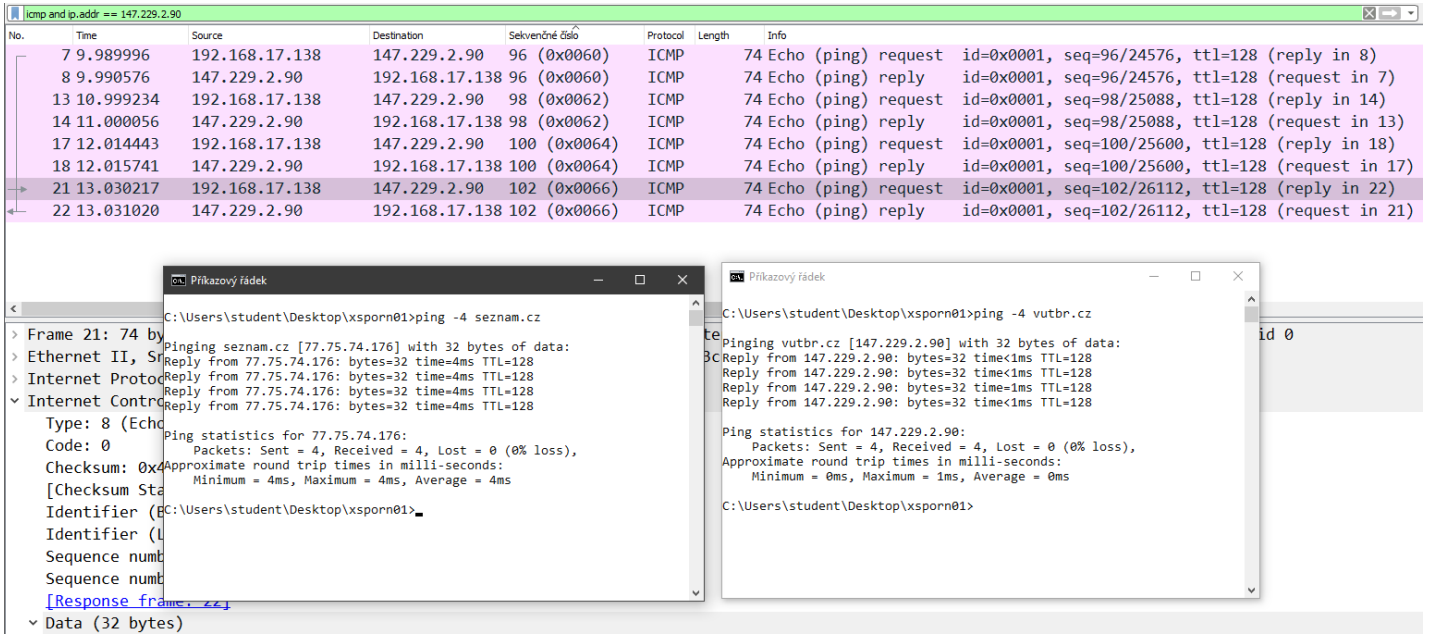
No.	Time	Source	Destination	Sekvenčné číslo	Protocol	Length	Info
21	13.030217	192.168.17.138	147.229.2.90	102 (0x0066)	ICMP	74	Echo (ping) request id=0x0001, seq=102/26112, ttl=128 (reply in 22)
22	13.031020	147.229.2.90	192.168.17.138	102 (0x0066)	ICMP	74	Echo (ping) reply id=0x0001, seq=102/26112, ttl=128 (request in 21)
23	13.654912	192.168.17.138	77.75.74.176	103 (0x0067)	ICMP	74	Echo (ping) request id=0x0001, seq=103/26368, ttl=128 (reply in 24)
24	13.659188	77.75.74.176	192.168.17.138	103 (0x0067)	ICMP	74	Echo (ping) reply id=0x0001, seq=103/26368, ttl=128 (request in 23)

---

11. číslovaný úkol z návodu

Zadání úkolu: **Jakým vhodným filtrem bychom zobrazili ve Wiresharku pouze pingy na vutbr.cz a odfiltrovali pingy na seznam.cz?**

Řešení: **icmp and ip.addr == 147.229.2.90**



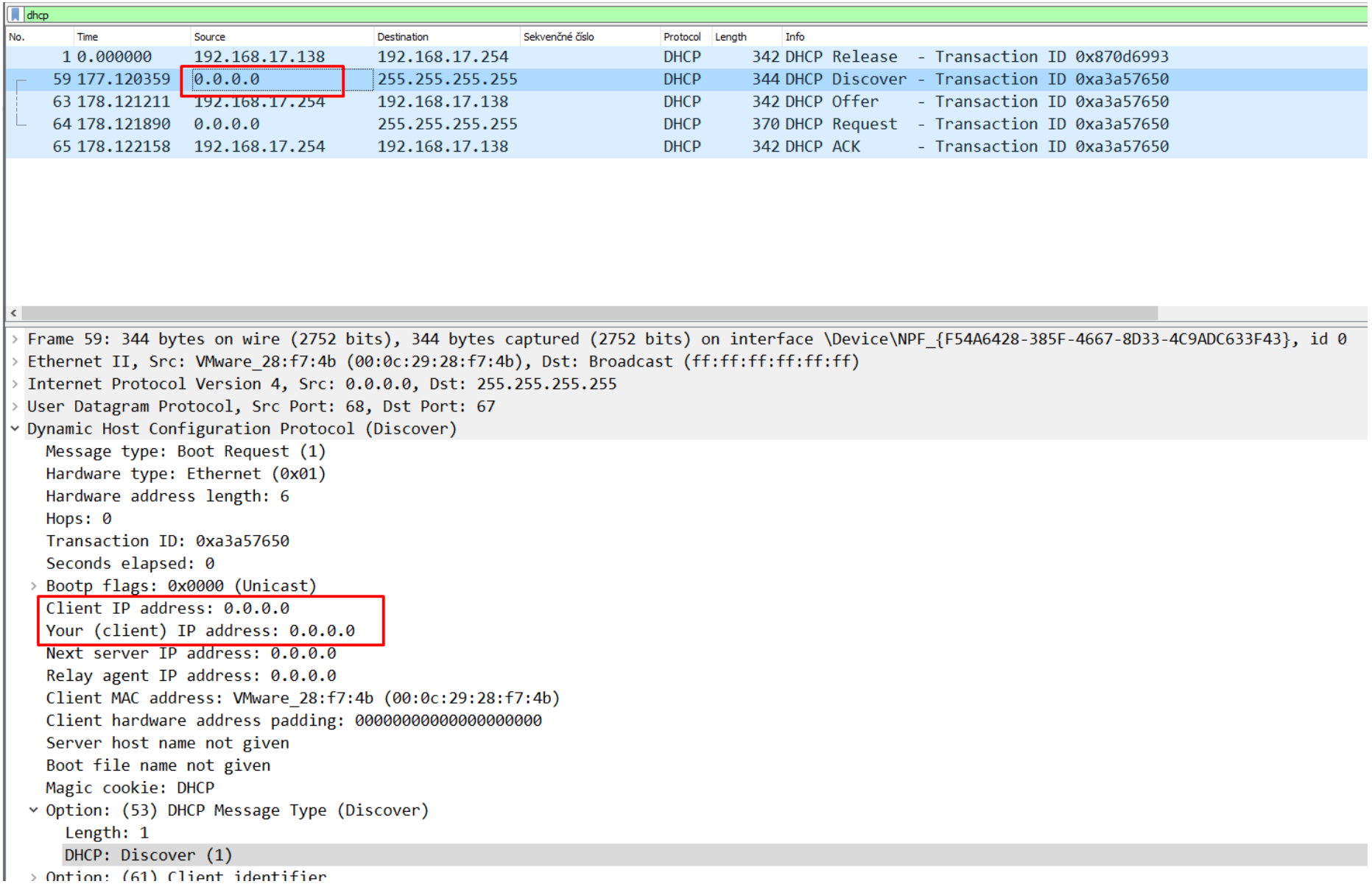
No.	Time	Source	Destination	Sekvenčné číslo	Protocol	Length	Info
7	9.989996	192.168.17.138	147.229.2.90	96 (0x0060)	ICMP	74	Echo (ping) request id=0x0001, seq=96/24576, ttl=128 (reply in 8)
8	9.990576	147.229.2.90	192.168.17.138	96 (0x0060)	ICMP	74	Echo (ping) reply id=0x0001, seq=96/24576, ttl=128 (request in 7)
13	10.999234	192.168.17.138	147.229.2.90	98 (0x0062)	ICMP	74	Echo (ping) request id=0x0001, seq=98/25088, ttl=128 (reply in 14)
14	11.000056	147.229.2.90	192.168.17.138	98 (0x0062)	ICMP	74	Echo (ping) reply id=0x0001, seq=98/25088, ttl=128 (request in 13)
17	12.014443	192.168.17.138	147.229.2.90	100 (0x0064)	ICMP	74	Echo (ping) request id=0x0001, seq=100/25600, ttl=128 (reply in 18)
18	12.015741	147.229.2.90	192.168.17.138	100 (0x0064)	ICMP	74	Echo (ping) reply id=0x0001, seq=100/25600, ttl=128 (request in 17)
21	13.030217	192.168.17.138	147.229.2.90	102 (0x0066)	ICMP	74	Echo (ping) request id=0x0001, seq=102/26112, ttl=128 (reply in 22)
22	13.031020	147.229.2.90	192.168.17.138	102 (0x0066)	ICMP	74	Echo (ping) reply id=0x0001, seq=102/26112, ttl=128 (request in 21)

---

12. číslovaný úkol z návodu

Zadání úkolu: **Jakou IP adresu používá stanice jako zdrojovou v situaci, kdy odesílá DHCP Discover paket?**

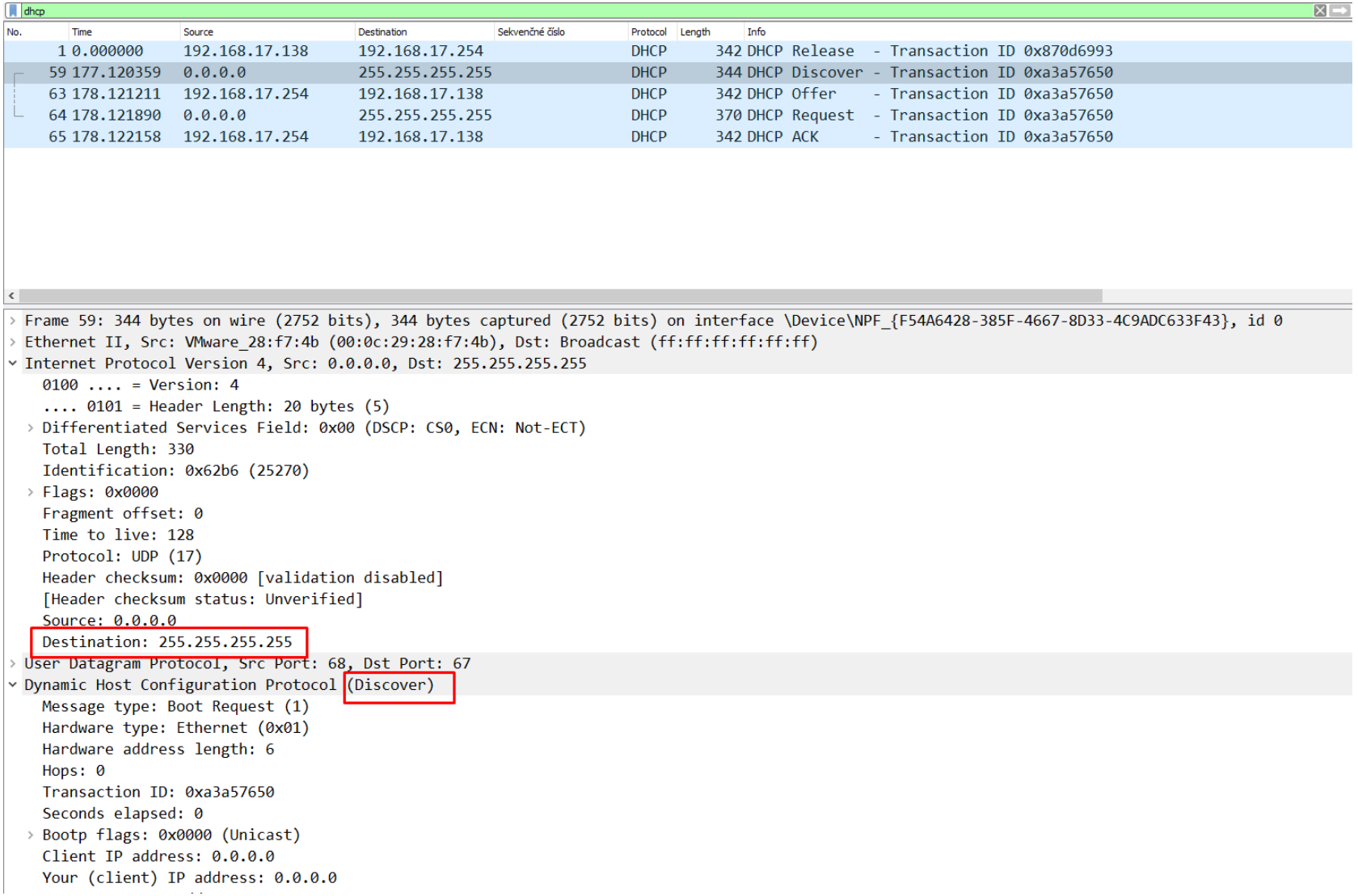
Řešení: Zdrojová stanica používa IP adresu **0.0.0.0** z dôvodu, že jej ešte nebola pridelená žiadna IP adresa.



13. číslovaný úkol z návodu

Zadání úkolu: **Na jakou cílovou IP adresu stanice odesílá DHCP Discover paket a z jakého důvodu?**

Řešení: Stanica odosiela požiadavku typu **Broadcast 255.255.255.255** všetkým dostupným zariadeniam na danej **LAN.** Zisťuje, či sa na LAN nachádza DHCP server, ktorý by potom unicastovou odpoveďou poslal požadovanú DHCP konfiguráciu. V nasledujúcej správe DHCP server s IP adresou **192.168.17.138** odpovedá klientovi.



14. číslovaný úkol z návodu

Zadání úkolu: **Ve zprávě DHCP ACK nalezněte hodnotu Lease Time a porovnejte ji s údaji v nově provedeném výpisu ipconfig /all.**

Řešení: Ako je možné vidieť na ukážke nižšie, tak sa obe hodnoty zhodujú. Jedná sa o **30** minútový lease time.

```
    1 0.000000    192.168.17.138  192.168.17.254  DHCP    342 DHCP Release  - Transaction ID 0x870d6993
   59 177.120359  0.0.0.0         255.255.255.255 DHCP    344 DHCP Discover - Transaction ID 0xa3a57650
   63 178.121211  192.168.17.254  192.168.17.138  DHCP    342 DHCP Offer    - Transaction ID 0xa3a57650
   64 178.121890  0.0.0.0         255.255.255.255 DHCP    370 DHCP Request  - Transaction ID 0xa3a57650
   65 178.122158  192.168.17.254  192.168.17.138  DHCP    342 DHCP ACK      - Transaction ID 0xa3a57650
```

```
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0xa3a57650
Seconds elapsed: 0
> Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0
Your (client) IP address: 192.168.17.138
Next server IP address: 192.168.17.254
Relay agent IP address: 0.0.0.0
Client MAC address: VMware_28:f7:4b (00:0c:29:28:f7:4b
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
v Option: (53) DHCP Message Type (ACK)
    Length: 1
    DHCP: ACK (5)
v Option: (54) DHCP Server Identifier (192.168.17.254)
    Length: 4
    DHCP Server Identifier: 192.168.17.254
v Option: (51) IP Address Lease Time
    Length: 4
    IP Address Lease Time: (1800s) 30 minutes
v Option: (1) Subnet Mask (255.255.255.0)
    Length: 4
    Subnet Mask: 255.255.255.0
```

```
Vybrat Příkazový řádek

   Host Name . . . . . . . . . . . . : DESKTOP-HVSVAFP
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : localdomain

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : localdomain
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-0C-29-28-F7-4B
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::5d39:9f06:218b:6eab%14(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.17.138(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Thursday, 11 March 2021 16:56:53
   Lease Expires . . . . . . . . . . : Thursday, 11 March 2021 17:26:52
   Default Gateway . . . . . . . . . : 192.168.17.2
   DHCP Server . . . . . . . . . . . : 192.168.17.254
   DHCPv6 IAID . . . . . . . . . . . : 100666409
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-27-D7-F3-51-00-0C-29-28-F7-4B
   DNS Servers . . . . . . . . . . . : 8.8.8.8
                                       8.8.4.4
   Primary WINS Server . . . . . . . : 192.168.17.2
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Users\student\Desktop\xsporn01>
```

```
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0110  00 00 00 00 00 00 63 82  53 63 35 01 05 36 04 c0   ......c· Sc5··6··
0120  a8 11 fe 33 04 00 00 07  08 01 04 ff ff ff 00 03   ···3···· ........
0130  04 c0 a8 11 02 06 04 c0  a8 11 02 0f 0b 6c 6f 63   ........ .....loc
0140  61 6c 64 6f 6d 61 69 6e  2c 04 c0 a8 11 02 ff 00   aldomain ,·......
0150  00 00 00 00 00 00                                 ......
```